

**AN ENHANCED SECURE DISTRIBUTED LEDGER INTEROPERABILITY
FRAMEWORK FOR MEDICAL SYSTEMS**

BUNDI DOROTHY GATWIRI

**A Thesis Submitted to the Institute of Postgraduate Studies of Kabarak University
in Partial Fulfillment of the Requirements for the Award of Doctor of Philosophy in
Information Technology Security and Audit**

KABARAK UNIVERSITY

NOVEMBER, 2024

DECLARATION

1. I do declare that:

- i. This thesis is my work and to the best of my knowledge, it has not been presented for the award of a degree in any university or college.
- ii. The work has not incorporated material from other works or a paraphrase of such material without due and appropriate acknowledgment.
- iii. The work has been subjected to processes of anti-plagiarism and has met Kabarak University 15% similarity index threshold.

2. I do understand that issues of academic integrity are paramount and therefore I may be suspended or expelled from the University or my degree may be recalled for academic dishonesty or any other related academic malpractices

Signed:.....

Date:.....

Bundi Dorothy Gatwiri

GDS/M/0270/01/19

RECOMMENDATION

To the Institute of Postgraduate Studies:

The thesis entitled “**An Enhanced Secure Distributed Ledger Interoperability Framework for Medical Systems**” written by **Bundi Dorothy Gatwiri** is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the thesis and recommend it be accepted in partial fulfillment of the requirement for award of Doctor of Philosophy in Information Technology Security and Audit.

Signed:.....

Date:.....

Prof. Simon M. Karume

School of Science and Engineering Technology

Kabarak University

Signed:.....

Date:.....

Prof. Stephen M. Mutua

School of Science and Engineering Technology

Kabarak University

COPYRIGHT

© 2024

Bundi Dorothy Gatwiri

All rights reserved. No part of this thesis may be reproduced or transmitted in any form using either mechanical, including photocopying, recording, or any other information storage or retrieval system without permission in writing from the author or Kabarak University.

ACKNOWLEDGEMENT

My immense gratitude goes to the Almighty God for seeing me through my academic journey. I would also like to express my sincere gratitude to my supervisors Prof. Simon Karume and Prof. Stephen Mutua for their invaluable guidance, support, and encouragement throughout my research. I appreciate Dr. Moses Thiga for being very instrumental in shaping my research. I am grateful to the academic and administrative staff of Kabarak University for the opportunity granted to undertake my postgraduate studies. I thank the National Commission for Science Technology and Innovation for authorization of this research and issuance of the research permit. The Kabarak University Research Ethics Committee (KUREC) for the review of my thesis document to ensure it adheres to the ethical guidelines.

I would like to thank my family, especially my spouse, children and parents, for their unwavering love and support. Before concluding this, it is essential to recognize my enduringly supportive foster sons, Kelly Maganah and Eric Kirima. Finally, I would like to thank my friends and colleagues for their encouragement and motivation. Without their help, this thesis would not have been possible.

DEDICATION

This thesis is dedicated to Dr. Amos Chege Kirongo, the most delightful and kind man I have ever met, as well as to my son, Abidan Mshindi Chege, and my daughter, Abigail Mugure Chege, whose sacrifices, prayers, and words of support have supported me throughout my academic career. There are no words to express the connection that unites us all, and you three have been my unwavering source of support. This thesis is dedicated to my parents, particularly to my late father Andrew Bundi, who supported me throughout my schooling and encouraged me to seek further education. I will forever be grateful for your belief in me. Your prayers, Moms Salome Kirongo and Jennifer Bundi, have kept me going. My father, Abel Kirongo, your love has inspired me to achieve my desire. Your encouraging comments, my sisters, brothers, nieces, and nephews, have exceeded my expectations in terms of strength, improvement, and fulfillment. Kelly, I am able to fulfill my aspirations because of your unwavering motivation and prayers. My church family, friends, and members of the Kaithe Home Fellowship for prayerfully providing me with support and encouragement during my academic journey.

ABSTRACT

Absence of consistent data formats and strong protocols in the current medical systems pose significant challenges to accomplishing interoperability. This study developed an enhanced secure Distributed Ledger (DL) interoperability framework as a solution to problems that impede interoperability of medical systems. The aim of the developed framework was to close gaps in the structure and meaning of data shared across medical systems so that it may be exchanged securely and consistently across various platforms. The goals of the study included determining the elements that contribute to safe interoperability; developing a secure framework for the exchange of medical data; verifying the proposed framework, and inventing an algorithm to strengthen security in DL interoperability frameworks. The study followed a mixed methods research design, incorporating systematic literature review, descriptive study and experimentation techniques to meet its objectives. The purpose of the systematic review and collection of qualitative and quantitative data was to provide insights into medical systems interoperability trends. Quantitative data was analyzed using SPSS version 28 and MS Excel. MAXQDA tool was used to analyze Qualitative data. The results are presented in tables, frequency tables, graphs and charts. The findings revealed that technical, semantic, structural and security are key factors that affect medical systems interoperability. Defined data formats and protocols are some of the fundamental components required for secure data sharing across various medical systems. The research solves many issues affecting secure data transmission across medical systems by developing an algorithm to fortify security in DT interoperability frameworks. Robust security elements are included in the secure framework for DL interoperability that has been built. Consensus, smart contracts, and data security layers are all part of the Master Medical DLT core. For standardized data formats and diagnostics, the framework incorporates standards such as HL7 FHIR, CDISC, ICD, and LOINC. Using administrative module in the framework, healthcare institutions may be accredited as nodes by regulatory organizations. Medical DLT Portal, API, and EMR system facilitate secure exchange of patient data in this framework. The study carried out validation processes to confirm that it can close current gaps in the existing medical systems, and guarantee safe interchange of medical data. The conclusions stress the need for medical systems to be standardized and secure interoperable, and emphasizes revolutionary structure of the created framework. The findings of the study will support policy recommendations for improvement of medical systems, and constant improvement of interoperability within medical systems.

Keywords: *Interoperability, Distributed Ledger Technology, Electronic Medical Records, Medical Systems, Secure Data Exchange, Security.*

TABLE OF CONTENTS

DECLARATION	ii
RECOMMENDATION	iii
COPYRIGHT	iv
ACKNOWLEDGEMENT	v
DEDICATION	vi
ABSTRACT	vii
TABLE OF CONTENTS	viii
LIST OF TABLES	xiii
LIST OF FIGURES	xiv
ABBREVIATIONS AND ACRONYMS	xvi
CONCEPTUAL AND OPERATIONAL DEFINITION OF TERMS	xviii
CHAPTER ONE	1
INTRODUCTION	1
1.1 Overview.....	1
1.2 Background to the Study	1
1.3 The Statement of the Problem	15
1.4 Objectives of the Study.....	17
1.4.1 General Objective of the Study	17
1.4.2 Specific Objectives of the Study	17
1.5 Research Questions.....	18
1.6 Justification of the Study	18
1.7 Significance of the Study.....	19
1.8 Scope of the Study	21
1.9 Limitations of the Study	22
1.10 Assumptions of Study.....	22
CHAPTER TWO	24
LITERATURE REVIEW	24
2.1 Introduction.....	24
2.2 Electronic Medical Systems	24
2.3 Distributed Ledger Technologies	26
2.3.1 Distributed Ledger Technologies Historical Perspective.....	27
2.3.2 Security in Distributed Ledger Technology	32
2.3.3 Algorithms used in Distributed Ledger	32

2.3.4 Distributed Ledger Platforms Functional Components.....	38
2.4 Distributed Ledger Technologies Architectural Frameworks	38
2.4.1 Difference between DLTs and Centralized Ledger	39
2.4.2 Existing DLTs Architectural Overview	41
2.4.3 High-Level Conceptual Architecture of DLTs.....	44
2.5 Evolution of Interoperability	45
2.6 Factors Affecting Interoperability of Medical System in Healthcare.....	47
2.6.1 Structural Factors	47
2.6.2 Semantic Factors	52
2.6.3 Security Factors.....	59
2.6.4 Technical Factors.....	64
2.7 Distributed Ledger Technologies Interoperability.....	68
2.8 Medical Systems Interoperability Frameworks	71
2.9 Theoretical Framework.....	75
2.9.1 DLT System Theory.....	75
2.9.2 Contractual Theory.....	76
2.10 Conceptual Framework.....	77
2.11 Research Gaps	80
CHAPTER THREE.....	83
RESEARCH DESIGN AND METHODOLOGY	83
3.1 Introduction.....	83
3.2 Research Design	83
3.2.1 Summary of the Methodology and Research Design.....	84
3.2.2 Systematic Literature Review	86
3.2.3 Descriptive Study	86
3.2.4 Framework Design Technique	87
3.2.5 Framework Development Setup.....	87
3.2.6 Interoperability Framework Validation.....	91
3.3 Location of the Study.....	91
3.4 Population of Study	92
3.5 Sampling Procedure and Sample Size	92
3.6 Instrumentation	94
3.6.1 Pilot Study.....	94
3.6.2 Validity of the Instrument.....	99

3.6.3 Reliability of the Instrument	100
3.6.4 Reliability and Validity Test Analysis Results	100
3.7 Data Collection Procedure	101
3.8 Data Analysis and Presentation	102
3.9 Framework Evaluation and Validation	102
3.10 Ethical Considerations	103
CHAPTER FOUR	104
DATA ANALYSIS, PRESENTATION AND DISCUSSION	104
4.1 Introduction.....	104
4.1.1 General Information	104
4.1.2 Systematic Literature Review Results	105
4.1.3 Response Rate	109
4.1.4 Medical System Software Developers Years of Experience.....	110
4.1.5 Type of Medical System Developed.....	111
4.1.6 Security as a Design Requirement	114
4.1.7 Adhering to Healthcare Design Policy	115
4.1.8 Correlational Analysis.....	118
4.2 Factors Affecting Secure Interoperability of Medical Systems.....	124
4.2.1 General Categories of the Factors Affecting Secure Interoperability of Medical Systems	124
4.2.1 Results Analysis and Discussion of the Findings	125
4.2.2 Specific Barriers to Secure Interoperability of Medical Systems under Technical, Semantic and Security Factors.....	130
4.2.2.1 Results Analysis and Discussion of the Findings	130
4.2.3 Type of Security Incorporated in the Developed Medical Systems.....	140
4.2.4 Level of Security used in the Medical Systems	142
4.2.5 Security Standards and Policies	144
4.2.6 Interoperability of Medical Systems	146
4.2.7 Architectures and Information Sharing.....	151
4.2.8 Results from the Interview Schedules and Discussions of the Findings.....	154
4.3 Algorithm to Enhance Security of Distributed Ledger (DL) Interoperability Framework for Medical Systems	155
4.3.1 Secure Medical DLT Interoperability Architectural Framework Design Requirements	156

4.3.2 The Medical DLT Interoperability Framework Architectural Design Tools and Technologies Used.....	158
4.3.3 The Enhanced Secure Distributed Ledger Interoperability Framework Architectural Layout.....	158
4.3.4 Patient Hospital Visit Instance Workflow.....	169
4.3.5 High level Workflow Design for Patient Hospital Visit Instance.....	172
4.3.6 A Detailed High-Level Explanation of the Enhance Secure Distributed Ledger Interoperability Framework Algorithm.....	174
4.3.7 Notations adopted in the Enhanced Secure Distributed Ledger Interoperability Framework Algorithm for Medical Systems.....	178
4.3.8 Proof of Authentication (PoA) Algorithm.....	179
4.3.9 Fetch Record Algorithm.....	182
4.3.10 Create Record Algorithm.....	183
4.3.11 Create Patient Wallet Algorithm.....	185
4.3.12 Generate and Store Symmetric Key (SK) Algorithm.....	187
4.3.13 Retrieve Symmetric Key (Sk) Algorithm.....	189
4.3.14 Sign Patient EMR Plaintext Algorithm.....	191
4.3.15 Hash Patient EMR Plaintext Algorithm.....	193
4.3.16 Encrypt Patient EMR Plaintext Algorithm.....	195
4.3.17 Decrypt Patient EMR Cipher Algorithm.....	197
4.4 Validation of the Developed Enhanced Secure Distributed Ledger Interoperability Framework for Secure Medical Data Exchange.....	199
4.4.1 Medical DLT Virtual Private Network (VPN) Module.....	200
4.4.2 Medical DLT Interplanetary File System (IPFS) Module.....	202
4.4.3 Medical DLT Smart Contract Module.....	203
4.4.4 The Master Medical DLT Module.....	207
4.4.5 The Patient Wallet Module.....	209
4.4.6 Medical DLT API Modules.....	210
4.4.8 Medical DLT EMR (Backend) Module.....	211
4.4.8 Medical DLT System (Web Interface) Module.....	212
4.4.8.1 Medical DLT System Login Interface.....	213
4.4.8.6 Medical DLT System Doctors Interface.....	218
4.4.9 Medical DLT Portal Module.....	219
4.5 Discussions of the Findings.....	226

4.5.1 Existing factors that affect Secure Interoperability of Medical Systems	227
4.5.2 Algorithms Designed to Enhance Secure Distributed Ledger Interoperability Framework for Medical Systems	227
4.5.3 An Enhanced Distributed Ledger Interoperability Framework for improving the Security of Medical Data Exchange Between Medical Systems	228
4.5.4 Validated Enhanced Secure Distributed Ledger Interoperability Framework	228
CHAPTER FIVE	236
SUMMARY, CONCLUSION AND RECOMMENDATIONS	236
5.1 Introduction.....	236
5.2 Summary of the Findings.....	236
5.2.1 To establish the factors affecting Secure Interoperability of Medical Systems	237
5.2.2 To Design an Algorithm to Enhance Security of DL Interoperability Framework for Medical Systems	237
5.2.3 To develop a Secure DL Interoperability Framework for Improving the Security of Medical Data Exchange Between Medical Systems.....	237
5.2.4 To validate the Developed Secure Distributed Ledger Interoperability Framework for Secure Medical Data Exchange	238
5.3 Conclusions.....	238
5.4 Recommendations.....	244
5.4.1 Policy Recommendations	244
5.5 Recommendations for Further Research	247
REFERENCES	249
APPENDICES.....	264
Appendix I: Questionnaire	264
Appendix II: Interview Guide Questions	268
Appendix III: Validation Guide Questionnaire.....	270
Appendix IV: KUREC Clearance Letter.....	274
Appendix V: NACOSTI Research Permit.....	275
Appendix VI: Evidence of Conference Participation.....	276
Appendix VII: List of Publications	277

LIST OF TABLES

Table 1: Summary of the Consensus Algorithms used in Distributed Ledgers.....	35
Table 2: A summary of the differences between the Distributed Ledger and Centralized Ledger.....	41
Table 3: Summary Table of the Research Gaps	81
Table 4: Summary Table of the Methodology and Research Designs	85
Table 5: Reliability and Validity Test Analysis.....	101
Table 6: Summary of Search Results.....	107
Table 7: Summary of Systematic Literature Review Results	108
Table 8: Summary of the Correlation Analysis	119
Table 9: Categories of Factors Affecting the Interoperability of Medical Systems	125
Table 10: Level of Awareness of Medical System Design.....	144
Table 11: Summary of the Awareness of Interoperability of Medical Systems.....	147
Table 12: Summary of the Notations used in the Developed Framework Algorithms....	179

LIST OF FIGURES

Figure 1: Medical Systems Interoperability Levels.....	3
Figure 2: High-level Conceptual Architecture of DLTs.....	38
Figure 3: Difference between DLTs and Centralized Ledger	40
Figure 4: An Overview of the Existing DLTs	43
Figure 5: Operation & Maintenance Layer of High-Level Conceptual Architecture of DLTs	44
Figure 6: Conceptual Framework	79
Figure 7: An in-depth implementation Conceptual Framework of an enhanced Secure Distributed Ledger Interoperability Framework for Medical Systems	80
Figure 8: System Architecture Diagram.....	90
Figure 9: Network Gateway Diagram	91
Figure 10: Years of Experience in Development of the Medical Systems.....	96
Figure 11: Type of Information Systems Developed	97
Figure 12: Knowledge on Interoperability of Medical Systems.....	99
Figure 13: Key findings based on the Analysis Showing Percentages of the type of Medical System Developed by the Medical Systems Software Development Companies	112
Figure 14: Adherence to the Healthcare Policy.....	116
Figure 15: Summary of the Barriers to Interoperability of Medical Systems	130
Figure 16: Type of Security Incorporated in the developed Medical Systems	141
Figure 17: Level of Security used in the Medical Systems	143
Figure 18: Security Standards Applied in the Medical Systems	145
Figure 19: Levels of Medical Systems Interoperability	148
Figure 20: Architectural Approaches Used in Developing Medical Systems for Data Sharing	152
Figure 21: Secure Medical DLT Interoperability Architectural Framework Design Requirements.....	157
Figure 22: The Enhanced Secure Distributed Ledger Interoperability Framework Architectural Layout	159
Figure 23: Fetch Record Algorithm Flowchart	181
Figure 24: Fetch Record Algorithm Flowchart	183

Figure 25: Create Record Algorithm Flowchart.....	185
Figure 26: Create Patient Wallet Algorithm Flowchart.....	187
Figure 27: Generate and Store Symmetric Key (SK) Algorithm Flowchart	189
Figure 28: Retrieve Symmetric Key (Sk) Algorithm Flowchart	191
Figure 29: Sign Patient EMR Plaintext Algorithm Flowchart	193
Figure 30: Hash Patient EMR Plaintext Algorithm Flowchart.....	195
Figure 31: Encrypt Patient EMR Plaintext Algorithm Flowchart	197
Figure 32: Decrypt Patient EMR Plaintext Algorithm Flowchart	199
Figure 33: Medical DLT Virtual Private Network (VPN)	200
Figure 34: The Medical DLT VPN using WireGuard.....	201
Figure 35: Medical DLT InterPlanetary File System (IPFS) Module	203
Figure 36: Medical DLT Smart Contract Module	204
Figure 37: The Patient Wallet Module	210
Figure 38: Medical Distributed Ledger Technology (DLT) Application Programming Interface (API) Modules	211
Figure 39: Medical DLT Electronic Medical Records (EMR) Backend Module	212
Figure 40: Medical DLT System web interface for Hospital 1 and Hospital 2.....	213
Figure 41: Medical DLT System Login Interface	213
Figure 42: Medical DLT system Dashboard	215
Figure 43: Medical DLT System Add Patient Interface.....	216
Figure 44: Medical DLT System Administrator Interface used for Creating Role and Role Management	217
Figure 45: Medical DLT System Nurse Interface	218
Figure 46: Medical DLT System Doctors Interface	219
Figure 47: Medical DLT Portal	220
Figure 48: The Medical DLT Portal Dashboard.....	221
Figure 49: Dashboard /Patient (Generate and Store Key/ Retrieve Key/ Grant and Revoke)	222
Figure 50: Medical DLT Portal Patients Record Page	223
Figure 51: Medical DLT System Fetch Historical Patient Records Sub-Module	224
Figure 52: Patient Multi-Factor Layer Authentication.....	225
Figure 53: Successful Symmetric Key Authentication for Decryption of Patient Records.....	226

ABBREVIATIONS AND ACRONYMS

API	Application Programming Interface
APTs	Advanced Persistent Threats
CDISC	Clinical Data Interchange Standards Consortium
CT	Clinical Terms
DAGs	Directed Acyclic Graphs
DBMS	Database Management Systems
DDBMS	Distributed Database Management Systems
DICOM	Digital Imaging and Communications in Medicine
DL	Distributed Ledger
DLT	Distributed Ledger Technology
dPOS	Delegated Proof of Stake
EHRs	Electronic Health Records
EHealth	Electronic Health
EIF	European eHealth Interoperability Framework
ReEIF	Refined eHealth European Interoperability Framework
EMR	Electronic Medical Records
eReferral	Electronic Referral
FHIR	Fast Healthcare Interoperability Resources
GDPR	Global Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
HL7	Health Level Seven
HIMSS	Healthcare Information and Management Systems Society
HTTP	Hypertext Transfer Protocol
ICD	International Categorization of Diseases
ICT	Information and Communications Technology
IGS	Interoperability Gateway Service
IPFS	InterPlanetary File System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
LOINC	Logical Observation Identifiers Names and Codes

KHISIF	Kenya Health Information Systems Interoperability Framework
MIS	Medical Information System
MoH	Ministry of Health
NAHIT	National Alliance for health Information Technology
NHIN	National Health Information Network
ONC	Office of the National Coordinator for Health Information Technology
PACs	Picture Archiving and Communication system
P2P	Peer-to-peer architecture
PHI	Personal Health Information
POI	Proof of Importance
POS	Proof of Stake
POW	Proof of Work
RPC	Remote Procedure Call
RBAC	Role-Based Access Control
SCP	Stellar Consensus Protocol
SNOMED	Systemized Nomenclature of Medicine
RPCA	Ripple Protocol Consensus Algorithm
TCP/IP	Transmission Control Protocol and Internet Protocol
TLS	Transport Layer Security
TMA	Tele-medicine Alliance
UHC	Universal Health Coverage
VPN	Virtual Private Network
WHO	World Health Organization
XML	Extensible Markup Language

CONCEPTUAL AND OPERATIONAL DEFINITION OF TERMS

Distributed Ledger also called a shared ledger or distributed ledger technology or DLT is a database or ledger of all transactions or agreements that is openly shared and synchronized between numerous sites, organizations, and locations and available to many users.

Interoperability refers to the ability of the computer systems or software, devices and applications from different software vendors to connect, exchange, integrate and make use of the exchanged data or information that is existing across different computer systems located at different organizations, regions and national boundaries with an aim to provide timely and seamless portability of information and optimize the services.

Medical System/ Medical Information System is an information system that helps medical practitioners in a medical facility to collect, manage, store, and share patients electronic medical record with an aim to diagnose, prescribe and treat patients.

Electronic Medical Record /Electronic Health Record this is an electronic version of a patients' medical history, demographic data, treatment plans, diagnosis reports, medications administered and laboratory reports that is maintained in a medical system of a medical facility over a period of time.

Ehealth is the use of information communication technology to support and aid medical service delivery in healthcare sector by automating medical services from data collection, processing, storing and dissemination of medical information.

Blockchain is one type of a distributed ledger that holds decentralized data and transactions that is duplicated and shared across multiple nodes offering transparent, immutable, time-stamped, anonymous, encrypted and verifiable records for every transaction without the need of the central repository.

Structural Interoperability this is the level of interoperability that defines the data format, syntax and organization of data exchange including the data field level, message format standards for packaging and interpretation.

Semantic Interoperability the usage of publicly available value sets and coding vocabularies, as well as agreed semantics for data elements, all contribute to a high level of interoperability that benefits both the user and the data itself.

Fast Healthcare Interoperability Resources is an interoperability standard that was developed by HL7 to exchange healthcare data and information electronically between different medical information systems regardless of how it was created and stored in those medical systems.

Smart Contract this is a program that is stored in a distributed ledger and will run once the predetermined conditions are met hence executing an agreement between various participants in the distributed network.

E-referrals or Electronic Referrals This is a digital or an electronic platform that enables the seamless transfer of patient information and clinical requests between medical service providers from a primary level medical facility to a secondary level medical facilities in the process of ensuring that patients receive specialized healthcare services using a medical management information system.

Interplanetary File System IPFS is a decentralized file storage and sharing network that uses content-addressing to provide each file its own distinct identifier throughout the global namespace that links all of the IPFS nodes.

Universal Health Coverage means making sure people and places can get the diagnostic, treatment, and care they need to stay healthy, and that those services are available when and where they need them without putting a strain on patients' budgets.

CHAPTER ONE

INTRODUCTION

1.1 Overview

This chapter gives an overview of the research thesis by outlining the background of medical systems interoperability architectural levels, frameworks and protocols used in distributed ledger technologies, which inform the study's objectives, research questions, justification, significance, scope, limitations, and assumptions that guided the research.

1.2 Background to the Study

The permeability of technological solutions has been on a steady rise across various organizations and domains. Consequently, information systems are becoming complex, dynamic, and distributed in terms of their data structure, architectural designs, structural layouts, semantics, codifications, standards and protocols (Gagnon & Stephen, 2018). As a result, they are used to store crucial and vital content which can be used in informing critical decisions. Subsequently, the need to share data resources, collaborate and exchange information securely across different technological platforms in order to facilitate faster decision making processes has occasioned a challenge of ensuring reliable interoperability between systems (Kannengießer et al., 2020).

In order to provide timely and seamless information portability and optimize services, interoperability of computer systems, software, devices, and applications is necessary, to aid connection, exchange, integration, and utilization of existing data or information across different computer systems, organizations, regions, and national boundaries (Belchior et al., 2020) (Belchior et al., 2020). However, it is not guaranteed that any interoperable systems can provide the crucial security concerns that arise in data transmission. The sensitivity of data being shared, its storage, and access varies from one sector of application to another (Liang et al., 2018). In the context of electronic health

(eHealth), interoperability has been defined as the ability to share health data among computerized systems of different organizations located in different geographical locations, while maintaining security and safety of the exchanged data (National health information network (NHIN) (HIMSS, 2022; European Commission & Directorate-General for Communications Networks Content and Technology, 2013; Tele-medicine Alliance (TMA) , 2020; National Alliance for health Information Technology (NAHIT) , 2005).

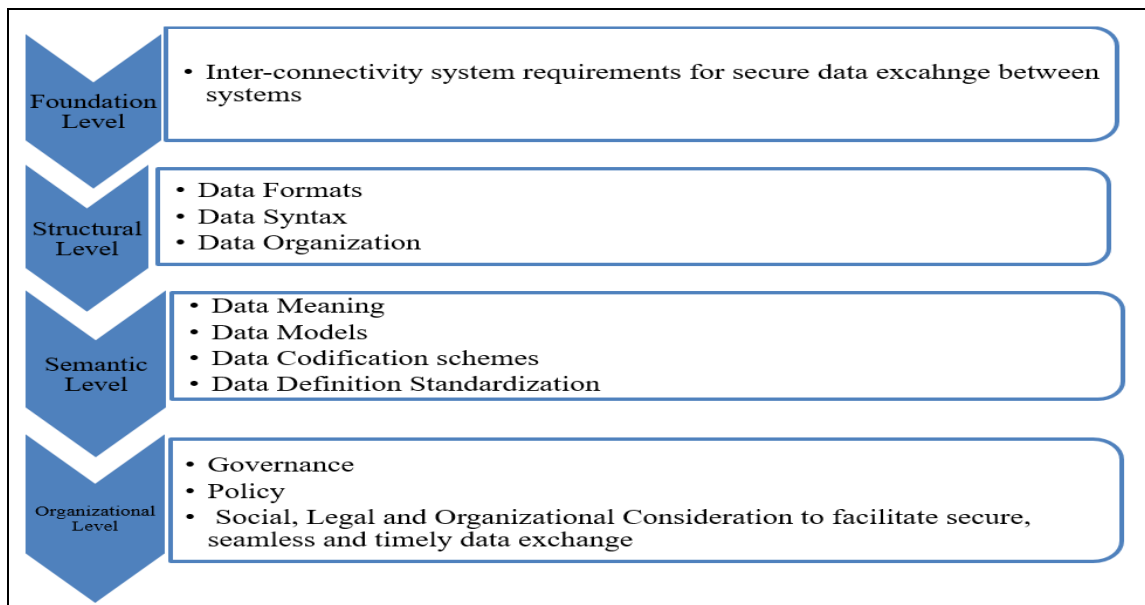
The healthcare sector might potentially overcome interoperability issues and transform data sharing, security, and efficiency by using distributed ledger technology (DLT) and blockchain (Thakur, 2022) and (Zhang & Boulos, 2022). Security and interoperability of medical DLTs are the main emphasis of this research. The study seeks to highlight the need for secure data interchange, data formats, data meaning, and better governance policies. It outlines interoperability levels as the foundation level, which constitutes interconnectivity system requirements for safe system-to-system data exchange. The structural level, which incorporates data organization, data syntax, and data formats. The semantic level, which represents standardization of data definition, data models, data codification schemes, and data meaning. The operational level, which defines secure, frictionless, and fast data transmission as facilitated by organizational, social, legal, and governance considerations. DLT integration in medical systems presents viable ways to overcoming interoperability constraints, and facilitating safe and effective exchange of electronic health data (Thakur, 2022). The aim of integrating DLT and blockchain into healthcare infrastructure is to improve patient involvement, and enhance data security and control (E. Li et al., 2022).

The use of block chain which is one of the types of DLTs, has been the subject of recent studies that have emphasized the advantages of decentralization, immutability, improved

security measures, and continuous availability (Baysal et al., 2023). In order to enable systems to integrate health data and communicate information to improve services to stakeholders, research on DLT interoperability has emerged (Bokolo, 2022). DLT and blockchain integration in the healthcare industry has the potential to alleviate interoperability issues, facilitate data interchange, and improve the security and effectiveness of medical systems. Recent research has sought to develop safe, decentralized data sharing protocols, while addressing interoperability constraints (Makridakis & Christodoulou, 2019). Integrating DLT into healthcare infrastructure presents viable ways to overcome interoperability issues, and enhance the sharing of electronic health data. The goal of this research in the field of DLT is to provide safe, decentralized data sharing protocols, while addressing interoperability constraints. The description of medical system interoperability levels is as shown in Figure 1.

Figure 1

Medical Systems Interoperability Levels



Whereas much of the business data can be shared without raising much sensitivity issues, leakages in the sharing of electronic medical records (EMR) can lead to severe

consequences to the parties involved. As a result, most existing medical systems are specific to an organization and are developed with a centralized database. Ensuring data security and trust during sharing of medical data remains a challenge for most of data systems, since they lack defined and standardized data formats and exchange protocols (Chenthara et al., 2020). Therefore, there is need to develop secure technologies that allow health organizations to share medical data while maintaining control and protection. Some available technological solutions to data security challenges include the use of database management systems, use of firewall, use of web services, and use of Blockchain technology.

The aforementioned technological solutions have some individualized limitations. To start with the Database Management Systems (DBMS) limitations includes vulnerability to cyber-attacks which implies that although database management systems (DBMSs) come with a number of security measures, such as encryption and access controls, they are nevertheless susceptible to cyber-attacks like SQL injection, data breaches, and unauthorized access if they are not maintained or configured correctly (Syed Arif Isalm & Dr.M.Mohan Kumar, 2022). Single Point of Failure is another limitation of the DBMS. There is a chance that a centralized database system will fail. Access to patient data and vital healthcare information may be disrupted if the database server goes down or is compromised (Xiong et al., 2020). Additionally, scalability Issues are also inevitable when dealing with DBMS. With the growing demand for storage and processing power in healthcare companies, traditional DBMS systems may face scalability issues when managing massive volumes of healthcare data (Prince, 2021). Lastly, the problems with data integrity may arise. It can be difficult to maintain data integrity, especially in contexts with several users where simultaneous access and updates to the database occur. Without proper error handling mechanisms and

transaction management data integrity issues such as data corruption or loss may arise when using DBMS. (Y. Li & Liu, 2021).

Secondly the use of firewall technologies with the aim of trying to sort the security challenge comes with some limitations which range from restriction and insufficient defense against advanced threats. Firewalls can be successful in sifting through network traffic and preventing unauthorized users from accessing network resources, but they can be less successful in identifying and thwarting sophisticated cyber threats like malware that evades conventional firewall defenses, advanced persistent threats (APTs), and zero-day attacks (Tabassum & Lebda, 2019). Potential insider threat blind spot is another limitation with the use of firewall. Firewalls tend to concentrate on threats coming from the outside and may not be able to identify or neutralize insider threats coming from the healthcare company. Sensitive healthcare data may be accessed by malicious insiders or hacked user accounts utilizing weaknesses to get past firewall defenses (Yeo & Banfield, 2022).

Complexity and maintenance overhead is also a limitation. Firewall configuration management and upkeep can be difficult and resource-intensive, especially for large-scale healthcare networks with numerous entry points and dispersed IT infrastructure. Patch management, routine updates, and configuration audits are required to guarantee the efficacy of firewalls and adherence to security guidelines (Shaik & Subhani, 2018). Lastly the performance impact because of their packet inspection, rule processing, and logging functions, firewalls can cause latency and overhead in network traffic. Network performance and user experience can be negatively impacted by firewall performance degradation in high-throughput healthcare environments where real-time access to patient data is essential (Shaik & Subhani, 2018).

Use of web services is another technological solution used to address the security challenges in healthcare. This also is faced by some limitations that include the security risks in API communication. In order to communicate with various healthcare systems and applications, web services rely on application programming interfaces (APIs). If an API is not properly secured or verified, it can lead to security issues like data leakage, illegal access, and API abuse.

Other common security vulnerabilities include injection attacks, weak authentication, exposed sensitive data, and inadequate logging and monitoring, can affect web services (Dawood et al., 2023). To reduce these dangers, healthcare organizations need to put strong security measures in place. Challenges with compliance and interoperability especially when integrating web services, it can be difficult to ensure compliance with healthcare standards like HIPAA (Health Insurance Portability and Accountability Act) and to achieve interoperability between diverse healthcare systems (Torab-Miandoab et al., 2023). Standardized procedures, encryption techniques, and authentication systems must be implemented by healthcare institutions in order to promote safe data interchange and interoperability. Issues with Scalability and Performance also arise when dealing with web services. Web services may have difficulties with scalability and performance when dealing with big amounts of healthcare data or multiple requests for simultaneous services. For web services to function reliably and responsively in healthcare settings, caching methods, infrastructure resource scaling, and service endpoint optimization are critical (Farahani et al., 2021).

Lastly use of Blockchain technologies is also faced by challenges that range from scalability and performance constraints, regulatory and compliance uncertainty, data privacy and confidentiality challenges and interoperability and integration complexity. Scalability and performance limitations arise when processing a high volume of

transactions or storing huge datasets. blockchain technology particularly public blockchains like Bitcoin or Ethereum may encounter scalability and performance issues. Solutions for scalability like sharding or layer 2 protocols are still in the early stages of research and might not be appropriate for real-time data processing and access in healthcare applications (Soltani et al., 2022). Uncertainty in regulation and compliance is another limitation. There are still a lot of unanswered questions about data privacy, security requirements, and legal compliance in the regulatory environment around blockchain technology in healthcare. To make sure that blockchain implementations adheres to legal and regulatory standards, healthcare firms must manage regulatory regulations and compliance frameworks like HIPAA (Moubarak et al., 2020).

Additionally, issues with data privacy and confidentiality are among the limitations when integrating blockchain technologies in healthcare sector. Although blockchain technology provides immutability and transparency, there are issues with data privacy and confidentiality as well particularly in regard to private medical information (Iyengar-Emens, 2018). Public blockchains may not be appropriate for storing medical data that need to be kept confidential and subject to stringent access controls since they keep data on a decentralized network that is accessible to all users. Integration complexity and interoperability when integrating blockchain technology in healthcare sector. It can be difficult and complex to integrate blockchain-based medical systems with legacy systems and the current information technology architecture. Interoperability protocols, safe data exchange methods, and defined data formats are necessary to achieve interoperability between blockchain networks and conventional databases or Electronic Medical Record (EMR) systems (Moubarak et al., 2020).

In Summary, firewall can be used as a middleware to provide critical component of the distributed network security. It allows different medical information systems (MIS) to

share and access data across different geographical locations (Guclu et al., 2020). However, due to the limitations provided earlier it inhibits smooth communication and occasions different middleware making interoperability impossible (Zhang et al., 2018). Consequently, other technologies such as use of web services in which communication rides on use of hypertext transfer protocol (HTTP) and can bypass firewall to enable smooth interpretability has been adopted in e-commerce, but not in health sector due to the security challenges it raises (Gomathy, 2021). Other web systems use XML and JSON as marshalling technology for packaging parameters in a technology neutral format (Lv et al., 2019). Marshalling is used to create various remote procedure call (RPC) protocols, where separate processes and threads often have distinct data formats, necessitating marshalling between them (Clunie, 2021).

Medical databases can be either centralized or distributed. A distributed database system allots a single logical database to two or more physical databases, or host data in multiple locations. Notably, providing data security in a distributed database remains an open challenge. This is so because distributed database needs to be secured, while at the same time maintaining access control. Additionally, independent distributed database systems lack universal communication standards (protocols) at the database level. Although transmission control protocol and Internet protocol (TCP/IP) is the de facto standard at the network level, there is no standard at the software application level (Prince, 2021). TCP/IP (Transmission Control Protocol/Internet Protocol) protocols are designed to handle communication at the network and transport layers, they do not directly address the specific requirements or complexities of applications. This means that different database vendors employ different data formats, communication standards and protocols that are often incompatible with different information systems. To alleviate this, there is

need for mechanisms to manage the distribution and processing of data in a distributed database management systems (DDBMS) environment (Prince, 2021).

Other protocols that have been applied in designing medical systems includes HTTP/HTTPS (Hypertext Transfer Protocol/Secure) which are applied at application layer and used for transferring data over the World Wide Web (Zhou et al., 2018). The two are widely used in medical systems for accessing web-based resources, such as electronic medical records (EMRs), medical portals, and online healthcare services. FTP/SFTP (File Transfer Protocol/Secure File Transfer Protocol) are protocols used for transferring files over a network (AIRA), 2020). They are commonly used in medical systems for sharing large files, such as medical images, documents, and data backups, securely between healthcare organizations and systems (Das & Port, 2018).

SMTP/IMAP/POP3 (Simple Mail Transfer Protocol/Internet Message Access Protocol/Post Office Protocol), these email protocols are used for sending, receiving, and accessing email messages over the Internet. They are utilized in medical systems for electronic communication between healthcare providers, patients, and other healthcare stakeholders. LDAP (Lightweight Directory Access Protocol), which is a protocol used for accessing and maintaining directory services, such as user authentication, authorization, and access control. It is commonly used in medical systems for managing user identities, credentials, and access rights across multiple applications and systems (HelpSystems, 2020). This implies that there are different protocols that are supporting different functions medical systems but none is geared towards standardization of medical systems architectures that could be applied by different medical systems vendors.

On the other hand, medical systems software developers develop medical systems based vast policies and standards that includes the global data protection regulation (GDPR),

Kenyan Data Protection Act of 2019, Health Insurance Portable and Accountable Act of 1996 (HIPAA), HL7 (Health Level Seven), DICOM (Digital Imaging and Communications in Medicine), FHIR (Fast Healthcare Interoperability Resources) (Clunie, 2021), SNOMED CT (Systematized Nomenclature of Medicine - Clinical Terms) (Torab-Miandoab et al., 2023), CCDA (Consolidated Clinical Document Architecture), OAuth (Open Authorization) and OpenID Connect, XDS (Cross-Enterprise Document Sharing)(Persons et al., 2020), SMART on FHIR SMART (Substitutable Medical Applications, Reusable Technologies) and NCPDP (National Council for Prescription Drug Programs) (Torab-Miandoab et al., 2023).

The infrastructure connecting all the nodes or devices in a distributed database system also needs to be secured to guarantee security of systems. A node in a distributed ledger is a single computer that is part of the distributed ledger network. Additionally, data integrity in the distributed database system is often compromised (Hegde & Maddikunta, 2023) because it allows for data redundancy in the database as it is stored at multiple locations (Ezéchiél et al., 2019). To address these limitations, a potential solution is the use of distributed ledger technology (DLT) based systems.

Distributed ledger is a broad term used to refer to a method of processing and storing data in a network consisting of multiple nodes. Its main aim is to eliminate the need for a central node, which enhances control of data processing in a network, and establishes trust in a trustless environment (Olsson, 2020). DLT does not require a central authority or intermediary to process, confirm, or authenticate transactions or other types of data transfers. All participants in the distributed ledger can see these records based on a common identifier, as they simply require a timestamp and a cryptographic signature for authentication. Therefore, DLT method provides an auditable and verifiable record of all information stored in the given dataset. In a trustless environment, opportunities to give a

strong support for data integrity, resilience, authenticity, decentralization, anonymity, autonomy, and provenance in various fields have arisen as a result of DLT's structural capacities (Chowdhury et al., 2019).

Subsequently, there are multiple architectural ways of implementing DLTs including, but not limited to Blockchains, Directed Acyclic Graphs (DAGs), Hashgraphs, Holochain and Tempo (Radix) using Cerberus consensus framework (Leonulous, 2020). However, most DLTs are siloed towards specific application platforms, and hence the increased need for interaction and sharing of data across different software application platforms.

Since the first release of Bitcoin crypto-currencies as a decentralized electronic cash system based on a peer-to-peer network (Nakamoto, 2018), blockchain has been the most widely utilized DLT. Bitcoin transactions are grouped together into "blocks" by the corresponding algorithms, and new blocks are added to the blockchain by signing them cryptographically (Gupta & Sadoghi, 2019). By solving a new cryptographic challenge, anyone can add a block of transactions to the Bitcoin ledger. This decentralized and 'permission less' design allows for the maximum possible transparency and efficiency. The system's primary objective is to supply a means to ensure Proof-of-Work and proof-of-stake, with the accompanying reward for each solution serving as an added incentive (Vujičić et al., 2018).

However, whereas this has worked well within the financial sector, it is marred with a number of challenges in health sector. First, the intensive processing power required to mine coins has not only been criticized due to its associated costs, but also leads to enormous carbon emissions (Andoni et al., 2019). Secondly, not all applications require consensus algorithms to add blocks to the chain but rather a mechanism to ensure secure interoperability. In addition, some application areas are crucial to human life than the allied reward of mining. Consequently, the choice of a particular consensus algorithm

has a considerable effect on the network speed, throughput, scalability, and transaction costs (Durneva et al., 2020).

There are several types of consensus algorithms that are applied to commit a distributed transaction to a database commonly used to synchronize data across a decentralized network (Yaga et al., 2018). Additionally, the algorithms are used to ensure data consistency and transparency of all transactions. The consensus algorithms are used to assign a node the status of leader (Frikha et al., 2021). Blockchain which is a distributed ledger depends on cryptography techniques and consensus mechanisms along with other algorithms for establishing strong security (Albarki et al., 2019). The consensus algorithms of blockchain are proof of work (POW), proof of stake (POS), delegated proof of stake (dPoS), proof of activity (PoA), ripple protocol consensus algorithm (RPCA), proof of capacity (PoC), delegated proof of stake (dPOS), proof of elapsed time (PoET), stellar consensus protocol (SCP), byzantine fault tolerance (BFT), practical byzantine fault tolerance (PBFT), delegated byzantine fault tolerance (dBFT), proof of identity (PoI) and proof of importance (POI) (Krishnamurthi & Shree, 2021).

All these consensus algorithms work well with financial systems in the finance sector due to the reward system and mining. While these consensus algorithms are applicable in the financial sector, in medical sector, they are faced by various challenges since there is no reward and financial gain when dealing with medical systems. Further, due to the mutating architectural designs, non-standardized data formats and varying protocols, Blockchains suffer from interoperability issues. This impedes the user's ability to see and access information across distributed ledger systems and the existing medical enterprise system (Belchior et al., 2020). These challenges, perhaps, call for development of a framework to address the interoperability issues.

Some of the interoperability frameworks that have been proposed include the Standards and Interoperability (S&I) Framework within the Office of the National Coordinator for Health Information Technology (ONC), (2019) was formed to orchestrate input from the public and private sectors to create harmonized health information technology specifications for use throughout the United States. In Kenya, the Kenya Health Information Systems Interoperability Framework (KHISIF) (MoH Kenya, 2020) that aims at supporting the ministry of health strategy of providing patient-centric health service has been proposed. This framework is still at the infant and proposal stages and it has not yet been actualized.

There are a number of interoperability tiers that can be used to implement DLTs, including structural, semantic, organizational, and logical. Level one interoperability, often known as "foundational interoperability," is in charge of defining the prerequisites for a given system or application to securely exchange data with another. Level two structural interoperability specifies the standards used to format messages transmitted from one system to another (da Conceição et al., 2018), and defines the formats, syntax, and arrangement of the data transferred. This is crucial to the readers since it enables them to grasp the point of the data. The third level of interoperability, called "semantic," describes the exchange of information across systems. Data elements and the system user may easily understand and interpret data because of the level of interoperability (Yang et al., 2022). The fourth level, organizational interoperability, encompasses the governance, policy, social, legal, and the organizational concerns required to ensure that data is shared and used in a way that is both private and timely (Bokolo, 2022). These parts allow for mutual agreement, trust, and unified user-facing procedures and processes.

The two major facets of medical systems interoperability occur at the levels of structural and semantic levels, each of which is necessary for the successful exchange of medical

data (da Conceição et al., 2018). Since medical data is complex, and its heterogeneous structures decrease the effectiveness of analysis and reduces understandability, the structural interoperability level is of big concern. Interestingly, these standards lack either the structural or the semantic interoperability aspect due to the dynamism of the independent systems. While they are effective in their own front, there is no standardized approach of achieving medical systems interoperability across the structural and semantic interoperability levels, mainly because aligning data encoded formats and protocols with disparate standards is a non-trivial task for the medical systems software developers (Soule, 2020). To overcome this challenge, several industry-wide standards have been advanced (McGhin et al., 2019), which include Fast Healthcare Interoperability Resources (FHIR) and Health Level Seven (HL7). This remains an open problem and the need for medical systems interoperability increases as the systems are developed constantly.

It is crucial to accurately codify healthcare data in order to make sense of it. In order for this to work, the healthcare industry needs to adopt the same codification methods, often known as controlled terminology (Yang et al., 2022). While it may be impractical to expect medical systems to adopt a unified vocabulary, narrowing the focus of vocabularies to cover a specific topic may prove to be a workable alternative. Together, structural models and these subsets, known as value sets, can limit the possible encodings of attributes and attribute types. FHIR, an HL7 standard, and related frameworks such as the European eHealth Interoperability Framework (EIF) and the Refined eHealth EIF (ReEIF) have been developed in an effort to achieve these goals (Braunstein, 2018).

Based on the foregoing context of the medical systems interoperability frameworks, architectural layouts of the medical systems pose a big challenge to medical data sharing.

Structural interoperability arises from the issue of standardizing syntax, data formats and protocols that can be universally used to link all medical systems and enable secure data exchange across the medical systems. Semantic interoperability requires usage of common models and codification of the medical data using data elements with standardized definitions and meanings. It is also worth noting that all interoperability frameworks operate in isolation and using a centralized database with varying structural and semantic formats.

The current frameworks for medical interoperability face a deficiency in different levels of interoperability. These challenges range from structural interoperability level challenges concerning data syntax and the standardization of data formats and protocols. Structural interoperability becomes a challenge in the context of standardizing syntax, data formats, and protocols that can be universally applied to connect various medical systems, facilitating secure data exchange among them. Another challenge is achieving semantic interoperability which involves adopting common models and codifying medical data, utilizing data elements with standardized definitions and meanings. To address these challenges, an enhanced secure distributed ledger interoperability framework that is capable of achieving interoperability of medical systems has been developed. The framework was developed and validated using the proof-of-concept prototype to show interoperability of medical systems.

1.3 The Statement of the Problem

The increasing adoption of electronic medical record (EMR) systems, especially in developing countries is not only encouraging but also presents a huge potential to improving quality of diagnosis as well as patient care and safety. Besides providing an efficient and effective mechanism of workflow processes within a health organization, leveraging on the historical data of a patient would greatly enhance the diagnosis and

prognosis of various medical conditions. However, the common practice among vendors is to develop EMR systems that conform only to their defined data formats. Consequently, the data generated and stored in their EMR systems remain isolated and is often exposed to data leaks and security threats. Additionally, these systems have varying structural models, data formats and semantic structures, thus becoming non-interoperable. To overcome this, interoperability of medical systems has been presented as key to the essential need for secure exchange of critical electronic medical records. This could not only aid in consolidating patients' medical historical records and resolving the challenges of fragmentation of data records, but also can go a long way in leveraging the vast amounts of data gathered to conduct research, analyze trends and improve patients' safety.

In this endeavor, some medical interoperability standards and frameworks such as European eHealth Interoperability Framework (EIF) and Refined eHealth EIF (ReEIF) have been developed. However, these frameworks suffer structural interoperability issues in dealing with data syntaxes and the standardization of data formats and protocols. This drawback prompted the development of Fast Healthcare Interoperability Resource (FHIR). Whereas FHIR was able to overcome the challenges of its predecessor interoperability frameworks by providing a fairly acceptable standardized structural format, FHIR focuses on the legacy systems data exchange without the consent of the patients which could further lead to data leaks. The exchange of data is expedited in plaintext that exposes it to security threats such as the man-in-the-middle attack. Additionally, it is faced with numerous technical barriers, including; lack of a common secure mechanism to ensure appropriate patients' privacy, inability to bridge patient identity across systems, lack of endpoint locator authentication and detection, as well as

the use of different FHIR versions for the record of a single patient. Further, secure interoperability between medical systems across various levels remains an open problem.

To address these challenges, the study developed an enhanced secure distributed ledger interoperability framework for medical systems that uses a Proof-of-Authentication algorithm as the consensus mechanism. Unlike what most DLTs use as a reward mechanism in their consensus algorithms, there would be no motivation in medical systems. The developed framework provides a mechanism to securely exchange patients' medical data among multiple nodes and grants patient the authority to allow their historical medical data access and usage.

1.4 Objectives of the Study

1.4.1 General Objective of the Study

To develop an enhanced secure distributed ledger interoperability framework for medical systems.

1.4.2 Specific Objectives of the Study

- i. To establish the factors affecting secure interoperability of medical systems
- ii. To design an algorithm to enhance security of DL interoperability framework for medical systems
- iii. To develop a secure DL interoperability framework for improving the security of medical data exchange between medical systems
- iv. To validate the developed secure distributed ledger interoperability framework for secure medical data exchange.

1.5 Research Questions

- i. What are the factors affecting security of medical systems at all levels of interoperability?
- ii. What is the algorithm for secure DL interoperability framework that enhances security of medical systems?
- iii. What are the features of the developed secure DL interoperability framework developed to improve security of medical data exchange between medical systems?
- iv. How will the developed secure DL interoperability framework be validated for secure medical data exchange?

1.6 Justification of the Study

The use of electronic medical records (EMRs) by both private and public health hospitals, and the quest for universal health coverage has been on the rise. The need to securely reference and share patients' medical records among health practitioners across health institutions before a patient's diagnosis is fundamental. Enhanced secure distributed ledger interoperability framework is therefore necessary. The actors in the health system prototype include doctors and other healthcare providers like the medical laboratory technologists and the pharmacists, who are authorized to use the system to update the patients' electronic medical records. The primary users of the enhanced secure interoperable medical systems are the patients. The patients have the sole ability of authorizing access to their electronic medical records. The key actors of the enhanced secure interoperable medical systems are medical facilities like hospitals and healthcare institutions, since they are hosting and networking the medical systems, the doctors and other health practitioners, and the databases storing the electronic medical records.

Some of the benefits that derive from the developed enhanced secure DL interoperability framework for medical systems include reduction in medical cost as patients need not repeat clinical lab tests at different healthcare institutions since their electronic health records and information is readily available for reference upon need, as well as effective and informed diagnosis decisions by the health practitioners. Besides reducing waiting time and improving healthcare service delivery, enhanced secure DL interoperability framework architectural design will also heighten real time access to secure EMRs regardless of the location of healthcare institution that the patient is seeking healthcare services.

During emergency referral process, enhanced secure DL interoperability framework will help doctors to securely reference the historical EMRs from the referring hospital, hence reducing the time taken in providing medical services and saving life. The enhanced secure DL interoperability framework allows secure logging in via the access control measures, which aim to authenticate the authorized medical service providers when accessing the patients historical EMRs through use of approved logging in credentials, their public key and private key. The enhanced secure DL interoperability framework supports encryption and hashing of EMRs; hence confidentiality and integrity is achieved.

1.7 Significance of the Study

Patients 'medical history data is private and proprietary stored in different medical systems in different hospitals managed by different people. However, security of these medical records depends on the integrity of the users of the systems. Patients and their families will benefit from this research results since it takes into account their wants and concerns because they are directly touched by healthcare decisions and outcomes. On the other hand, doctors need to reference patient's medical history data when making their

diagnosis and prescriptions, hence the need to access their electronic medical data in a secure platform that is confidential, secure and immutable so as to facilitate decision making and avoid misdiagnosis.

Healthcare providers group comprises physicians, nurses, and other medical specialists who provide treatment and might also be involved in putting this study results into practice. Healthcare providers can share the patient's data with other authorized healthcare givers with the consent of the patient through the use of enhanced secure distributed ledger interoperable platform that uses a unique universal patient identifier to aid in better health services without the worry of the architectural design at any interoperability levels. Healthcare institutions and organizations will apply the results of this research to aid them to improve patient outcomes, enhance the quality of care, and create novel therapies and technology, hospitals, clinics, research institutions, and pharmaceutical corporations.

Academic institutions that include students, instructors, and researchers will use the results in their training to improve science and prepare the next generation of healthcare professionals.

Health insurance companies will use this research results since it has impact on choices about coverage, rules for reimbursement, and methods for controlling medical expenses due to the linkage of healthcare institutions and hence enhance transparency of the medical processes. Community and advocacy groups will use the framework to push for research that targets their particular needs and objectives since they represent certain communities or health issues. Ethical review boards that are charged with making sure that research involving human subjects abides by moral standards and protects the welfare and rights of participants will also benefit since the results of the research provide details of how patients' data will be secured during transit and storage.

The government can use the results of this study to provide policy guidelines and standards that would regulate the access and sharing of patients EMRs, and further guarantee privacy of patients' medical records across different HISs platforms. Government agencies and policymakers charged with developing healthcare regulations, financing, and policies, will apply this research to help them make decisions on public health programs, budget allocation, and healthcare delivery.

Research gaps in the extant EMRs were useful in developing an enhanced secure interoperable distributed ledger framework for secure sharing of patients' data across different medical systems. The distributed ledger medical system prototype can be used by healthcare stakeholders to secure storage of electronic health records, improve referral processes and promote safe sharing of patients' medical records.

1.8 Scope of the Study

The study analyzed medical systems interoperability frameworks and reviewed their architectural designs in order to identify and address their structural inadequacies which hinder secure interoperability of medical systems. The study also aimed to achieve security and privacy of electronic medical records (EMRs) and enhance secure access and sharing of EMRs across health facilities using DLTs across geographical areas. The study population, which is also known as the accessible population, used as the actual sampling frame from which purposive sampling was used to sample the medical systems developers in Kenya.

The developed enhanced secure distributed ledger interoperability framework for medical systems adopted security-by-design and privacy-by-design approaches in its infrastructure. To achieve this, a high level conceptual architecture recommended by international telecommunication union (ITU) (ITU-T FG DLT, 2019), and which comprises of the application layer, service layer and core layer, was utilized. Distributed

ledger prototype was used to validate its architectural design. Free secondary data from medical data sets, medical reports and medical publications based on patients' medical data was used to generate the diagnostic data that was analyzed and used in the testing and validation of the developed prototype.

1.9 Limitations of the Study

This study was limited to interoperability architectural designs of electronic medical systems (EMRs). Medical cases were utilized to test the sharing and exchange of electronic medical records across medical systems using the developed framework. Further, the study was confined to prototype development of EMRs as opposed to full system development. Validation of the prototype was done using secondary medical data available in free medical data sets for anonymity. The study's methodology, data analysis, and result interpretation were subjected to a rigorous peer review process by impartial specialists in the field. In order to confirm results, validate assumptions, and offer insightful criticism on the planning and conduct of the study, expert input was also sought. To minimize the impact of the limitations to the outcome of the research, a strategic approach through use of a robust methodology, sampling techniques, data validation and triangulation to test for validity and reliability and use of statistical techniques was employed.

1.10 Assumptions of Study

In order to ensure the protection of patient data and privacy during storage and sharing across the medical systems, the enhanced secure DL interoperability framework for medical systems assumed that the medical system software developers will abide by healthcare regulations such as HIPAA, GDPR (General Data Protection Regulation), Kenyan Data Protection Act of 2019, and other international healthcare regulatory

standards. It also presupposes that all parties must adhere to strong security procedures in order to protect against security lapses, illegal access, and cyber-attacks, all of which are essential to preserving integrity, privacy and confidence in the healthcare system. The developed framework assumes that all involved medical systems will adhere to recognized interoperability standards (e.g., HL7 FHIR) to enable secure exchange of electronic medical records and information across different platforms and healthcare organizations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature related to this study. The reviewed literature is broken down into sections that describe the state of art of the medical systems, existing distributed ledger technologies, architectural frameworks of DLTs, opportunities and challenges of distributed ledgers in medical systems, and security and interoperability issues of the electronic medical systems. Theoretical framework and research gaps of in DLT interoperability frameworks for secure medical systems are also presented in this chapter.

2.2 Electronic Medical Systems

Medical System are constantly altering medical service delivery in the healthcare sector. These systems have been used to ease access to medical services, increase efficiency and to improve the health sector outcomes (Mishra et al., 2023). A continuous medical process is now supported by medical systems, which have evolved from a standalone software used only in primary care clinics. A wide range of healthcare providers and facilities use the pervasive computing healthcare environments made possible by recent technological developments (Hassan et al., 2017). The need to examine how medical systems share data in an interactive setting is clear. All pertinent patient medical data in a usable format can be readily available to healthcare practitioners whenever they need it (Thakur, 2022).

A major component of the medical system is the electronic medical record (EMR), which is used to store medical data in any given health facility. EMRs are digital forms of patients' medical records stored in an electronic database. EMRs store patients'

biodata, contact information, medical tests, test interpretations, diagnoses, treatment, patient's medical history, including allergies, medical laboratory test reports, treatment plans, doctor's appointments and recovering progress reports. These EMRs can exist in databases, cloud storage or centralized storage area for future retrieval (Chenthara et al., 2019). EMR systems are selected by healthcare facilities depending on a variety of factors, including available funds, patient volume, and capacity to train personnel. Interoperability is difficult since not all institutions utilize the same HIS. If two healthcare organizations employ non-interoperable networks, it may be a significant administrative burden to move electronic medical record information from one system to another in a secure manner. Therefore, medical professionals may have to wait for crucial patient health data or be unaware of the patient's treatment history at another hospital. The capacity to transmit information between medical systems using different EMR solutions is made possible through interoperability (Kritsas et al., 2020).

The safety and confidentiality of patients' personal health data records is an important issue in the medical industry even with the increasing need to achieve universal health coverage (Mitchell & Kan, 2019). Electronic medical records (EMRs) form an important part of the used healthcare-based systems, and it is vital that EMRs are kept safe. Electronic health records have a wide range of functionality which includes patients' data capture, use, storage, sharing and management. The health-related information stored in EMRs needs to be readily available and reliable to the authorized persons at the time when it is required so as to offer quality medical services to patients during the time of need (M. Kim et al., 2020).

Electronic health records or files must be digitally signed by the people who made them or contributed to them, and the people who could look at them must be named. Each record is retrieved at a later date and used for many purposes, including but not limited to

patient review, initial physician review, review by other physicians for further diagnosis and treatment, and judicial processes (Hegde & Maddikunta, 2023). Due of this, we need to take new precautions to stop accidental or deliberate destruction and alteration of medical data. Hospitals with varied supporting technology architecture and medical infrastructure is a major barrier to sharing patients' diagnostic data (Patel, 2019). Diagnostic information for patients is particularly difficult to share since it often necessitates either a centralized data source or the transmission of bulk diagnostic information to other institutions (Kim et al., 2020).

Implementation of secure architectures and technologies can improve access control mechanisms of medical systems so that only authorized users can access the data. Protected health data can be housed in databases and shared through encrypted channels and interoperable technologies. Systems built on distributed ledger technology, which provide both security and interoperability, can accomplish this.

2.3 Distributed Ledger Technologies

Distributed ledger unlike a traditional database is an electronic database that is shared, replicated, and synchronized among numerous locations, nations, or organizations in a consensual manner (Olsson, 2020). Unlike a traditional centralized database, a distributed ledger does not require a central administrator or manager hence does not have a single point of failure. It relies on a peer-to-peer (P2P) computer network architecture and consensus algorithms to ensure that the ledger is reliably replicated across distributed computer nodes. Each node in the distributed network independently processes data in the ledger update transactions and collectively uses consensus algorithms to determine the correct copy of the updated ledger to be saved for future reference (Lv et al., 2019). Once a consensus is reached, all nodes in the ledger update themselves with the latest and correct copy of the ledger. This decentralized architecture

allows for a system of record that goes beyond a simple database, enabling the formalization and securement of distributed ledgers. The lack of a central authority reduces the cost of trust and avoids single points of failure, enhancing security and reliability in data management and communication across distributed ledgers during data exchange.

2.3.1 Distributed Ledger Technologies Historical Perspective

Since ancient times, people have used paper ledgers to record financial transactions. As computers became more commonplace towards the end of the 20th century, paper ledgers were gradually replaced by digital versions that were largely identical to their paper predecessors. Historically, ledgers have needed a trusted third party to verify the accuracy of the transactions they record. Banks, for instance, must check the legitimacy of the monetary transactions they handle (Laurier et al., 2020). With the advent of cryptography, more sophisticated algorithms, and stronger and nearly ubiquitous processing power in the twenty-first century, the distributed ledger has emerged as a credible alternative to traditional record-keeping methods (Zhang & Jacobsen, 2018).

Roman Empire banking allowed citizens to take part in cross-regional transactions, which can be traced back to the earliest days of DLT. As the Roman Empire continued to experiment with distributed ledger, improvements in updating and recording transactions were made using paper checks (Suciu et al., 2018).

According to the Hong Kong Monetary Authority, (Hong Kong Monetary Authority, 2016) DLT is one of the most exciting developments in IT because of its potential to revolutionize economic, social, and industrial collaboration. As described by Rauchs et al. (2018), DLT is a digital system for recording transaction of assets in which the transactions and information thereof are stored in numerous locations simultaneously

(Singh et al., 2023). DLT can also be thought of as a distributed database or an information archive. Access to the database may be granted to the general public or be limited to a selected set of individuals (Natarajan et al., 2017) and (Tomić, 2021). Distributed ledgers are decentralized, and hence lack a centralized data store or centralized administration (Chowdhury et al., 2018). DLT implements a protocol for a trustworthy distributed digital database. Where distributed networks are used, there is no need for a governing body to ensure that manipulation is prevented. Public key encryption mixed with a one-way hash function provides an accessible and secure method that ensures information transfer without a central authority provider in DLT (Xu et al., 2019).

DLT use encryption to store data in an impenetrable and verifiable fashion. Cryptographic signatures and cryptographic keys are used in DLTs to ensure that only authorized users can access the data. Further, any changes made to a database using DLT are preserved permanently and cannot be erased. Hence, a distributed ledger is a database in which every node processes and validates every transaction, creating a record of each transaction and establishing consensus on its authenticity. Static data, like that found in a registry, can be recorded, as can dynamic data, such as financial transactions (Kannengießer et al., 2020).

Opportunities for the safe transfer of data between institutions have expanded thanks to the development of DLT, whose defining characteristics include robust support for data integrity, resiliency, authenticity, decentralization, anonymity, autonomy, and provenance.

A distributed ledger is designed to work without a trusted third party or a central server for processing, validating, or authenticating any transactions or other exchanges of data.

Only when these records have been time stamped and signed with a cryptographic key are they recorded in the ledger. The distributed ledger uses a personal identity for each user to ensure that every user has access to their own personal copy of the ledger. There are many applications of DLT in the world today. Blockchains, DAGs, Hashgraphs, Holochain, Tempo (Radix), and the Cerberus consensus framework (Leonulous, 2020) are all examples. The most well-known kind of DLT is blockchain, which records transactions in chronologically ordered blocks and distributes them throughout the network's nodes. Crypto currencies like bitcoin rely on it for their functionality (Nakamoto, 2008). When it comes to Internet of Things (IoT) ecosystems, DLTs like Tangle shine. The Tangle EE (Tangle Enterprise Edition) Working Group, founded by the Eclipse Foundation and the IOTA Foundation, defines Tangle as "a permission less, feeless, scalable distributed ledger, designed to support trustworthy data and value transfer between humans and machines." Corda, Ethereum, and Hyperledger Fabric are a few other examples of popular distributed ledger technology.

Blockchain and DLT are two words that are commonly used interchangeably. However, they are not interchangeable. Blockchain technology is used in some forms of distributed ledger technology, but this is not always the case. Both are employed in the development of cryptographically-secure distributed ledgers. Both produce time-stamped, immutable recordings (El Ioini & Pahl, 2018). Both are almost impossible to hack. Both can be public, where anybody can use them, as with bitcoin, or private, where access is granted only to those who have been granted permission and have agreed to the terms of service (Mikula& Jacobsen, 2018). Blockchain, in contrast, uses data blocks that are chained together to construct the distributed ledger, as the name implies (Zaman et al., 2021). A distributed ledger can be created with any number of different technologies, and DLT encompasses them all. A DLT does not require data to be organized in blocks.

By altering the foundations of how businesses acquire and share the data that goes into their ledgers, DLT can bring about substantial enhancements to record-keeping. To grasp this, think about the inherent flaw in both traditional paper and computerized ledgers: the need for an administrator to approve any changes before they are reflected in the system. Centralized control in such a system is extremely time-consuming and resource-intensive for companies. Furthermore, ledgers are not always complete or up to date due to centralized control. Every node that adds data to the ledger opens up the system to the possibility of fraud or errors (Chowdhury et al., 2018); hence, the process is not foolproof. Furthermore, no other contributors to the centralized ledger can effectively verify the veracity of data originating from any other contributors. However, DLT enables data sharing in real time, thus the ledger is always accurate. It also promotes openness, since all nodes in the network can observe the alteration (Natarajan et al., 2017).

Since there is no central point of failure or single target for hackers or manipulation, DLT is inherently more secure. Since there is no longer any need to involve a third party or central authority, DLT has the potential to drastically reduce the time it takes to complete a transaction. Likewise, transaction fees may be lowered with DLT. The performance of DLTs is proven to suffer in specific networking scenarios when compared to centralized ledgers (Antal et al., 2021). This is because executing the highly decentralized verification process and distributing copies of the ledger need large computer resources. Financial transactions have been the first focus of distributed ledger technology. That's understandable, considering how bitcoin became a globally recognized money, while simultaneously validating the viability of DLT. Financial institutions, such as banks, were among the first to experiment with DLTs. However, advocates of DLT argue that digital ledgers may serve a variety of purposes beyond the

financial sector. The government is investigating the possibility of using the technology to keep track of deed transfers and other types of transactions. Supply chain data maintenance is an area where several companies are now testing DLT. The legal industry is also exploring the potential of DLT for the processing and execution of legal documents. Those who advocate for the use of digital ledgers point out that DLTs may be used to keep better tabs on who owns what in the realms of art, commodities, music, cinema, and more (Tasatanattakool & Techapanupreeda, 2018).

In an effort to streamline the process of keeping patient records up-to-date, healthcare companies are testing with DLT. Experts believe DLT technology gives people more say over their personal information, such as patients' medical records, by letting them choose which parts of those records to share and for how long (Catalini, 2017). Despite the fact that DLT adoption is still in its infancy, the technology has already proven its ability to bring users a number of benefits, such as greater insight and transparency of data contributed to the ledger, reduced operational costs due to the lack of a centralized authority, faster transaction speeds due to the lack of a lag in updates to ledgers, greatly reduced risks of fraudulent activity, tampering, and manipulation, and improved dependability. The establishment of numerous checkpoints as opposed to a single gateway for sensitive data is another excellent opportunity brought about by distributed ledger technology. Patients have the option of granting or denying permission for others to view, share, or make changes to their personal health information (Randall et al., 2017). The confidentiality and reliability of patient data are thereby enhanced.

However, the introduction of DLT introduces points that can be used to verify transactions made to the records, leading to more reliable, secure, and interoperable transactions protecting patients' medical information stored in hospital databases and medical systems. The confidentiality of patients' medical records can be strengthened by

the use of encryption when stored in databases. The patient and the doctor have each a public key that is shared, and each is required to keep their own private key in order to accomplish this encryption. When a doctor retires, he or she has the option of transferring ownership of his or her medical reports to another doctor or the system itself (Dubovitskaya et al., 2018). It is not the first choice for patients, but it is the best alternative. After that, a wide variety of alternatives become possible. DLTs are also considered to be a part of the "internet of value," where financial transactions can take place instantly over international networks. The widespread availability of the internet is crucial to the existence of digital ledger technology.

2.3.2 Security in Distributed Ledger Technology

Security in distributed ledger technology is designed to be achieved by having multiple copies of digital records and transactions being stored in all computers termed as nodes throughout the network. The data stored in the ledger is immutable, hence it cannot be changed but new data can be updated into the ledger (Natarajan et al., 2017). The transaction records data is hashed, copied and distributed throughout the network, making it hard for hackers to compromise its security. Any attempt to hack and compromise the records results into high cost in terms of time and other resources. Hence, the security of DLTs is thought to be assured since there is no single point of access and thus no single point of failure in the information (Mitchell & Kan, 2019).

2.3.3 Algorithms used in Distributed Ledger

Distributed ledgers like blockchain use consensus algorithms to validate the right participants in the transaction process and to determine who has the right to add the blocks or nodes. Consensus algorithms are critical components of blockchain networks because they preserve the integrity and security of these distributed computing systems

(Olsson, 2020). Proof of Work (PoW) is one of the consensus techniques used by blockchain, and it's how a miner is chosen to create the next block after solving a mathematical puzzle (finding a cryptographic hash of that block). This consensus algorithm is faced by some challenges which includes waste of resources and a very high level of energy consumptions hence making it unsuitable for medical systems applications. (Le Nguyen, 2018). Proof of stake (POS) relies on hardware and software resources rather than solving the mathematical puzzle it rewards the participants based on number of tokens they have, hence the miner who owns more gets more control over the consensus mechanism, this can result to network related attacks (Sriman et al., 2021).

The Ripple protocol consensus algorithm (RPCA) makes use of the fact that many networks nowadays consist of separate, poorly connected sub-networks. Each node uses it every few seconds to ensure the network is consistent and proper, this algorithm relies on the synchrony timing assumption. The Ripple Protocol Consensus Algorithm (RPCA) functions by utilizing frequent voting rounds to determine which transactions are to be added to the distributed ledger. (Facundo et al., 2017).

This consensus algorithm, known as delegated proof of stake (dPOS), is based on a voting system in which "delegates" select their preferred validator to aid in establishing and maintaining the blockchain network's consensus state for new blocks and transactions in exchange for a share of the transaction fees generated by these actions. Each delegate has a vote worth a certain percentage of their total blockchain holdings (Krishnamurthi & Shree, 2021). Proof of Elapsed Time (PoET) uses a fair lottery system that is based on the computing challenge of random leader election, commonly used in hyper ledgers, where the participants rely on randomized timer system for network participants rather than using mining hardware in the network after waiting for a randomly chosen time (Chen et al., 2017). Proof of Authority (PoA) is a consensus

algorithm based on reputation of trusted parties participating in the blockchain network. Validators stake their own identities and reputation instead of their resources. It works well for private blockchains (Manolache et al., 2021). The Stellar consensus protocol (SCP), which is also known as federated Byzantine agreement (FBA), is a consensus process that achieves robustness via quorum slicing, in which the trust judgments of individual nodes add together to determine quorums at the system level. These Blocks are the glue that holds the blockchain together (Suciu et al., 2018).

Byzantine fault tolerance (BFT), practical byzantine fault tolerance (PBFT) and delegated byzantine fault tolerance (dBFT) are consensus algorithms based on the idea used to fix the problem of unreliable nodes in the blockchain network, hence making it possible for BFT system to operate even when nodes act maliciously or fail. It is able to tolerate byzantine faults (Zheng & Feng, 2021). In proof of capacity (PoC), the miners, beforehand, create a list of all possible hash in the scheme process and store these hashes in the hard drive. This can be seen to imply that the more the storage capacity a miner has, the more chances they stand and the more possibility of finding solutions of correct hash combinations, hence increasing their chances to win the rewards (Azbeq et al., 2021). Proof of identity (PoI) consensus algorithm is attached to cryptographic confirmation of authorized identity using the user's private key.

This means that a block of data can be created and managed by each identified user in a network and presented to others (Krishnamohan, 2022). Proof of activity (PoA) in this consensus algorithm enable the miners solve cryptographic problem as soon as possible using electric energy and hardware. But, when one comes across a given set of blocks in the network, the only information known to them is about the identity and reward transaction of the winner (Belfer et al., 2020). Proof of importance (POI) consensus algorithms uses a decision-making process for a group where the individual participants

of the group construct and support the decision that works best for all the members. It models a win-win model for the network since the consensus only agrees to what benefits the majority members by voting for what is beneficial for all participants in the network (Siham & Alyaseen, 2019).

A summary of the consensus algorithms used in distributed ledgers showing the functionalities; advantages and limitations are shown in Table 1.

Table 1

Summary of the Consensus Algorithms used in Distributed Ledgers

DLT Algorithms	Functionalities	Advantages	Limitations
Proof of Work (PoW)	Based on solving mathematical puzzle which is the cryptographic hash of the block	Provides high level of security, allows for decentralized transaction verification and Miners are incentivized to participate	Computational power, leading to high energy consumption and environmental concerns.
Proof of Stake	Relies on hardware and software resources based on the number of tokens the miner owns	Energy efficiency, high scalability and decentralization	Nothing at stake problem, high stake requirement and vulnerability to 51% attacks
Ripple Protocol Consensus Algorithm (RPCA)	Uses series of voting rounds and agreement that validates transaction.	Fast transaction finality, energy efficiency, high scalability, reliability, reduced costs and byzantine fault tolerance:	Hardware dependency, trust in validators, validator selection criteria and the network partitioning process.
delegated proof of stake (dPOS),	Users stake their tokens and vote for delegates.	Reputational-based, fast to reach consensus, enhances voting power, highly scalable and minimal hardware is required	Malicious token holders, lower decentralization and engagement requirement required

Proof of Elapsed Time (PoET)	Uses a trusted execution environment (TEE) to randomly select a leader to create new blocks in the network. Each node generates a random wait time and sleeps for that duration.	Energy efficiency, decentralization, security since nothing is at stake and high scalability	Reliance on TEE, centralization concerns and hardware requirements
Proof of Authority (PoA)	Reputation-based consensus mechanism that relies on validators' identities.	High efficiency, fast speed, high security and allows for efficient governance.	Less decentralized, not suitable for public networks, predictability is high hence compromising security and susceptibility to corruption.
Stellar consensus protocol (SCP), also known as federated Byzantine agreement (FBA)	Uses quorum slices to achieve consensus then consensus is achieved through federated voting among quorums.	Allows open membership, provides decentralized control and has lower barriers to entry.	Reliance on quorum slices, potential for sybil attacks and its process and quorum slices add complexity to the consensus mechanism compared to other approaches.
Byzantine fault tolerance (BFT), practical byzantine fault tolerance (PBFT) and delegated byzantine fault tolerance (dBFT)	Nodes go through a three-phase protocol (pre-prepare, prepare, commit) to reach agreement on the order of requests. In dBFT, a set of nodes called bookkeepers are elected to validate transactions	BFT provides a way to achieve consensus in the presence of malicious nodes. PBFT is efficient and can handle a large number of requests. dBFT is more efficient than PBFT as it has a smaller number of nodes involved in consensus. dBFT allows for open membership as nodes can vote for	BFT requires at least $3f+1$ nodes to tolerate f faulty nodes. PBFT assumes a fixed set of nodes and may not be suitable for open membership networks. dBFT relies on a set of elected bookkeepers and vulnerable to Sybil attacks.

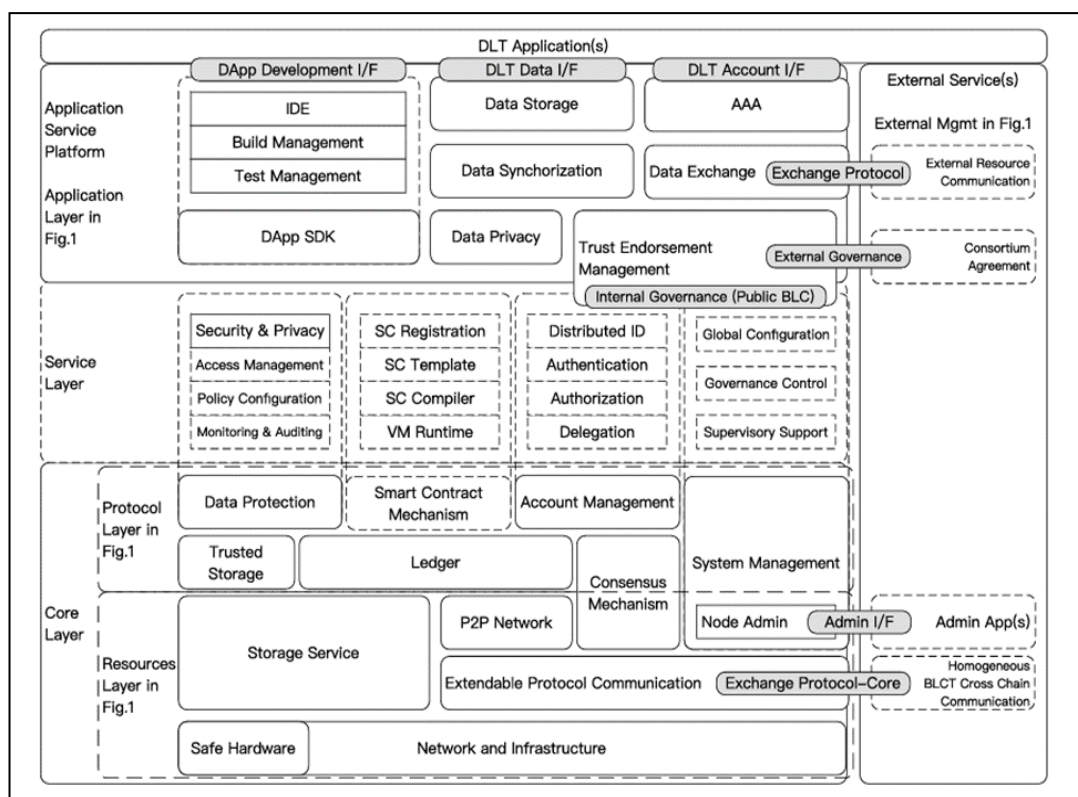
Proof of capacity (PoC)	Burstcoin's mining technique, which uses hard drive space for mining	bookkeepers More energy-efficient, faster block production and highly decentralized	Requires specialized hardware like ASICs for effective mining process and susceptibility to malware.
Proof of identity (PoI)	Based on cryptographic confirmation of authorized identity using the user's private key.	Identity verification that enhances network security and trust. More efficient. Promotes accountability among network participants, reducing the risk of malicious activities.	Centralization Concerns, identity verification challenges and scalability challenges.
Proof of activity (PoA)	Blends the mechanisms of proof of stake (PoS) and proof of work (PoW). Phase 1: Proof of Work mining is used by PoA, miners do complex mathematical computations to prove their efforts and sincerity to the network. Phase2: PoS, where a group of validators is randomly selected to validate the block.	Enhanced security, more energy efficient and resilience to attacks.	Requires high computational power for solving mathematical puzzles, which leads to energy consumption and more hardware requirements. Lacks a solution to prevent double signing by validators, posing a security risk.
Proof of importance (POI)	Models a win-win model for the network since the consensus only agrees to what benefits the majority members by voting for what is beneficial for all participants in the network	Takes a more holistic approach for holistic evaluation of node contributions, helps mitigate the centralization risks and dynamic importance score that promotes active participation in the network.	Complex scoring criteria and Network activity dependency challenges

2.3.4 Distributed Ledger Platforms Functional Components

According to the United Nations organization for telecommunications and information (ITU) (ITU-T FG DLT, 2019), distributed ledger platforms share a similar architecture at a high level but have distinct details. Figure 2 illustrates the high-level conceptual architecture of DLTs.

Figure 2

High-level Conceptual Architecture of DLTs



Source: ITU-T FG DLT, (2019)

2.4 Distributed Ledger Technologies Architectural Frameworks

DLT is the set of tools and protocols that underpin distributed ledgers and make it possible for multiple users to access, validate, and update the same set of data in real time. The system is based on a computer network that spans many organizations and physical places. Data stored in a distributed ledger is protected from unauthorized access

using cryptography in the form of cryptographic signatures and keys. Data entered into the system cannot be altered after it has been saved, and any changes made to the database are also kept for all time (Ballandies et al., 2018).

Bitcoin, the first crypto currency to be powered by Blockchain technology, was released in 2009, sparking widespread interest in the emerging field of DLT (Chowdhury et al., 2019). Since then, businesses in a wide range of sectors have been exploring DLTs in an effort to streamline service delivery and internal operations. The early sectors that adapted use of DLTs include the financial, supply chain management, pharmaceutical and health industries (Laroiya et al., 2020).

A distributed ledger is an idea that has been around for a while. Businesses have been collecting and storing data in disparate formats (paper, siloed software) for a long time; occasionally, bringing it all together. Different divisions in a company may keep their own records and only share them with the master ledger when absolutely necessary. Similarly, when multiple entities work together, they often keep their own records, and only report to a centralized ledger overseen by an authorized person when required to do so or when requested to do so (Zhang & Jacobsen, 2018).

2.4.1 Difference between DLTs and Centralized Ledger

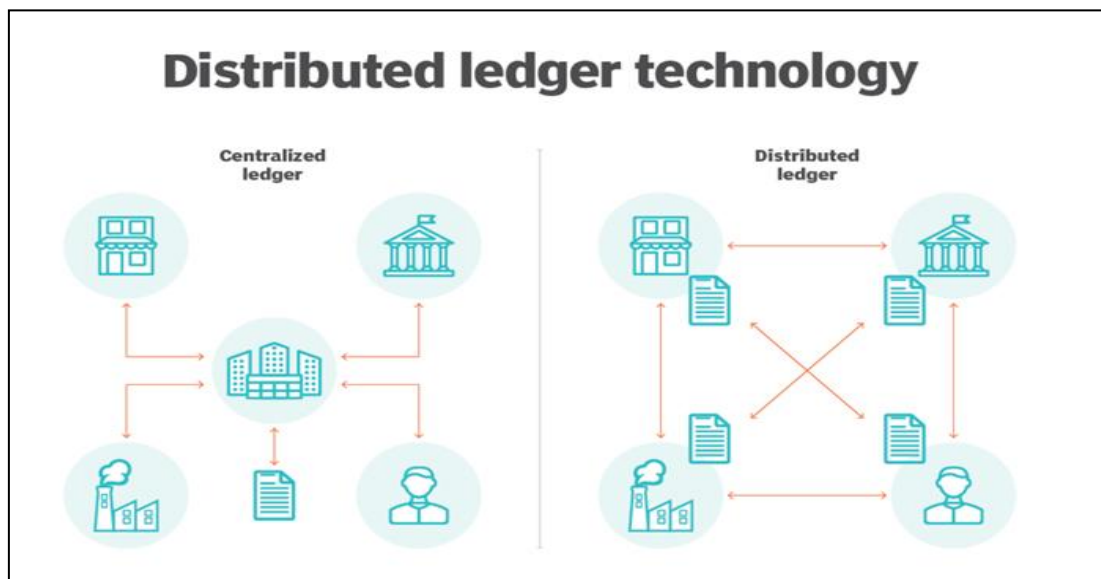
By shifting record-keeping from a centralized, authoritative location to a decentralized system where all pertinent entities can read and amend the ledger, the DLT architecture marks a substantial change in how information is acquired and conveyed. As a result, everyone can see who is accessing the ledger and making changes. Since all transactions are visible to all users, DLT fosters a culture of trust among its users and effectively prevents the possibility of fraudulent acts within the ledger (ITU-T, 2019). This means that entities utilizing the ledger no longer have to rely on the central authority controlling

the ledger, or a third-party supplier to fulfill this duty and provide a check against manipulation because DLT eliminates the need for either. (Bhartiya & Mehrotra, 2013).

Figure 3 below shows the architectural design difference between centralized ledger and distributed ledger and Table 1 gives a summary of the differences.

Figure 3

Difference between DLTs and Centralized Ledger



Source: Troy, (2021)

A summary of the differences between the distributed ledger and centralized ledger is as shown in Table 2.

Table 2

A summary of the differences between the Distributed Ledger and Centralized Ledger

S. No.	Distributed Ledgers	Centralized Ledgers
1.	Decentralized Architecture: In a DLT network, data is shared, replicated and synchronized across various nodes.	Centralized Architecture: Data is kept in a single and central database that is administered by a single entity in an organization.
2.	Multiple Validators: A number of separate, autonomous network members, or nodes, validate transactions.	Single Validator: A single, central authority or a small group of reliable and trusted entities in the organizations validates transactions.
3.	No Single Point of Control: This promotes transparency and lowers the risks and possibility of centralized corruption or failure because no one entity has total control over the entire ledger.	Single Point of Control: The ledger is completely under the control of one person or entity, which might speed up decision-making but increases the possibility of centralized corruption or poses a higher risk of system failure.
4.	Immutability: A DLT's transactions are unchangeable and inerasable, guaranteeing the integrity of the data.	Immutability: Centralized ledger transactions are subject to alter at any time.
5.	Permission: Usually not necessary to obtain authorization in order to view and alter the ledger.	Permission: Needs authorization in order to access and alter the ledger.

2.4.2 Existing DLTs Architectural Overview

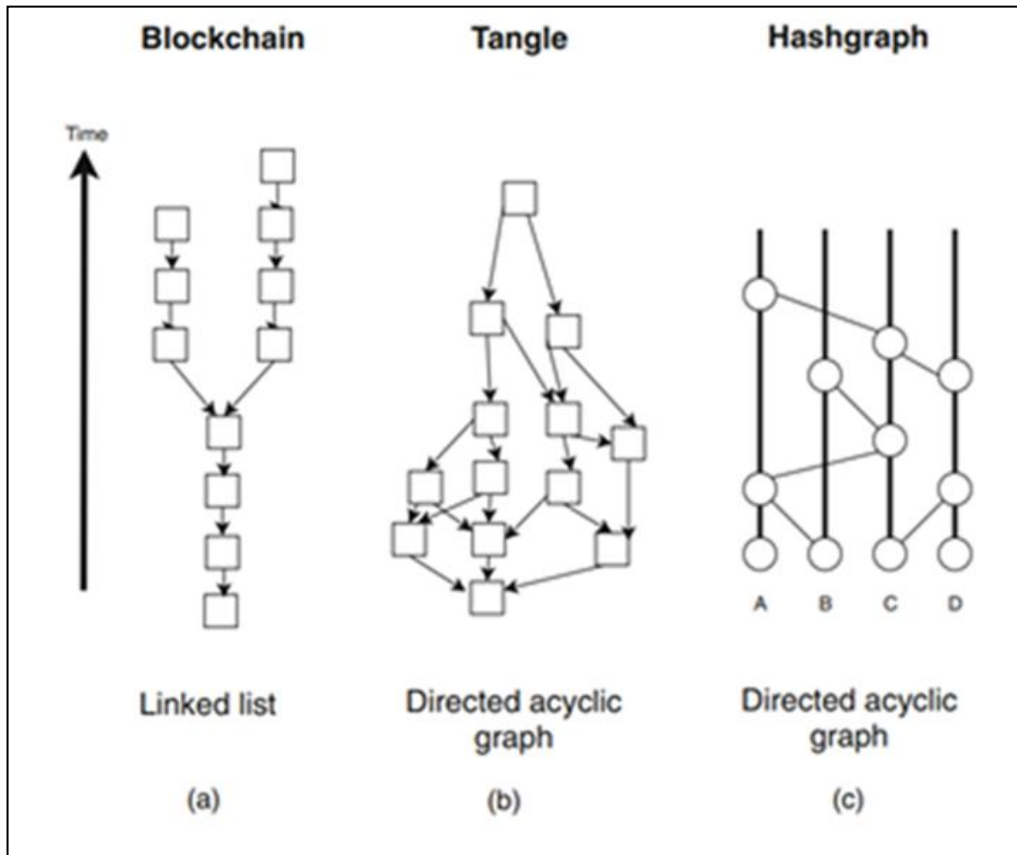
DLTs were designed with the aim of allowing users who do not necessarily trust each other or have some degree of mistrust between the participating parties to interact without the need of a trusted third party. DLTs bring transparency, traceability, and security to an otherwise untrustworthy setting through their underlying architecture.

Distributed ledger technologies (DLTs) are fundamentally data structures and sets of operations designed to record and verify transactions. While each DLT has its own unique data model and technology, they are all built on the same foundation of three well-known technologies, namely: (i) public key cryptography, (ii) distributed peer-to-peer networks, and (iii) consensus processes. In order to function in an unsecured setting, public key cryptography is employed to give each user a unique and secret online id. To add transactions to the Distributed Ledger (DL), each user is provided with two keys, namely, a public and a private one. This digital id is used to prove ownership of DL-managed items and enforce access permissions. Peer-to-peer networking is used so that the network can grow without a central point of failure, and so that no one player or group of players can dominate the system.

The P2P architecture addresses the data insecurity issue by incorporating encryption mechanisms to protect data in transit and at rest within the peer-to-peer network. It also implements authentication, access control and authorization mechanisms to authenticate participants and enforce access control policies and authorization mechanisms to restrict unauthorized access to sensitive data and resources within the P2P network. The P2P architecture utilizes role-based access control (RBAC), access tokens, or cryptographic keys to control access permissions and ensure that only authorized peers within the network can access or modify data (Antal et al., 2021). In a DL, a consensus mechanism enables all nodes to reach agreement on a single truth statement without resorting to a central authority (El Ioini & Pahl, 2018). Figure 4 below gives an overview of the architectural design data structure of some of the existing DLTs.

Figure 4

An Overview of the Existing DLTs



Source: El Ioini & Pahl,(2018)

The existing DLT architectural data structure of Blockchain is distributed, decentralized and immutable ledger designed inform of blocks that aid in storage of historical data and transactions(Antal et al., 2021). Tangle DLT is based on a directed acyclic graph (DAG) data structure that is has a decentralized data storage architecture that uses consensus protocol(Anthony Jnr., 2023). Unlike Blockchain where the architectural design allows storage of transactions in blocks, in Hashgraphs, information is stored in hashes which describe the events, hence the name. Hashgraph is also based on DAG data structure that aids in storage of transactions and based on a voting algorithm that is supported by the gossip protocol used to reach consensus among the involved nodes. Additionally, Hashgraphs architecture creates a general pattern from the transactions or event in which

the transactions are arranged in a chronological order to support the tracing of their history (El Ioini & Pahl, 2018).

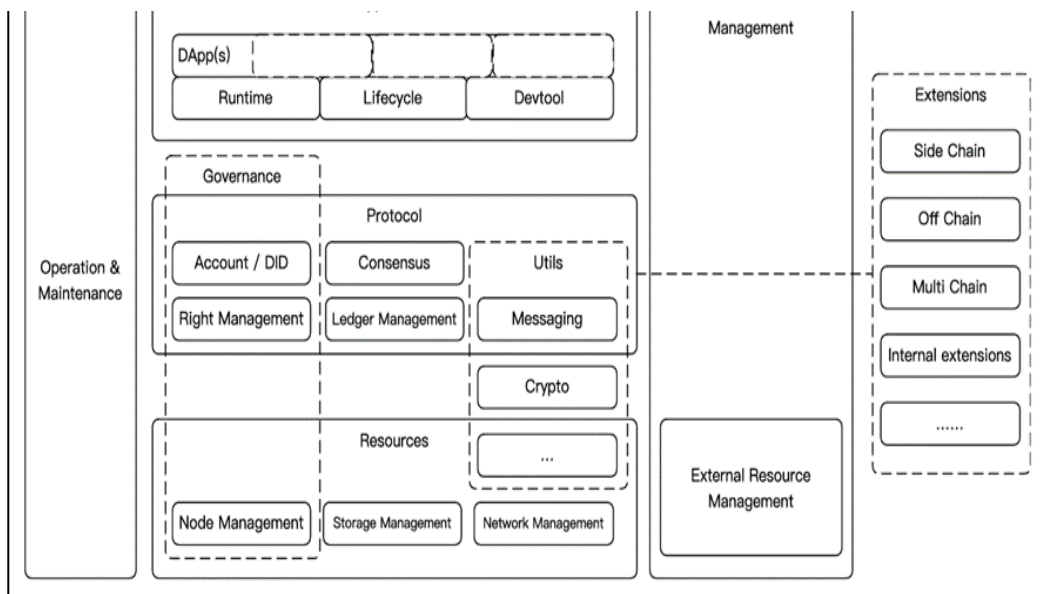
2.4.3 High-Level Conceptual Architecture of DLTs

With DLT, the cumbersome and error-prone processes required to reconcile the many contributions to the ledger, to ensure that everyone has access to the most up-to-date version, and to verify that its accuracy can be trusted, are greatly reduced or eliminated.

The extremely abstract hierarchical design of distributed ledgers is constrained by the high-level architecture, as stated by the International Telecommunication Union (ITU) unified nations agency (ITU-T FG DLT, 2019). Figure 5 shows how the overarching design may accommodate a wide variety of distributed ledgers, from public chains like Ethereum [b-ethe] and Bitcoin [b-bitc] to private chains like Hyperledger Fabric and even non-Blockchain systems.

Figure 5

Operation & Maintenance Layer of High-Level Conceptual Architecture of DLTs



Source: ITU-T FG DLT, (2019)

2.5 Evolution of Interoperability

The term "interoperability" is used throughout this research to refer to the capacity of various IT systems and software applications to share information with one another, and with healthcare providers, as defined by HIMSS (HIMSS, 2022). The need for patients and doctors to access their records from anywhere, as well as the presence of heterogeneous distributed systems that need to communicate with one another, have all contributed to the difficulty of achieving interoperability (Clunie, 2021). According to the research, it is important that the user of the system have no idea which system they are using to get the information, hence the underlying methods for data sharing and exchange must be kept secret. The data's accessibility depends on the healthcare system being available. This information needs to be readily available whenever needed.

Information systems that are interoperable have the ability to exchange information in real-time, without the need for specialized Information Technology experts' support or any extra behind-the-scenes coding. Interoperability of information systems has evolved from using middleware like firewall which is used to provide critical component of the distribute network security (Cohen, 2020a). The use of firewall security layer allowed different HIS to share and access data across different geographical locations (Guclu et al., 2020) by filtering the traffic in and out of the distributed network. However, the challenge with the use of firewall as a security technology inhibits smooth communication and use of different middleware making interoperability impossible.

Consequently, other technologies like use of web services have been adopted in which the communication rides on use of hypertext transfer protocol (HTTP) and can bypass firewall making interpretability smooth for e-commerce sector and not health sector since it raises the security challenge (Gomathy, 2021). Other web systems use Extensible Markup Language (XML) and JavaScript Object Notation (JSON) as marshalling

technology for packaging parameters to be communicated over the internet in a technology neutral format (Lv et al., 2019). Different processes and threads generally employ different data formats; therefore, marshalling is required in order to exchange information between them (Clunie, 2021). Marshalling is used to develop multiple remote procedure call (RPC) protocols. DLT based systems are an option for resolving the interoperability issues that have arisen. The banking and e-commerce sectors have adopted blockchain technology, a type of distributed ledger technology, because of its advantages. The ability of one blockchain to interact with another is known as interoperability (Lafourcade & Lombard-Platet, 2020). Cross-chain messaging protocols are the backbone of blockchain interoperability, allowing one blockchain to access and update data stored on another blockchain (Belchior et al., 2020). Additionally, the incentive for using blockchain technology is an associated reward system and use of reward algorithms and mechanism to ensure Proof-of-Work and proof-of-stake (Vujičić et al., 2018).

However, whereas this has worked well within the financial sector, it is marred with a number of challenges in health sector. First, the intensive processing power required to mine coins has not only been criticized due to its associated costs, but it also leads to enormous carbon emissions (Andoni et al., 2019). Secondly, not all applications require consensus algorithms to add blocks to the chain, but rather a mechanism to ensure secure interoperability. Further, some application areas are crucial to human life than the allied reward of mining. Consequently, the choice of a particular consensus algorithm has a considerable effect on the network speed, throughput, scalability, and transaction costs (Durneva et al., 2020). Due to the mutating architectural designs, non-standardized data formats and varying protocols, Blockchains suffer from interoperability issues. This impedes their ability to see and access information across distributed ledger systems and

the existing medical enterprise system (Belchior et al., 2020). These challenges perhaps call for development of a framework to address the interoperability issues of the medical systems.

2.6 Factors Affecting Interoperability of Medical System in Healthcare

The literature reviewed in the foregoing sections revealed that there are several factors that hinder interoperability of medical systems. These factors range from structural to semantic, security and technical aspects. A more detailed explanation of the factors affecting interoperability of medical records in healthcare industry are discussed in the subsequent sections.

2.6.1 Structural Factors

Structural factors affect the structural interoperability of medical systems. Structural interoperability refers to the ability of different medical systems to exchange and use medical data effectively and accurately (Persons et al., 2020). It involves alignment of data formats, data structures and data standardization to aid seamless medical data exchange among disparate medical systems. The structural related factors are as discussed in subsequent sections.

a. Architecture of Networks

Interoperability of medical systems can be strongly impacted by the topology and protocols of the network, which are part of its structural design. A network's structural design includes bandwidth, protocols, topology, and overall infrastructure. A well-optimized network architecture can significantly improve data exchange capabilities among healthcare businesses. Hospitals may increase the speed, dependability, and accessibility of vital patient data by ensuring the network can send and receive data

efficiently. A well-thought-out network can improve the exchange of data across healthcare institutions (Rahmani et al., 2018).

According to Uddin and others,(Uddin et al., 2018) interoperability improved in 85% of healthcare facilities that invested in optimal network architecture(Budman, 2021). This study shows how network architecture affects medical systems in real-world applications. The significance of investing in network infrastructure that can meet the needs of contemporary healthcare, including the smooth sharing of diagnostic imaging, electronic health records, and other patient data, is highlighted by this finding.

b. Viability and Scalability

Fundamental structural elements such as scalability and throughput significantly influence a medical system's ability to achieve interoperability. The report from the Healthcare Information and Management Systems Society (HIMSS) highlights the difficulties healthcare companies encounter. The ability of the system to manage a growing number of users and data is referred to as scalability. A medical system in the healthcare industry needs to be scalable to handle increasing patient data and transactions (Mishra et al., 2023). Data sharing may be hampered by system bottlenecks and decreased performance by inadequate scalability.

The speed at which data may be processed and sent over a network is known as throughput. A high throughput system is essential for rapid and effective data exchange. In the medical field, where timely retrieval of vital patient data frequently means the difference between life and death, low throughput can cause inefficiencies and delays. The practical implications of these problems are shown by the HIMSS research 2022, which revealed that 64% of healthcare organizations cited scalability as a structural difficulty for their medical systems(Emergen Research, 2022). Medical systems are

constantly producing large volumes of data, and they need to be able to handle this increase in data. Healthcare companies and medical systems' developers need to invest in strong infrastructure, use effective data management strategies, and use technologies that can manage growing data loads without sacrificing performance to overcome scalability and throughput issues. Ensuring medical systems can transmit patient data seamlessly, promoting interoperability, and eventually improving healthcare outcomes are contingent upon this.

c. Architecture for Data Storage

The structural architecture of the data storage architecture must be carefully considered in order to achieve interoperability in medical systems. In order to enhance data sharing and retrieval and enable healthcare companies to efficiently share information, well-designed data storage systems are crucial. Data retrieval, storage, and organization are the primary determinants of medical system interoperability in terms of data storage architecture. A well-designed data storage architecture facilitates efficient data retrieval and sharing, which benefits healthcare organizations by streamlining the transfer of critical patient data, including diagnostic images and medical records. Many healthcare facilities assessed in a research published in the *Journal of Biomedical Informatics* (Katehakis & Kouroubali, 2019), considered data storage architecture to be an essential structural component for interoperability. This graphic emphasizes the significance of data storage architecture in medical systems. When designing a data storage infrastructure, it is important to take into account the particular needs of healthcare data in order to guarantee data security, effectiveness, and integrity (Arslan et al., 2020).

d. Application Programming Interfaces (APIs) and Data Integration

Data integration capabilities and application programming interfaces (APIs) are crucial to attaining successful interoperability in medical systems. Within a medical system, APIs and Data Integration (Torab-Miandoab et al., 2023) act as the link that permits data exchange and communication across various healthcare apps and systems. Equally important are data integration capabilities, which guarantee that different data sources may be merged to offer a complete picture of patient information. The importance of APIs and data integration is highlighted by Panda et al. (2023), who showed that most healthcare organizations were actively striving to improve their API infrastructure for the greater medical systems' interoperability. The adoption of APIs is becoming increasingly important for healthcare companies as they work to improve interoperability and make it easier for patient data to be shared across various systems. APIs facilitate integrating external services (Juárez et al., 2022) and applications, and allow data sharing within the medical system, thereby resulting in a more complete and patient-focused healthcare ecosystem. APIs facilitate faster decision-making, better care coordination, and ultimately, better patient outcomes by facilitating access and sharing of patient data.

e. Data Protocols and Standards

A crucial prerequisite for attaining structural interoperability in medical systems is the usage of standardized data formats, coding systems, and communication protocols. For healthcare data to be accurately and consistently transferred across various medical systems and healthcare systems, standardized data formats, coding systems like Systemized Nomenclature of Medicine – Clinical Terms (SNOMED CT) and Logical Observation Identifiers Names and Codes (LOINC), and communication protocols (like HL7 FHIR) are necessary (A. Singh & Chatterjee, 2020). A structural obstacle to medical systems interoperability, according to the healthcare providers surveyed for the

2022 ONC Health IT Challenge (Acuña Ulloa & Cabanillas Castillo, 2022; AlQudah et al., 2021), is the lack of defined data protocols. The practical consequences of non-standard data might result in incorrect data interpretation, obstacles to interoperability, and possibly hampered patient treatment. Healthcare organizations may guarantee that patient data is accurately and securely exchanged across various systems and institutions by following established data standards and processes. Standardization enhances data integrity and continuity of service in addition to encouraging consistent data interpretation.

f. Data Policies and Governance

One essential prerequisite to guaranteeing interoperability in medical systems is the construction of a robust structural framework for data governance and rules. In medical systems, data governance outlines the procedures for managing, sharing, protecting, and accessing patient data. It includes guidelines and practices that guarantee data security, privacy, and adherence to pertinent laws like GDPR and HIPAA. The practical significance of this issue is demonstrated by (Truong et al., 2020) and (Torab-Miandoab et al., 2023), who found that healthcare institutions acknowledged the need for strong data governance mechanisms to ensure medical systems' interoperability. Ensuring privacy, upholding the integrity of patient data, and complying with regulations all depend on strong data governance frameworks. Good data governance frameworks also help to ensure data consistency and quality (Ajayi et al., 2020) both of which are necessary for smooth interoperability. Healthcare companies may make sure that data is handled and shared responsibly, securely, and uniformly by putting in place clear rules and procedures for data management and access.

g. Infrastructure and Hardware

A medical system physical hardware and infrastructure are essential structural elements that have a big influence on interoperability (Andoni et al., 2019). The foundation of any medical systems is its physical infrastructure, which include data centres, servers, and storage. These elements are necessary for safe and effective processing, storage, and transmission of medical data. In light of the growing need for data processing and storage, healthcare organizations need to make investments in hardware that is both dependable and up-to-date in order to maintain a seamless operation of their medical systems. Interoperability attempts may be hampered by bottlenecks, sluggish data retrieval, and downtime caused by outdated or inadequate hardware. To handle the increasing amounts of healthcare data and guarantee seamless information flow between various systems and healthcare facilities, a strong and scalable infrastructure is required (Andrew et al., 2023).

2.6.2 Semantic Factors

Semantic factors affect semantic interoperability, which refers to the ability of medical systems from different healthcare facilities to exchange, share and understand the shared medical data for use in offering medical services to the patient (Patange et al., 2021). Semantic factors that affect medical systems interoperability includes data format and semantic standardization, data mapping and ontology, semantic harmonization, consents and permissions for data sharing, cross-border communication, semantic risks and cyber security as discussed in subsequent sections.

a. Data Formats and Semantics Standardization

Consistent data formats and semantics are essential for interoperability in medical systems. The lack of a common language for health information may hamper interoperability initiatives. According to (Mehta et al., 2020) in “*The Future of*

Blockchain in Healthcare: Potential to Improve the Accessibility, Security and Interoperability of Electronic Health Records”, blockchain technology has been found to possess several benefits. This can be stated as the potential for enhancing augmentation of the exchange of information in health, enabling advancements in data transparency, enhanced patient safety and care, and improved efficiency in healthcare. Healthcare providers reported the absence of standardized data as a significant obstacle to achieving interoperability (Kotey et al., 2023; Szarfman et al., 2022). To achieve interoperability in medical systems, standardization of data formats and semantics is essential (Colombo et al., 2020; Elvas et al., 2023). However, there is a need to balance guidelines, regulations, adoption of local practices, and human factors for enhanced use and adoption of technological usage in digital platforms. A multidisciplinary approach is also needed to ensure optimum information exchange, while preserving patient safety through the engagement of patients, technology developers, legal personnel, and healthcare providers.

Interoperability, or the smooth data transfer between various medical systems and organizations, is necessary to deliver thorough and effective patient care. Sufficient evidence supports the idea that standard data formats and semantics are necessary for interoperability. Without a standard vocabulary and framework for health data, it is difficult for systems to reliably comprehend and interpret data (Brogan et al., 2018; García et al., 2020). Errors, inefficiencies, and possible threats to patient safety result from this. Healthcare organizations encounter difficulties connecting various health information systems due to lack of standard data formats. Different coding schemes and data representations might lead to a misinterpretation of crucial clinical data, which makes it more difficult for healthcare practitioners to make informed decisions (Haque et al., 2022; N. Kuo, 2015; Moon et al., 2020). Standardization agencies and organizations

like HL7 and DICOM have created data formats and coding standards for the healthcare industry to address this problem (AlQudah et al., 2021; Institute, 2020; Muinga et al., 2020). Adopting these standards by encouraging consistency in data representation makes safe and accurate data sharing possible. Thus, establishing and upholding standardized data formats and semantics is essential to improving patient care overall and increasing healthcare interoperability.

b. Data Mapping and Ontology

A common obstacle to semantic interoperability is the requirement for ontology building and data mapping (de Mello et al., 2022; Haque et al., 2022). Data reconciliation might be difficult since various healthcare companies may utilize different ontologies. Enabling interoperability, allows systems to talk to one another about data in EHRs, and in the process alter medical systems with ontologies that make data sharing possible. Data mapping and ontology creation are essential for medical systems to achieve semantic interoperability. Accurate interpretation and comprehension of data transferred throughout different healthcare organizations is ensured via semantic interoperability. It is well-established that the requirement for data mapping and ontology creation impedes semantic interoperability. (Belmonte & Ot, 2021; E. Li et al., 2021; Schulz et al., 2018). It is common for various healthcare institutions to define medical concepts, processes, and patient information using their own data structures, terminologies, and ontologies. This variability in data representation poses a challenge when trying to integrate and reconcile data from multiple sources.

In order to offer a common understanding, data mapping comprises converting and interpreting data across different formats. Ontology development, on the other hand, aims to provide a consistent language and framework for the explanation of medical ideas. Closing the semantic gap between different medical systems requires these steps.

To address these challenges, groups like SNOMED CT and LOINC have developed extensively utilized ontologies and coding systems for the healthcare industry. Adoption of such standardized ontologies improves semantic interoperability and makes data mapping easier (Belmonte & Ot, 2021; de Mello et al., 2022; Schulz et al., 2018; Torab-Miandoab et al., 2023). Development of ontologies and data mapping are essential components in guaranteeing semantic interoperability in healthcare. They enable various healthcare institutions to exchange information coherently, thereby enhancing communication and eventually improving patient care and results.

c. Semantic Harmonization

Interoperability requires semantic harmonization(de Mello et al., 2022; Torab-Miandoab et al., 2023) or coordinating the meaning of data across many systems. Semantic harmonization poses distinct issues in the healthcare industry, primarily because of the diverse data types involved, such as clinical, administrative, and financial data. It is often known that semantic harmonization presents difficulties in the healthcare industry. Clinical data, which includes medical codes, diagnoses, and patient records, is very different from administrative data, which can contain billing codes, insurance information, and scheduling specifics. Thorough mapping and standardization(Eklund, 2019; Health Act, 2017) are necessary to achieve harmonization across these disparate data types. Different organizations and systems utilize distinct vocabularies and coding systems, which is one of the main barriers to semantic harmonization in the healthcare industry. Data interpretation may become inconsistent if, for instance, a diagnosis code in one system does not immediately match a code in another.

Healthcare standards' organizations like SNOMED CT and HL7 have created coding schemes and common terminology to help with semantic harmonization in response to these issues (Kim et al., 2020). By facilitating consistent data sharing between healthcare

organizations and systems, adopting these standardized vocabularies enhances interoperability and improves patient care. In conclusion, the variety of data types in the healthcare industry makes semantic harmonization more complicated, even though it is necessary for healthcare interoperability. Standardization initiatives and the application of uniform coding systems are essential to overcome these obstacles and guarantee that healthcare data can be exchanged and comprehended efficiently.

d. Consents and Permissions for Data Sharing

Taking patient preferences, consents, and data-sharing permissions into account is essential to interoperability in healthcare, especially within medical systems. The healthcare sector is aware of this reality which has ample supporting documentation. Abernethy et al. (2022) found that semantic issues with data-sharing permissions were necessary for efficient functioning of healthcare facilities. Patient privacy and permission are legally and morally significant aspects of healthcare data sharing. The rules and regulations governing patient data access, sharing, and storage may differ throughout jurisdictions. Because of this, it becomes more challenging to guarantee that medical systems function within the parameters of the laws while permitting efficient data interchange. For example, medical systems operating within the European Union's authority must comply with the strict guidelines set forth by the General Data Protection Regulation (GDPR) regarding patient consent and data protection (Truong et al., 2020; Zheng et al., 2018).

On the other hand, patient data exchange in the US is governed by the Health Insurance Portability and Accountability Act (HIPAA) (Savage & Savage, 2020; Torab-Miandoab et al., 2023), which has its own set of regulations. Mechanisms for handling consents and permits in medical systems must be created with flexibility and adaptability (Belmonte & Ot, 2021; Katakis & Kouroubali, 2019) to keep these jurisdiction-specific rules in

mind. This promotes interoperability between medical systems and organizations while guaranteeing that patient data is transmitted in a secure and compliant manner. Creating distributed ledger-based solutions and consent management platforms offering transparent and auditable consent records are two initiatives aimed at tackling these issues. Ultimately, these systems protect patients' privacy by giving them more excellent choice over who can access their data and when.

e. Cross-Border Communication

In cross-border settings, achieving interoperability in medical systems becomes considerably more difficult (Pawczuk et al., 2019). Several nations may have laws and standards governing healthcare, while a small percentage of healthcare facilities have cross-border semantic interoperability solutions deployed in their medical systems. It is critical to ensure that patients' health data (Seaberg et al., 2021) can be accessed, shared, and used safely and compliantly in today's globalized world, as they may seek healthcare services or treatment in different nations. However, working with disparate healthcare standards and regulatory frameworks makes establishing interoperability more difficult. For instance, the GDPR (June Okal, 2018) of the European Union places stringent regulations on the management of personal data, including health-related data. On the other hand, HIPAA (McGhin et al., 2019) governs healthcare in the United States. To permit cross-border data sharing (Kouroubali & Katehakis, 2019) while abiding by the legal requirements of each nation, it is necessary to carefully manage these variances in data protection laws and privacy rules.

The creation of international agreements that specify how data should be exchanged and safeguarded across borders, and defined data exchange methods, are common components of cross-border interoperability solutions. Initiatives like the EU-U.S. Global and standards organizations like Privacy Shield strive to make data transmission

in healthcare easier, and guarantee that all applicable laws are followed. To advance the interoperability levels, Cohen (2020b) and Durneva et al. (2020) report that various International health information (HIT) standards like HL7 CDA (Torab-Miandoab et al., 2023) have been developed. The intricacy of cross-border medical systems interoperability highlights the need for international standards to be harmonized and for solutions to be developed that can securely manage data sharing while considering national legal and regulatory differences.

f. Semantic Risks and Cyber security

Cyber security and semantic hazards need to be addressed via interoperable medical systems. Maintaining patient privacy requires ensuring that information is safely transferred and understood by authorized parties. Some of the semantic risks and cyber security issues include the cyber security risks and the semantic risks.

Cyber security Risks: Since patient data is so sensitive, cyber threats and hacks are a continual worry in the healthcare industry. Strong cyber security safeguards must be incorporated into interoperable medical system to guard against data breaches and illegal access. Cyber attacks are widespread against healthcare businesses, and breaches can have serious repercussions. According to a report by (Dagher et al., 2018; Edemekong & Micelle, 2020), a healthcare data breach in 2021 could typically cost \$9.23 million, which is a 29.5% increase from 2020 as reported (IBM, 2021).

Semantic Risks: Inaccurate interpretation of data can result in semantic interoperability problems that compromise patient safety, and cause medical blunders (de Mello et al., 2022). Serious dangers might arise from inaccurate diagnoses and treatments resulting from misinterpreting clinical data. In medical systems, semantic interoperability is crucial to guaranteeing proper understanding and security of shared data between various

medical systems (Yang et al., 2022). Medical errors are one of the top 10 causes of death worldwide, according to World Health Organization research, and semantic problems can be the cause these medical errors. Healthcare organizations experienced a 42% rise in semantic cyber security incidents in 2022 compared to the year before, according to a report by (Abernethy et al., 2022). It is critical to address cyber security and semantic risks in interoperable medical systems to protect patient privacy, stop data breaches, lower the risk of medical errors, and ultimately improve the quality of healthcare as a whole.

In summary, establishing semantic interoperability in a medical system with many moving parts (Seaberg et al., 2021) is difficult. Several factors, including the absence of standardized data formats and semantics, data mapping, semantic harmonization, permissions for data sharing, cross-border issues, and semantic cyber security concerns, influence the success of interoperability efforts. It is essential to address these problems through appropriate standards, ontology development, and robust security mechanisms so as to use medical systems successfully.

2.6.3 Security Factors

When it comes to the healthcare industry's medical systems interoperability, security is a critical consideration. The following evaluation looks at the security aspects that affect medical systems' capacity to protect patient data's confidentiality, integrity, and privacy; and ways of utilizing medical data and statistics from many sources to back up findings.

a. Data Encryption

One of the most important security features of medical systems is data encryption. It guarantees the integrity and confidentiality of medical records. This is a well-known phenomenon, and the Ponemon Institute's image illustrates the negative effects of

insufficient encryption (Elvas et al., 2023). To convert sensitive patient data into safe, unreadable formats, cryptographic techniques are used. This is crucial to avoiding unwanted access to medical records and guaranteeing that the information is safe even in the case of a breach. The importance of encryption in protecting patient data is shown by Seh et al. (2020), who found out that healthcare data breaches were caused by lack of encryption. Without adequate encryption, healthcare organizations run the risk of having their data compromised, which can have serious financial, legal, and reputational repercussions. Numerous regulations about healthcare data privacy, such as HIPAA and GDPR, mandate encryption of data both in transit and at rest. Robust encryption techniques shield data from unsanctioned internal access in addition to external threats.

b. Management of Identity and Access

In medical systems, efficient access control and identity management are essential security components that guarantee the integrity and confidentiality of patient data. Identity management and access control procedures (Arslan et al., 2020; Wang et al., 2022) specify who has access to patient data and what they can do with it. Identity management ensures people are legitimate and have the right kind of authorization for their access. These are essential elements of medical systems patient data security. The usefulness of these security measures found that on average, 80% of healthcare facilities have their employees aware of the type of security training (Accenture, 2019) being offered to them, much as they appreciate that strong identity and access management is a crucial security component for medical systems interoperability. Patient treatment may be jeopardized and privacy violated as a result of unauthorized access to patient data (Eunice et al., 2019).

Healthcare organizations may apply the principle of least privilege by limiting access to patient data to only those who are allowed, thanks to robust access control and identity

management systems. By doing this, the possibility of insider threats and data breaches which can raise serious issues in the healthcare industry is reduced. As HIMSS picture illustrates, access control and identity management are essential components of medical systems security. Strong security measures in these domains are necessary to protect patient information, preserve privacy, and guarantee that the system's healthcare data can only be accessed and modified by authorized individuals.

c. Consensus Mechanisms in Blockchain

Indeed, the security and long-term viability of medical systems can be greatly impacted by the consensus techniques selected. Consensus mechanisms on the blockchain govern the validation and addition of transactions to the blockchain. Proof of Work (PoW), as utilized in Bitcoin and other systems, consumes a lot of energy and demands a lot of processing power to secure the network. On the other hand, Proof of Stake (PoS), which is utilized in networks such as Ethereum 2.0, is more sustainable and energy-efficient. The research report by Ibanez and Ruathat was published in 2023 emphasizes the notable advantages of PoS in terms of energy efficiency. It found that PoS-based medical system had 99% lower energy usage compared to PoW-based systems (Ibañez & Rua, 2023). This is crucial to lowering medical system's operational expenses and environmental effects without sacrificing security. Although PoW has proven to have strong security features, it can be difficult to scale and is energy-intensive especially in medical systems. PoS provides a more sustainable and ecologically friendly option, which is crucial in healthcare applications where energy security and efficiency are critical.

d. Smart Contracts and Vulnerabilities

There is ample evidence to suggest that the use of smart contracts in medical systems may have security flaws. On blockchain networks, smart contracts are self-executing pieces of code that can be manipulated by malevolent parties. Smart contract security

flaws can have serious repercussions, especially in healthcare applications where patient data and vital functions are at risk. The startling frequency of security flaws is brought to light by the Quant stamp study in 2021, which discovered that 58% of smart contracts in healthcare medical systems had at least one severe vulnerability. It is crucial to carefully audit and secure smart contracts since they include critical vulnerabilities that could result in data breaches, financial losses, and other negative consequences (Dai et al., 2019; Saxena et al., 2021). For medical systems smart contracts to be reliable and safe, security audits, code reviews, and best practices in smart contract creation are essential to minimizing vulnerabilities. Furthermore, by mathematically demonstrating the accuracy of smart contracts, the application of formal verification techniques might improve their security.

e. Immutability and Data Integrity

It is commonly known that the immutability of data on a blockchain can greatly improve data integrity. Immutability refers to the inability of data in a blockchain to be changed or removed after it has been added (Urkude et al., 2021). This characteristic improves data integrity by making sure that medical records and other data are impenetrable to tampering. The significant advantages of blockchain in maintaining data integrity as researched by Liang et al. (2023), showed that medical systems using blockchain technology experienced a 98.7% reduction in data integrity incidents compared to traditional health information systems. Healthcare companies may keep patient data accurate and reliable by utilizing Blockchains immutability, which lowers the possibility of illegal changes, data breaches, and other integrity-related events. This is especially critical in the healthcare industry, as patient care and medical decision-making depend heavily on accurate data.

f. Privacy Preserving Techniques

In medical systems, privacy-preserving methods are essential for safeguarding sensitive patient data. Sensitive patient information can be kept private when sharing and analyzing data by healthcare institutions through the use of strategies like differential privacy and zero-knowledge proofs (Holweger et al., 2021). These methods are essential for protecting patient privacy and facilitating data-driven medical decisions.

The practical significance of these strategies is highlighted by Deloitte report in 2021, which found that as consumers become the center of digital transformation, there arises the need to employ privacy-preserving techniques for securing patient data in medical systems (Anthony Jnr, 2021). Healthcare organizations have a moral and legal duty to protect patients' privacy. By using privacy-preserving strategies, they can fulfil this requirement while still making use of data analytics and interoperability. These methods allow medical systems to strike a compromise between data utility and privacy protection by aggregating and analyzing data without disclosing personal identification or sensitive health information. This is especially important in the healthcare industry because privacy is very important.

g. Frequent Monitoring and Auditing

To detect and avert possible risks, medical systems require constant infrastructure auditing and data access monitoring: monitoring and Auditing. The medical system infrastructure and data access are regularly audited and monitored, which assists healthcare companies in recognizing and addressing security threats, vulnerabilities, and unusual activity. The confidentiality and integrity of patient data must be preserved, and this proactive approach is essential. The observable advantages of these security measures are highlighted by the Kaspersky survey (Xia et al., 2017), which agrees that due to the sensitivity of health information, healthcare organizations need to have an

enhanced security posture by putting frequent auditing and monitoring procedures into their medical system. Frequent audits and monitoring help healthcare businesses lower the risk of data breaches and unauthorized access by enabling them to quickly notice and address security events. In the healthcare industry, where patient data is extremely sensitive and vulnerable to various risks such as insider threats, cyber attacks, and unintentional data exposures (Sun et al., 2018), this proactive security approach is essential. Healthcare businesses can improve their security posture and better secure patient information by regularly monitoring and auditing their medical system.

2.6.4 Technical Factors

The interoperability of medical system in the healthcare industry is greatly influenced by technical considerations. The following examination looks at several technological aspects that impact interoperability and provides data and facts from several sources to back up the argument.

a. Blockchain Structures and Procedures

The medical systems scalability, speed, and interoperability are greatly impacted by the blockchain platform and protocol selection. The features and capabilities offered by various blockchain platforms and protocols vary. The compatibility with other systems within a medical system, transaction speed, and scalability can all be impacted by the platform and protocol selection. The real-world significance of this element, as researched by Saeed et al., revealed that healthcare organizations have employed the use of blockchain platform as a significant technical consideration for maintaining medical system interoperability (Saeed et al., 2022).

Healthcare companies need to be sure the blockchain platform they choose meets their unique scalability and interoperability needs. For instance, smart contract functionality is

available on some blockchain platforms, such as Ethereum, which qualifies them for sophisticated healthcare applications. Others, like Hyperledger Fabric, provide more of an emphasis on control and privacy and might be more appropriate for medical systems with particular requirements for data sharing and security.

b. Mechanisms of Consensus

The efficiency and security of medical systems can be significantly impacted by the consensus mechanisms chosen, such as Proof of Work (PoW) and Proof of Stake (PoS), which can also have an impact on how well-integrated these systems are with other systems. Mechanisms of Consensus which refers to the process of verifying and appending transactions to the blockchain is determined by consensus procedures (Hafid et al., 2020). The consensus technique selected can affect security, energy efficiency, and transaction speed. This shows how important it is to choose the right consensus mechanism in the real world. For instance, PoS is more energy-efficient but depends on validators who have an interest in the network, while PoW is renowned for its strong security but energy-intensive (Union et al., 2020). To guarantee that the healthcare system can function effectively, safely, and in a way that promotes interoperability with other medical systems, the consensus mechanism selected should be in line with the particular requirements and objectives of the system.

c. Solutions for Data Storage

In medical system, the choice of data storage solutions including on-chain versus off-chain storage has a big impact on how easily healthcare data may be retrieved. Within the medical system, data storage solutions specify where and how medical records are kept. While off-chain storage could make use of other databases or storage systems, on-chain storage maintains data directly on the blockchain. The practical importance of this element is highlighted by the HIMSS research in 2021, which found that a good

percentage of healthcare institutions were worried about selecting the best data storage options for medical system interoperability. The decision of on-chain (Onik et al., 2019) versus off-chain storage affects transaction costs, scalability, and data accessibility. To guarantee that medical data can be efficiently accessed and retrieved and that the medical system can develop to accommodate the increasing volume of medical data, while preserving compatibility with other medical systems, it is imperative to choose the right data storage solution (M. Kim et al., 2020).

d. Smart Contract Development

The medical system technological interoperability is greatly impacted by smart contract quality and compliance with industry standards. The dependability, security, and standard compliance of smart contracts self-executing programs on blockchain networks can affect how well they interface with other medical systems (Elvas et al., 2023). The fact that healthcare companies were committed to improving the security and quality of smart contracts to promote medical system interoperability is evidence of the practical understanding of the significance of this element, as reported by Deloitte's investigation (Budman, 2021). Maintaining the integrity and security of healthcare operations depends on smart contracts being well designed, secure, and compliant with industry standards. Healthcare organizations can improve the technical interoperability of medical system and facilitate the smooth interchange of data and transactions while reducing the risks associated with vulnerabilities or defective contracts by concentrating on the development and quality of smart contracts.

e. Standards for Interoperability

Indeed, current medical systems cannot share the medical data without the usage of interoperability standards like HL7 FHIR and DICOM. These set forth the common data formats and protocols that provide seamless information sharing between various

healthcare systems. To ensure data sharing between medical system and current healthcare systems, standards like (Clunie, 2021) DICOM (Digital Imaging and Communications in Medicine) and HL7 FHIR (Fast Healthcare Interoperability Resources) are essential.

The practical significance of implementing these standards is highlighted by Ulloa & Castillo (2022), who found that healthcare providers cited adherence to existing interoperability standards as a critical technical component for medical systems interoperability. To improve the overall healthcare coordination and quality, interoperability standards are essential for fostering the sharing of patient data, including clinical records and medical pictures. Healthcare companies can support data sharing and interoperability efforts inside the medical system and throughout the larger healthcare ecosystem by adopting and putting these standards into practice. This guarantees that data is transferred accurately and consistently.

f. Interfaces for Application Programming (APIs)

Indeed, the capacity to integrate medical systems with other healthcare applications and systems depends on the functioning and availability of Application Programming Interfaces (APIs). APIs are bridges that facilitate seamless data interchange and communication across various software systems, including medical systems. They are essential to the healthcare industry because they link various applications and promote interoperability.

The practical significance of this factor is further underscored by Abernethy et al, as their study reports that ONC should ensure timely, full implementation of standards of structure, coding, security, and common APIs, as these standards are foundational for most progress on digital health (Abernethy et al., 2022). Strong APIs enhance patient data interchange, interoperability, and the improvement of healthcare services by

enabling healthcare organizations to integrate and interact with a variety of healthcare systems. Healthcare organizations can leverage medical systems to facilitate seamless data sharing and workflow automation by providing well-designed and secure APIs that enable interaction with telemedicine platforms, EHR systems, data analytics tools, and other critical healthcare applications.

g. Structure and Network

Medical systems depend on the stability of the underlying network and infrastructure, which includes servers, bandwidth, and security protocols, to ensure technical compatibility. The foundation of medical system is provided by the underlying network and infrastructure, whose security, scalability, and dependability are critical to the smooth interchange of data and interoperability.

Infrastructure preparedness is an important technical factor for medical system interoperability, as indicated by a (Australia, 2020) KPMG poll. High availability, scalability, and data transmission capabilities necessary for medical systems to function together effectively are supported by a strong infrastructure which highlights the practical significance of this factor (Anthony Jnr., 2023; Laroiya et al., 2020). To make sure that patient data is available when needed and is shielded from unwanted access, medical systems must be able to manage the growing volume of healthcare data, offer low-latency access, and secure data. Interoperability and patient care may be hampered by bottlenecks and downtime, which can be avoided with the correct infrastructure.

2.7 Distributed Ledger Technologies Interoperability

Similar to database interoperability, DLT interoperability is concerned with systems, data, and information. However, DLT interoperability also necessitates the capacity to read, observe, and respond to state and events. An event, often a transaction, proposes a

new state of the ledger, which must be continuously refreshed and synced to ensure uniformity. Here, state is the sequence of transactions at a given point in time. The siloed architectural structure of the hundreds of ledger initiatives now underway means that interoperability is not guaranteed (Natarajan et al., 2017).

However, each of these three approaches can be used to structure DLTs' interoperability. It can first occur between a DLT and the enterprise systems of a single company. Both the Blockchain and the conventional banking/fiat payment system have experienced this (Lafourcade & Lombard-Platet, 2020). However, this is underutilized outside financial cryptosystems where it has shown promise as a solution. Second, different DLT platforms can communicate with one another. For example, Bitcoin and DogeCoin are two examples of permission less ledgers, while Corda and Ethereum are examples of permissioned and permission less ledgers respectively (Pillai et al., 2020).

The financial sector is one of the few places where this is observed. However, this is understandable given the limited development of Blockchains beyond financial systems. Interoperability across smart contracts on the same blockchain is now a reality. Corda applications, which are actually just smart contracts on the same Corda ledger (Zeuch et al., 2019), are a common case in point. This study suggests using the first form of interoperability to guarantee that the DLTs connect safely with the particular organizational medical systems established across the various interoperability levels. This is necessary because there are multiple medical systems now in existence.

There are several interoperability tiers at which the DLTs can be implemented. Level 1 connection standards allow one system or application to securely communicate and share data with and receive data from another system or application, without either system or application needing to understand the meaning of the data being exchanged (Kouroubali

& Katerakis, 2019). Level 2 structure (Braunstein, 2018) specifies the form, grammar, and organization of data field-level exchange for meaning. This signifies the receiver system's skill at deciphering data from the field level.

Providing shared understanding and meaning to the user is the goal of Semantic (Level 3), which entails providing common underlying models and codification of the data, such as the use of data items with standardized meanings from publicly available value sets and coding vocabularies. At this stage, Health Information Systems (HISs) are able to share data, make sense of it, and put it to good use (de Mello et al., 2022). As a result, doctors and nurses using one hospital's EMR system are able to share their patients' medical record summaries with other doctors and nurses using other EMR systems. This improves the quality, efficiency, and safety of healthcare services for everyone involved. At this juncture, medical facilities are able to easily communicate patient data, which helps cut down on unnecessary procedures, improves healthcare coordination, and more accurately diagnoses patients.

Healthcare Information and Management Systems Society (HIMSS) (Persons et al., 2020) states that Level 4 is Organizational, and that it includes governance, policy, social, legal, and organizational considerations to enable secure, seamless, and timely data communication and use within and across organizations, entities, and individuals. Data may be communicated and used efficiently inside and across companies, entities, and individuals when these elements are in place, including shared permission, trust, and integrated end-user processes and workflows. Healthcare organizations are aiming at achieving interoperability of medical systems at all levels, but most are still developing independent medical systems that are not interoperable due to use of different data formats, protocols and architectural designs. Current health data standards, such as health level 7 Fast Healthcare Interoperability (HL7 FHIR), can help healthcare organizations

to achieve medical data standardization that would be necessary for medical systems interoperability.

2.8 Medical Systems Interoperability Frameworks

Interoperability is key to sharing data between programs that are written for various operating systems. When talking about medical records, interoperability refers to how well clinical intent is communicated across organizational silos. Due of the nature of healthcare data, this is a challenging goal to set for yourself.

The two major facets of medical systems interoperability occur at the levels of structural and semantic levels, each of which are necessary for the successful exchange of medical data (da Conceição et al., 2018). Structural level defines the formats, syntax and organization of the data to be exchanged. Since medical data is complex, and its heterogeneous structures decrease the effectiveness of analysis and reduce understandability, the structural interoperability level is of big concern. To combat this, several industry-wide standards have been advanced (McGhin et al., 2019), but they lack the interoperability aspect due to the dynamism of the independent systems. While effective in their own front, there is no standardized approach of achieving medical systems interoperability since aligning data encoded formats and protocols with disparate standards is a non-trivial task for the medical systems software developers (Soule, 2020). This remains an open problem and the need for medical systems interoperability increases as the systems are developed constantly.

Semantics is the process of assigning meaning to data through the use of standardized language. The understanding of healthcare data relies on this kind of codification. The healthcare industry as a whole, however, needs to settle on a single set of codification schemes, or controlled terminologies, for this to work (Patange et al., 2021). In contrast

to the impracticality of trying to standardize medical terminology, narrowing the focus of vocabularies to cover a specific topic may prove to be a workable alternative. Together, structural models and subsets, known as Value Sets, can limit the possible encodings of attributes and attribute types. The Health Level 7 (HL7) standard and the FHIR are two initiatives that aim to accomplish these goals.

The Health Level 7 (HL7) is a global consortium that sets norms for the IT used in healthcare. HL7's original goal was to facilitate communication between systems by establishing syntactic rules for point-to-point messaging. Based on its flagship "version 3"(v3), (Blobel, 2016), HL7's current aim is to develop standards for semantic interoperability in healthcare IT. Unfortunately, v3 has been beset by quality and consistency difficulties, and it has not been able to keep up with current breakthroughs in semantics and ontology or in computer science and engineering (Yang et al., 2022). In response, HL7 developed the "Services-Aware Interoperability Framework" (SAIF), intending to use it as a foundation for future organization-wide standardization initiatives. It is necessary to consider the main design principles of a semantic interoperability framework, such as those related to computational behavior and static semantics. At this point, SAIF is unable to support the crucial HL7 v3 family of standards change (Braunstein, 2018). Inconsistent use and interpretation of the standard have led to problems with HL7, impeding smooth data flow and requiring extra translation layers. These challenges led to the HL7 and SAIF frameworks being abandoned in favor of the FHIR standard.

An open-source standards framework known as FHIR has replaced the HL7 and SAIF frameworks in the healthcare sector. FHIR was created to make it easier for platforms to share healthcare data with one another. For the purpose of organizing and interpreting data by different computer systems or applications, such as patient, condition, and

prescription resources, FHIR provides a specified format, and may be used to organize financial and workflow data, including as claims data, and appointment scheduling (STU, 2018). Financial and workflow data, like as claims information, appointment scheduling, and more, can be structured using FHIR, as stated by Persons et al. (2020). In FHIR, 'resources' serve as the foundation for all data transfers. The resources must primarily use either JSON, XML, Atom, HTTP, or OAuth as their underlying data format. Despite its rapid progress, FHIR is being developed by a wide variety of organizations. Proactive groups such as the UK's INTEROPen and France's Interop' Santé are producing FHIR recommendations for specified use cases, but no complete guide is in place to address these issues (Zhang et al., 2018). While the FHIR has made progress in addressing structural data exchange formats, the compatibility of its semantics remains an open question.

The European Union also made an effort in this direction in 2012 when it established the European eHealth Interoperability Framework (EIF). This framework defines a standardization of standards, profiles, and procedures for the electronic delivery of healthcare. Organizational, legal, technological, and semantic interoperability are the four stages identified by this framework (European Commission & Directorate-General for Communications Networks Content and Technology, 2013) for linking e-Health systems. In 2017, in the context of the digital single market policy in Europe, the new European Interoperability Framework (new EIF) was adopted to enhance interoperability in the public sector. It is hoped that the new EIF's suggestions, models, and guidelines lead to better government services across Europe. The new EIF has been expanded upon to become the Refined eHealth EIF (ReEIF). Through sophisticated interoperability mechanisms for public services in all EU member states, ReEIF was created to encourage open and secure movement of data inside the EU. When deploying eHealth,

member states were encouraged to make use of the framework (Kouroubali & Katehakis, 2019). Data syntax and the standardization of data formats and protocols provide difficulties for both the EIF and the ReEIF frameworks. Due to the technical nature of the standards and protocols employed, only European Union member states have adopted and begun implementing the two frameworks.

The Kenya Health Information Systems Interoperability Framework (KHISIF) (MoH Kenya, 2020) aims at supporting the ministry of health strategy of providing patient-centric health service has been proposed. This framework is still at the infant and proposal stages and it has not yet been actualized, hence the need to actualize the idea of making medical systems interoperable.

According to the examined interoperability frameworks for medical systems, the two most significant obstacles are those of structural and semantic compatibility. Standardizing the syntax, data formats, and protocols that may be used globally to link all medical systems and enable secure data exchange across the medical systems is a challenge that gives rise to structural interoperability. Codification of medical data using data pieces with agreed definitions and meanings is essential for achieving semantic interoperability. The capacity of HISs to communicate, comprehend, and make use of one another's data is the focus of the field known as semantic interoperability. It is also important to remember that each of these frameworks runs independently, tapping into a unified data store that stores information in a wide variety of structural and semantic formats. To overcome these obstacles, an enhanced secure distributed ledger interoperability framework for medical systems can be implemented.

According to Chowdhury et al. (2019), DLT is a new form of database technology in which databases are linked in a decentralized manner via a peer-to-peer network and

maintained by a consensus process. Supporters of DLT argue that technology has the potential to solve interoperability problems by making the flow of medical information immutable and safe (Katehakis & Kouroubali, 2019).

Participants can verify the accuracy of distributed ledgers at any node in the network and have access to a carbon copy of all network-wide records. When the ledger is updated, all of the participants receive a copy of the new version. The database is synchronized between devices to guarantee consistency. Since distributed ledgers are inherently decentralized, they give an extra degree of protection while also facilitating interoperability. Due to the database's global distribution, it is hard to breach.

2.9 Theoretical Framework

Theoretical framework comprises all the important ideas, terms, and sources used in this investigation. The goal of theoretical framework is to show how well the research team understands the significance of interoperability in establishing trustworthy medical systems using selected concepts from distributed ledger technologies (DLTs) (Kivunja, 2018).

2.9.1 DLT System Theory

A distributed ledger (DL) is a database in which numerous users simultaneously create and update identical replicas of the database. The term "distributed ledger technology" (or "DLT") is used to describe a digital system for documenting asset transactions in which the transactions and details about those transactions are recorded in various locations simultaneously. Special attention is given to protocols and underlying architecture that enable dispersed computers to propose and validate transactions and update records in a coordinated fashion across a network (Rauchs et al., 2018).

Due to their distributed structure, DLTs do not require a trusted third party to verify or authenticate data or conduct transactions. All participants on the distributed ledger can examine the records in question based on a unique identifier, as they are only recorded in the ledger when they have been time stamped and given a unique cryptographic signature for authenticity. Furthermore, this approach offers an auditable and verifiable record of all data in that repository. Chowdhury et al. (2019) note that the structural abilities of these systems to provide a strong support for data integrity, resilience, authenticity, decentralization, anonymity, autonomy, and provenance have opened up opportunities in various domains to permit secure sharing of data in a trustless setting. As a result, DLTs can be implemented with a wide variety of different architectures, such as Blockchains, Directed Acyclic Graphs (DAGs), Hashgraphs, Holochains, Tempo (Radix), and the Cerberus consensus framework (Leonulous, 2020). However, most DLTs are segregated towards certain application platforms, leading to a rise in the requirement for interoperability and data sharing between disparate pieces of software.

2.9.2 Contractual Theory

According to contractual theory, any relationship between agents that intend to exchange data and information is costly in terms of drafting the contract, controlling and trusting the involved agents which results to parties facing irregularities of information. The agents can be viewed to be different health institutions and the medical practitioners or health care givers. To limit the transaction cost during the data and information exchange in using DLTs calls for use of smart-contracts (Radanović & Likić, 2018; Moubarak et al., 2020).

A smart contract is a computer program that, once stored in the distributed ledger of the blockchain, carries out the terms stipulated within it (Dagher et al., 2018). These contracts can be automatically triggered from the DLTs they are stored in. Smart

contracts offer a novel solution for archiving EMR-related information. Patients would have more control over their own diagnostic data utilizing this technology, while hospitals and other healthcare providers would have easier access to patient data stored at other facilities. With their added privacy and compatibility, DLTs could greatly benefit EMR systems. Implementing useful agents for data management is a possible application of smart contracts. Rules governing who can view what in a patient's encrypted medical record; for instance, can be included in smart contracts. Thus, smart contracts may be used to add a layer of privacy to a decentralized database. By automating the process of categorizing and storing data at varying levels of privacy and detail, smart contracts may prove useful in the data-cleansing process (Arlindo et al., 2018).

From the contract theory point of view, one main advantage of using smart contracts is their ability to reduce transaction costs. Unlike the traditional contracts, where parties are at liberty to decide whether to fulfill and honor their contract obligation, the smart-contracts cannot be compromised or breached since they are internally integrated into the DLTs architecture. Smart-contracts are also less expensive to implement and are transparent (Baron & Chaudey, 2019).

This study used DLT System Theory and Contractual Theory to guide the design of the enhanced secure distributed ledger interoperability framework for medical systems.

2.10 Conceptual Framework

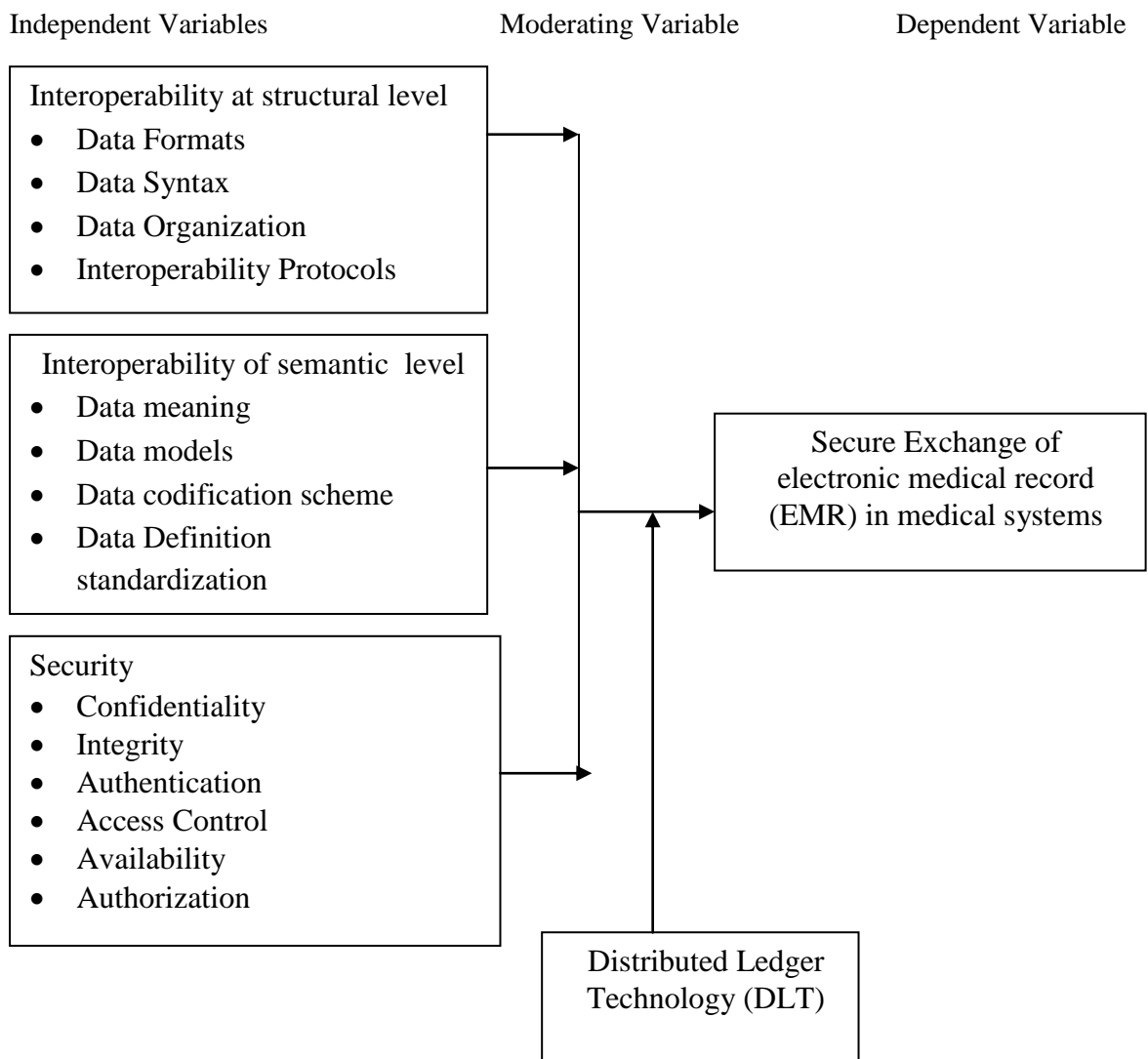
The conceptual framework of the study indicates the dependent variable as secure medical systems to aid secure exchange of electronic medical records (EMRs). The independent variables are secure interoperability, which encompasses structural interoperability level that defines the data formats, data syntax, data organization and interoperability protocols. Semantic interoperability level that shows the data meanings,

data models, data codification and data definition standardization. Additionally, the other independent variable entails the security of medical system which defines the security requirements like confidentiality achieved through encryption, integrity achieved through hashing, authentication achieved through use of digital signatures, access control achieved through user login accounts and passwords, authorization achieved through user roles segregations and availability achieved through ensuring that secure EMRs are exchanged and made available to authorized users at the time when needed.

The moderating variable is distributed ledger technology that helps in enhancing the secure interoperability of medical systems. This implies that independent variables security requirements and interoperability architectural layouts influence the security of medical systems and they exchange the electronic medical records (EMRs) moderated by the digital ledger technologies as the moderator variable. The conceptual framework is as depicted in Figure 6, which identifies the dependent variable, independent variables, and moderating variable.

Figure 6

Conceptual Framework

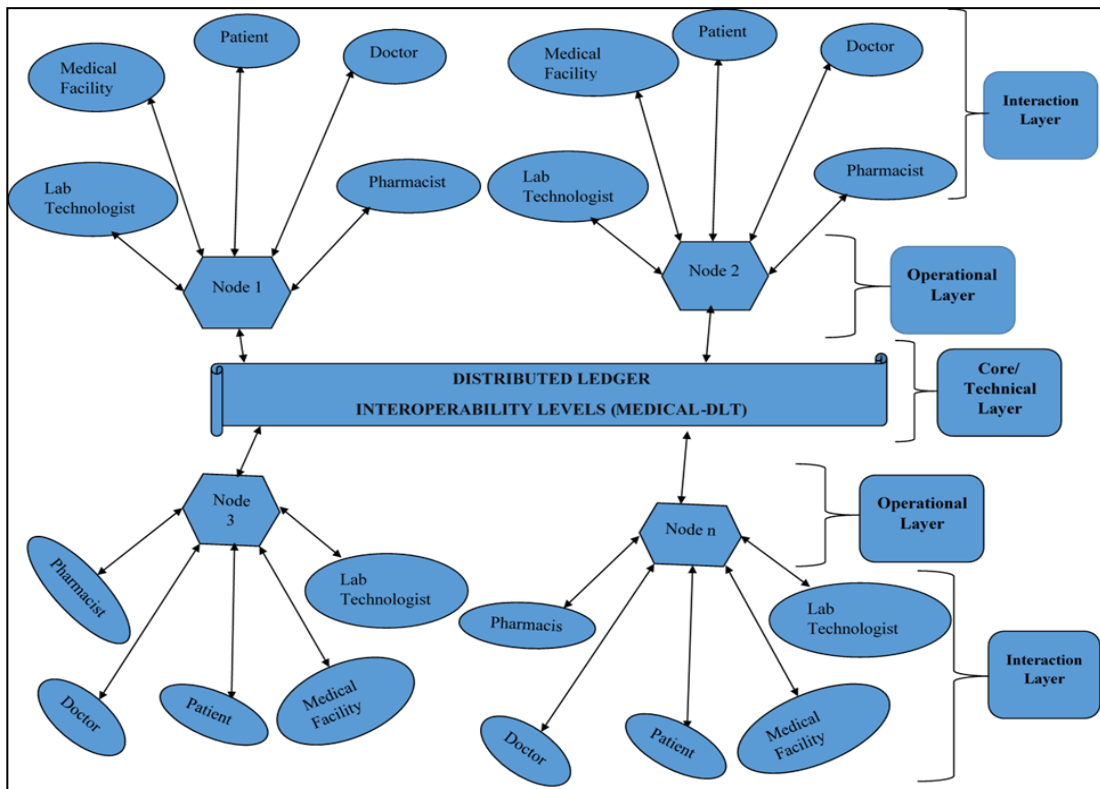


Source: Author, (2024)

By leveraging distributed ledger technology, all data is securely encrypted using different cryptographic algorithms and hashed using the hashing algorithms, providing a secure and transparent environment where no person or entity can tamper with data stored in the distributed ledger, unless those that are authorized. An in-depth implementation conceptual framework of an enhanced secure distributed ledger interoperability framework for medical systems that comprises of core layer, operational layer and interaction layer is shown in Figure 7.

Figure 7

An in-depth implementation Conceptual Framework of an enhanced Secure Distributed Ledger Interoperability Framework for Medical Systems



2.11 Research Gaps

The existing medical interoperability frameworks lack structural interoperability for dealing with data syntax and standardization of data formats and protocols. Structural interoperability arises with the issue of standardizing the syntax, data formats and protocols that can be universally used to link all medical systems and enable secure data exchange across medical systems. Semantic interoperability requires usage of common models and codification of the medical data, using data elements with standardized definitions and meanings. This is depicted in the summary table of the research gap illustrated in Table 3.

Table 3*Summary Table of the Research Gaps*

S.No.	Framework Name	Strengths	Gaps / Weakness
1.	Health Level 7 (HL7)	<ul style="list-style-type: none"> • Syntactic standards that supported point-to-point messaging for data exchange across medical systems 	<ul style="list-style-type: none"> • Lacks both structural and semantic interoperability
2.	Fast Healthcare Interoperability Resources (FHIR)	<ul style="list-style-type: none"> • Based on a standardized structure that aids structural interoperability across medical systems 	<ul style="list-style-type: none"> • Lacks common secure mechanism to ensure patients privacy. • Inability to bridge patients' identity across different medical systems • Lacks endpoint locator authentication and detection.
3.	European eHealth Interoperability Framework (EIF)	<ul style="list-style-type: none"> • Supports organizational interoperability by improving governance. • Establishes cross-organizational relationships • Ensures adherence of existing and new legislation 	<ul style="list-style-type: none"> • Lacks structural interoperability to deal with data syntax and the standardization of data formats and protocols
4.	Refined eHealth Interoperability Framework (ReEIF)	<ul style="list-style-type: none"> • Supports legal and organizational interoperability 	<ul style="list-style-type: none"> • Lacks the structural interoperability

Some of the medical interoperability standards and frameworks include the Health Level 7 (HL7) standard, FHIR, European eHealth Interoperability Framework (EIF) and Refined eHealth EIF (ReEIF) which is an extension of the new EIF. HL7 sought to enable data exchange via the creation of syntactic standards which supported point-to-point messaging. HL7 challenges arise from the way the standard was interpreted and

implemented affecting both the structural and semantic interoperability (Braunstein, 2018).

FHIR is based on a standardized structure for data organization and interpretation by different computer systems or applications (STU, 2018). FHIR has mainly been able to address the structural data exchange formatting and semantics interoperability but it does not address the patient data privacy and confidentiality to aid secure interoperability. EIF and ReEIF supports both legal and organizational interoperability. Legal interoperability ensures that the organizations that are operating under different legal standards, frameworks, policies and strategies are able to work together.

Organizational interoperability ensures alignment and conformity of business processes, public administrations responsibility and exceptions to aid different organization in achieving mutual beneficial targets and goals (Katehakis & Kouroubali, 2019). According to Kouroubali and Katehakis (Kouroubali & Katehakis, 2019), both European eHealth Interoperability Framework (EIF) and Refined eHealth EIF (ReEIF) frameworks face structural interoperability challenge in dealing with the data syntax and the standardization of data formats and protocols.

As a result, lack of secure interoperability in existing medical interoperability framework makes it hard for medical systems to securely exchange medical data. This implies that the current medical systems operate in isolation using centralized databases with varying structural and semantic formats and protocols. These are associated with knowledge void that exist within the medical system development architectural structural and semantic interoperability issues. Hence, there is need for an enhanced secure distributed ledger interoperability framework for medical systems that would address security and interoperability challenges.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter explains the research design and research methodology used in this research. It also outlines the location of the research, population, sample and the sampling techniques applied in the research. The chapter also outlines the instrumentation, data collection procedures, data analysis, presentation techniques used and ethical consideration.

3.2 Research Design

A research design is a plan to answer research questions. While a research design provides an appropriate framework for a study, a research method is a strategy used to implement that plan through addressing the research objectives (Thwaites, 2020). The study followed a mixed methods research design which included the quantitative research methods and qualitative research methods, to aid a comprehensive understanding of the research problem and to meet the study objectives. Systematic literature review was used to explore and synthesize the factors that affect interoperability between medical systems. A descriptive study was conducted in form of a survey in order to establish factors that affect secure medical systems at all the interoperability levels. Appropriate experimentation techniques were employed to meet the remaining objectives of the study. The details of these research designs are explained in the subsections that follow and a summary of the methodology chapter is provided in the Table 4.

3.2.1 Summary of the Methodology and Research Design

This section explains the summary of the research design and method, study location, population, sampling procedure and the sample that the study adopted. The instrumentation, including the pilot study, validation and reliability of the instruments that were used in the study are also discussed. Data collection procedures, analysis, presentation and the ethical considerations are articulated, on top a summary of the methodology is shown in Table 4.

Table 4*Summary Table of the Methodology and Research Designs*

Objective	Research Question	Data Source	Collection Method	Analysis Method	Output
To establish the factors affecting secure interoperability of medical systems	What are the factors that are affecting medical systems structural and semantic interoperability levels?	<ul style="list-style-type: none"> • Literature • Software • Developers 	<ul style="list-style-type: none"> • Systematic Review • Integrated Review • Survey 	<ul style="list-style-type: none"> • Thematic Analysis • Descriptive (Non-Parametric Analysis) 	<ul style="list-style-type: none"> • Specification Metrics
To design a DLT based architecture and algorithm of structural and semantic interoperability framework for secure medical system	How will the DLT based architecture and algorithm of structural and semantic interoperability framework be designed to secure medical systems?	<ul style="list-style-type: none"> • Semantic and Structural Specification Metrics from Objective 	<ul style="list-style-type: none"> • Observation • Function Oriented Design (FOD) technique 	<ul style="list-style-type: none"> • Experiment 	<ul style="list-style-type: none"> • Architecture Design • Algorithm Design
To develop a DLT based structural and semantic interoperability framework for secure medical data exchange	How will the structural and semantic interoperability framework be developed to aid secure data exchange between medical systems using DLTs?	Design Specifications from Objective two	<ul style="list-style-type: none"> • Coding using Agile software development method 	<ul style="list-style-type: none"> • Experiment 	<ul style="list-style-type: none"> • Prototype
To validate the developed DLT interoperability framework at structural and semantic levels for secure medical data exchange	How empirically valid is the developed DLT interoperability framework at structural and semantic levels for secure medical data exchange?	<ul style="list-style-type: none"> • Prototype • Software • Developers 	<ul style="list-style-type: none"> • Simulation Data • Delphi Method 	<ul style="list-style-type: none"> • Simulations 	<ul style="list-style-type: none"> • Validated Framework

3.2.2 Systematic Literature Review

The systematic literature review was conducted to establish factors that affect interoperability of the existing medical systems, hence affecting the security of electronic medical records. Extensive document reviews and analysis was conducted to identify various standard medical systems vocabularies, linking elements, transfer policies as well as crucial guidelines and policies governing the operation of the medical systems. Similarly, the medical systems entities were explored to identify their weaknesses, and to inform the interoperability levels issues and implement the suggested recommendations.

3.2.3 Descriptive Study

Further, to supplement the established factors, a descriptive survey research design was used to gather facts from the domain experts, who are the medical systems software developers; and to describe the existing medical systems architectural layouts and technical characteristics of medical systems interoperability levels which in turn helped the researcher to uncover new interoperability facts and meanings. The survey primarily targeted to address the security and interoperability of the medical systems used in the healthcare industry. The results from the survey were used to inform the design and development of the enhanced secure distributed ledger interoperability framework for medical systems.

3.2.3 Experimental Set-up

Experimental research design was applied in the design development and validation process of the developed enhanced secure distributed ledger interoperability framework for medical systems. The choice of this research design is founded on its capacity to allow to the researcher analyze prior achievement of the developed frameworks in order to establish an equivalent solution for the study and validate the developed framework

(Suciu et al., 2018). For purposes of clarity, the design techniques used in the experimental set up are presented in three-fold. First, the function-oriented design method in section 3.2.5 explains the design of DLT based architecture and algorithm for secure interoperability. Second, the development methods and approach used for the developments of Medical DLT based interoperability framework is presented in 3.2.6. Finally, the validation process is described in 3.2.7.

3.2.4 Framework Design Technique

The system was designed using a function-oriented design (FOD) technique. Function oriented design is a software design technique in which a software model is decomposed into small sets of interacting modules or units where each of these modules or units have clearly defined functions (Fernandez et al., 2000). During system analysis, functional needs were discovered, and the FOD method was used to further clarify those requirements and break down the design into sets of interacting units, each with its own clearly defined purpose.

The system's approach to managing data flows among processes, nodes, and entities is illustrated via dataflow diagrams. To describe the system flow, a system sequence diagram to depict the data flows between the primary actors is used. The system's features via use case diagrams has been modelled. This helped the researcher to identify and categorize system players independent of use cases.

3.2.5 Framework Development Setup

The study used different components to simulate the developed enhanced secure distributed ledger interoperability framework prototype, which helped in achieving secure interoperability functionalities of medical systems. These components are the distributed ledger module, interoperability gateway service module, WireGuard based

Virtual Private Network(VPN) Module and End-User Electronic Medical Record (EMR) Plugins explained in the subsequent subsections.

i. Distributed Ledger Module

This is the main distributed ledger software that securely encrypts using asymmetric encryption algorithms, validates, and stores data (e.g. patient health records, employees, etc.). This Module leverages the core concepts of most popular DLTs, such as Blockchain and use of interplanetary file system (IPFS) which is a distributed system for storing and accessing files, websites, applications, and data. IPFS is based on a protocol hypermedia and file sharing peer-to-peer network for secure sharing of data. Hashing algorithms have also been used to provide integrity of the stored electronic medical records. For demo purposes and to avoid the reinvention of the wheel, the study used Ethereum programmed using solidity programming language for the distributed ledger component in the demo system. At a high scale usage, the distributed ledger contains structured modules for different health information types, for example, Patients service, Medical Doctors service, Picture Archiving and Communication system (PACs) service, Insurance service, and Healthcare providers' service, among others.

ii. Interoperability Gateway Service(IGS) Module

To facilitate a guided high-level integration with the different HISs, this module is a software service & component that acts as a middleware that takes control of information WRITE or READ operations from the distributed ledger. This service contains core encryption algorithms and sits at the top of the distributed ledger module. The IGS contains authentication and peer (node) identity information in the network. It offers a RESTful Application Programming Interfaces (API) service for independent integration by disparate medical information systems.

iii. **WireGuard based Virtual Private Network(VPN) Module**

WireGuard is an open-source Virtual Private Network (VPN) tool that uses state-of-the-art cryptography, like the Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF, and secure trusted constructions. It makes conservative and reasonable choices and has been reviewed by cryptographers, End-User electronic medical record (EMR), API & Plugin(s), Distributed Ledger Module, VPN Module, and Interoperability Gateway Service.

The VPN module dealt with the threat of middlemen and facilitates secure communication of peers over a public network. This module configures a virtual private network in the peer (node). It also stores a copy of its public key for identity by the private network. All peers (nodes) in the network store a copy of their own Public Key and identity information which is used for authentication by the network. The distributed ledger module is in charge of securely issuing of a copy of keys for each peer joining the network.

iv. **End-User Electronic Medical Record (EMR) Plugins**

Since different medical information systems used are unique and separately developed, End-User Electronic Medical Record (EMR) Plugins are generic modules that can be integrated into any generic EMR that they're designed for. This Plugin is a high-level consumer of the application programming interface (API) module that is exposed by the Interoperability Gateway Service that is running in the local node, that is, the peer in which it is installed.

v. **Demo Setup**

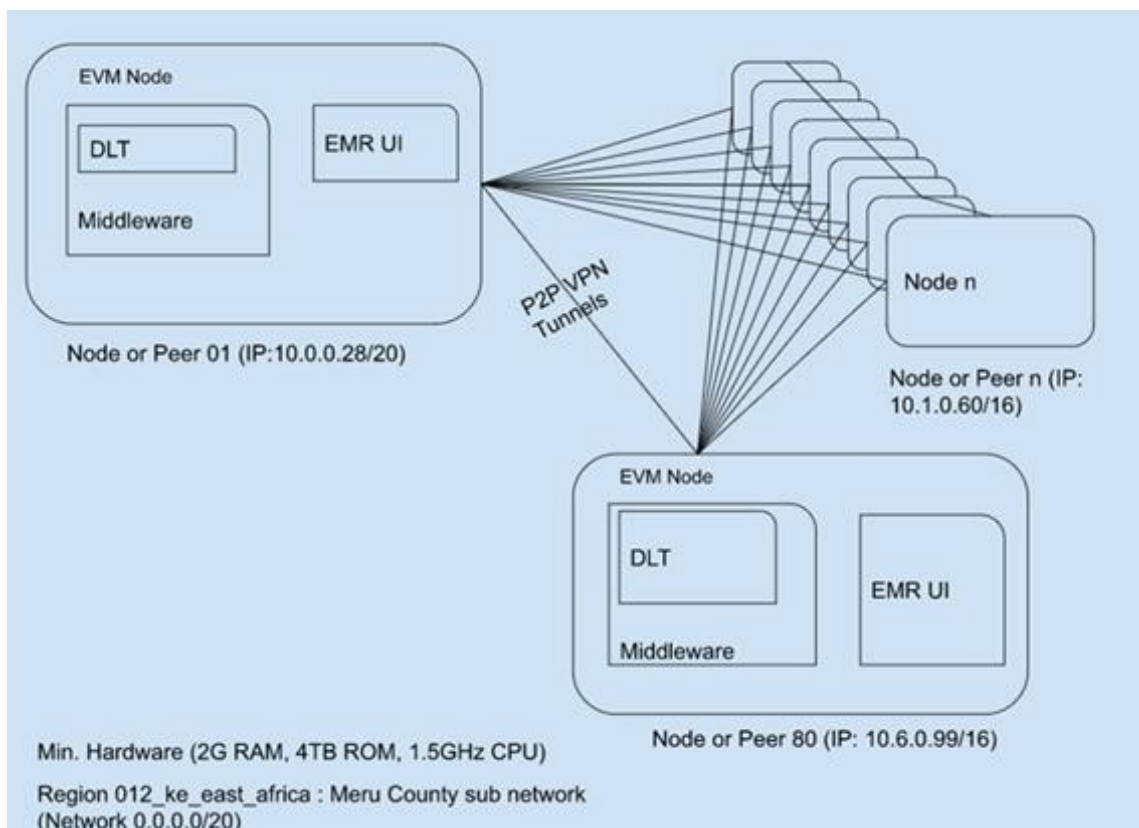
Simulation of functioning hospital systems that demonstrate the medical information systems interoperability framework developed has the system architecture layout shown in figure 8 and network gateway layout as illustrated in figure 9.

a. System Architecture Diagram

The high-level view system architecture diagram setup of the developed interoperability framework showing components, gateway and nodes of the system that was developed is shown in Figure 8.

Figure 8

System Architecture Diagram

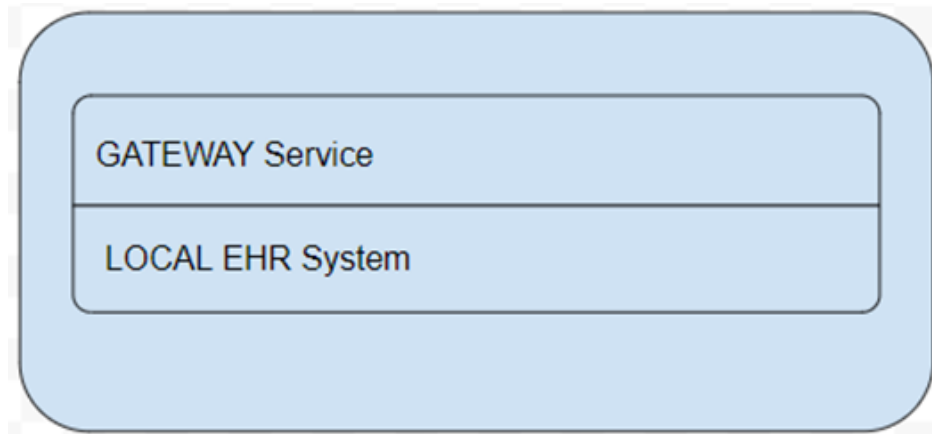


b. Network Gateway Diagram

Connecting two networks or systems that employ different transmission protocols is the function of a gateway (Kuo&Kuo, 2017). Gateways are the entry and exit points for a network, as all data must travel through or communicate with the gateway prior to being routed as shown in Figure 9.

Figure 9

Network Gateway Diagram



3.2.6 Interoperability Framework Validation

Having developed the framework prototype using the analysis results obtained from analysis of documents, interviews with domain experts, questionnaire to the medical software developers and also informal discussions was used. The Delphi method of validation was employed in which domain experts were questioned in a set of questions after being exposed to the developed framework. The empirical data collected was statistically analyzed to ascertain the degree of validity of the developed interoperability framework. Further, experimental results were presented from the simulated scenarios involving select medical systems.

3.3 Location of the Study

The study considered the target population, also known as the theoretical population, as the medical system software developers who are the domain experts from the whole world whom the results of the study were generalized as indicated by Qureshi, (2018). Additionally, the study population, which is also known as the accessible population, used as the actual sampling frame from which purposive sampling was used to sample the medical systems developers in Kenya. (Qureshi, 2018).

The study considered the medical systems architectural requirements at structural and semantic interoperability levels. The developed enhanced secure distributed ledger interoperability medical systems prototype was simulated following the FHIR standard and medical DLT EMR as an enterprise medical system which was used to simulate different medical systems used in case scenarios. The findings were used to guide the development of the enhanced secure distributed ledger interoperability framework for secure electronic medical records exchange.

3.4 Population of Study

The term target population is used to describe a subset of a larger population used in the study in order to generalize findings to the larger population. (Kothari, 2004). The target population of this study was the medical systems software developers in the world. The criteria for inclusion in the study was the specific staff in the targeted medical systems software developers' companies drawn from the sample frame or the accessible study sample which entails the medical system developers in Kenya. These medical systems developers are the domain experts who are directly involved in the design and development of these medical systems of interest at all levels of interoperability.

3.5 Sampling Procedure and Sample Size

The sampling frame included all the medical system software development companies in Kenya. Multistage cluster sampling procedure was used to select medical system software development companies in Kenya to be included in the study. The second stage entailed sampling medical systems software development companies. Finally, purposive sampling was used to sample medical system software developers as the domain experts who are involved directly with the analysis, design and development of these medical systems.

The process of identifying the medical systems and the staff to be interviewed was done through snowballing sampling technique. Snowballing sampling technique also known as chain referral sampling or network sampling, is a non-probability sampling technique used in qualitative research. It involves identifying initial participants who meet specific criteria and then asking them to refer other potential participants who also meet the criteria. Snowballing process was applied to help the researcher identify the specific vendors of medical systems software development companies that were developing and installing medical systems software in the healthcare institutions in Kenya. According to the medical review report of 2021 by the ministry of Health (MoH, 2021) an initial list of seventeen (17) medical systems were identified. A further consultation with the Kenya Health Informatics Association (KeHIA), Ministry of Health staff and other healthcare stakeholders were used to get a more up-to-date list of medical systems.

The study focused on these seventeen (17) major medical systems vendors in Kenya and selected two developers from each of the vendors who develop medical systems that specifically dealt with system analysis, system design, coding or programming, deployment or installations, user support and system management. The seventeen (17) medical systems software development companies sampled were Med 360, Coretec, Appkings Solutions, Forties Innovation, Medbook, Intellisoft Consulting, Shimba Technologies, DSL Systems and solutions, Mito Mhealth Solutions, Dynasoft Business Solutions, Abno Softwares International LTD, Neutek Systems and Solution, IlaraHealth, DocCareHealth, Tripple software, Corebase Solutions and Hanmark Technologies. A total of 34 respondents, two from each of the sampled and selected 17 medical system software development companies were included in the study.

3.6 Instrumentation

The study was carried out using informal discussions, observation, documents inspection, questionnaire and interviews. The data collected was used to analyze the current medical systems interoperability levels architectures, and came up with requirements of the developed interoperable medical system, so as to determine the usability of the enhanced secure distributed ledger interoperable medical system developed.

3.6.1 Pilot Study

The reliability of the instrument that was used for this study was ascertained by conducting a pilot study at two of the identified medical systems software development companies in Kenya that is Aphicons Ltd and TambuaHealth Ltd. The two medical system software companies were used for the pilot study as a results of resource feasibility in terms of resource constraints, time limitations, and logistical considerations. During the pilot study, the questionnaire was tested by distributing it to ten (10) respondents from the two sampled medical systems software development companies. In which five (5) respondents from each of the two (2) pilot study company were purposively sampled resulting to a total of ten (10) respondents and used as the pilot study accessible sample. The results from the pilot study showed that the respondents had experience in development of medical systems for both public sector and private sector. The respondents also indicated that the design and development of medical systems does not differ for clients from either the public sector of private sector, hence necessitating the revision of the questionnaire question that sort to understand if the respondents had developed medical systems for public sector agencies or private sector companies.

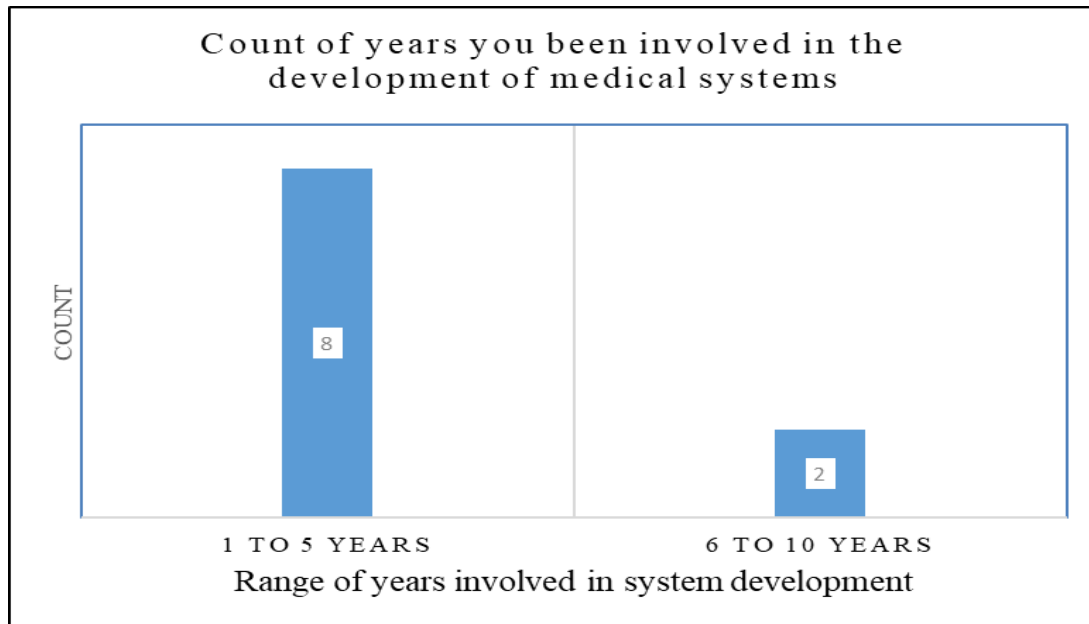
The research questions were drafted in a questionnaire and then sent to the selected medical systems software development companies via google form to test the extent to which the respondents could understand and answer the respective questions without strain. Some of the area that the questionnaire focused on were the years of experience in medical systems development, whether the developers had developed medical systems for the public and private sector, the focus of software development of their companies if they developed medical systems or other types of systems. The questionnaire further sort to understand if the respondents had knowledge on the standardization of medical systems. The pilot study sort to understand if the respondents had knowledge on the medical systems regulations, standards and protocols that are required to be adhered to when developing medical systems. The knowledge on interoperability of medical systems and the factors hindering interoperability of medical systems was also sort by the pilot study. Results from the pilot study have been discussed in details in the subsequent subsections.

3.6.1.1 Years of Experience in Development of the Medical Systems

The respondents were required to indicate the number of years they have been involved in the design and development of medical systems. The findings are summarized in figure 10.

Figure 10

Years of Experience in Development of the Medical Systems



The pilot study revealed that most of the respondents, approximately 80%, had 1 to 5 years of experience in developing medical systems. The study found that most of the organizations targeted fresh graduates from various universities within and outside the country due to the need of programmers who are fully available and able to work for long hours with less commitments and engagements. Understanding the years of experience is vital as it helps in determining how it affects quality assurance, innovation and invention, and risk mitigation hence the question was retained in the questionnaire.

3.6.1.2 Design and development of Medical Systems for Public or Private Sector

All the respondents responded that they were involved in design and development of medical systems for both private and public institutions. Hence it was clear that the results had no impact in the study and did not affect or influence the architectural designs of medical systems. This question was later restructured to allow the respondents to record the software organization name from which they are doing the design and

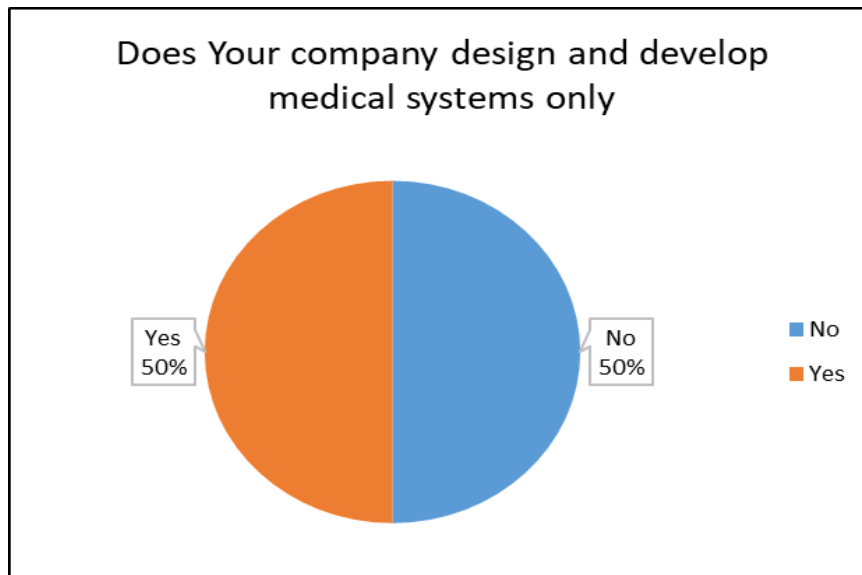
development of the medical systems instead of the type of their clients if they were from public or private sector in the actual research questionnaire.

3.6.1.3 Type of Information Systems Developed

The study also sought to discover whether the developers had a focus on the development of medical systems only or other types of information systems. The response findings are in Figure 11.

Figure 11

Type of Information Systems Developed



The results revealed that the two companies were involved in developing of medical systems with a response rate of 50%. This response shows that it was necessary to retain the questionnaire questions on the type of information systems that were being developed by the sampled medical systems software companies.

3.1.6.4 Knowledge on Standardization of Medical System's

The response from the pilot study on rating the level of knowledge on standardization of medical systems, the structural data formats, syntax, and organization of data exchange and rating the level of standardization of the medical systems' semantic standards,

codifications, and protocols was not sufficient to respond to the research questions and objectives of the study. Hence the questions in the questionnaire were restructured to explore the awareness of the respondents on the standards, frameworks and protocols, level of interoperability in medical systems.

3.1.6.5 Knowledge on the Medical Systems Regulations, Standards and Protocols

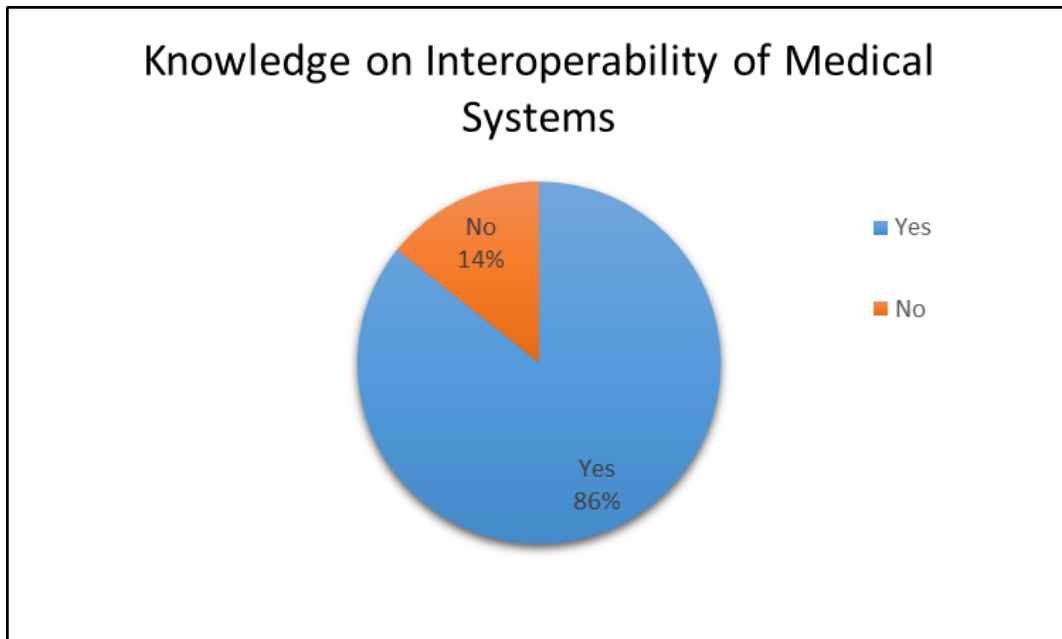
The pilot study sort to understand if the respondents had knowledge on the medical systems regulations standards and protocols that are required to be adhered to when developing medical systems. All the respondents indicated that they were aware of the World Health Organization's regulations and they also indicate that they adhered to Health Insurance Portability and Accountability Act of 1996 (HIPAA) standard and the Kenyan data protection act of 2019 in the design and development of medical systems process. This response indicated that it was necessary to retain the questions on medical systems regulations, standards and protocols.

3.1.6.6 Knowledge on Interoperability of Medical Systems

The pilot study further sort to understand if the respondents were aware of interoperability of medical systems. The findings revealed that 86% of the respondents have knowledge on interoperability of medical systems and 14% of the respondents had no knowledge on interoperability of medical systems. This response shown that it was necessary to retain the questionnaire questions on knowledge and awareness of interoperability of medical systems as shown in Figure 12.

Figure 12

Knowledge on Interoperability of Medical Systems



3.1.6.7 Factors Hindering Interoperability of Medical Systems Was Also Sort by the Pilot Study

The respondents indicated that some of the factors hindering interoperability of medical systems includes structural, semantic, security and technical factors. The response from the respondents shown that it was necessary to retain the questions on the factors hindering of interoperability of medical systems by the medical systems developers.

3.6.2 Validity of the Instrument

The validity of a study is measured by how well it captures the phenomena of interest (Mohajan, 2017). A simulation depicting the type of transaction that takes place between two separate participants in the system was carried out to verify the study. The hash of the transaction mined on the system is also essential to the system's integrity. The study's proof-of-concept prototype was validated with the help of professional reviews from Medical Software Developers.

3.6.3 Reliability of the Instrument

The degree to which outcomes are repeatable is called reliability. Reliability refers to the extent to which a study's findings are representative of the population at large, while validity refers to the ease with which a study's findings may be replicated using the same procedures (Taherdoost, 2018).

The test-retest reliability technique was used to establish dependability in this study. The test-retest reliability approach involves giving the same test twice to the same set of people at different times. It is possible to assess the test's stability over time by correlating the results from Time 1 and Time 2. Then, a coefficient of stability, or test-retest coefficient, is calculated. The dependability coefficient in this case is calculated by comparing the Pearson product-moment correlation between the same individuals' test scores from both occasions. The Pearson Correlation Coefficient is used to determine test-retest consistency; its value can range from -1 to 1, with -1 indicating a perfectly negative linear correlation between two scores, 0 indicating no linear correlation between two scores, and 1 indicating a perfectly positive linear correlation between two scores (Vilagut, 2014). Since reliability was established, the researcher went forward to carry out the investigation.

3.6.4 Reliability and Validity Test Analysis Results

The internal consistency and reliability of the measurement scales employed in the questionnaire were evaluated by reliability analysis. "N of items" represented the number of variables derived and coded from the questionnaire. To test for reliability of the questionnaire that was used for data collection, "N of items" was picked at 16 variables out of 23 total variables. These variables were the variables relating to different facets of system architecture, interoperability, and security, Cronbach's alpha coefficient was

calculated. The reliability of the scale was determined by the Cronbach's alpha coefficient, which measures how strongly each variable's items connect with one another.

Table 5

Reliability and Validity Test Analysis

Reliability Statistics	
Cronbach's Alpha	N of Items
.819	16

The fact that these variables all have constant Cronbach's alpha coefficient values of 0.819 means that each variable's items measure a valid and consistent construct as shown in table 5. These results support the internal reliability, hence supporting the validity of the survey instrument used to evaluate the opinion of the domain experts; and implied that the replies were reliable in expressing the notions that were intended.

3.7 Data Collection Procedure

Quantitative and qualitative data was gathered through the use of questionnaires and semi-structured interviews respectively from medical software developers who serve as domain experts. From the literature review, the survey questions were generated. The researcher gained a better grasp of the research problem and the requirements and constraints of the current medical systems after analyzing the survey responses. Both the Institute of Postgraduate Studies at Kabarak University and the National Commission for Science, Innovation, and Technology (NACOSTI) endorsed and approved the research proposal before any data was collected.

3.8 Data Analysis and Presentation

Data was analyzed in an exploratory fashion to draw parallels between previous efforts and the ways in which distributed ledger technologies are being used today to improve healthcare. Further, analysis of data generated insights on the trends to improve current distributed ledger technologies.

An enhanced secure distributed ledger interoperable medical system prototype was developed and the simulated results from the demo was used to guide the development of the framework. A clear documentation of the results was generated and explained.

3.9 Framework Evaluation and Validation

The evaluation of the developed enhanced secure distributed ledger interoperable framework for medical system was through development of a Medical DLT prototype following a defined architectural layout. After development of the prototype, the Delphi method was used to validate the different security, privacy and interoperability parameters like authentication of users, levels of authorization, access control, encryption, hashing, signing and ability to securely exchange patient EMR across different health facilities. Delphi method involved collecting opinion and feedback in several rounds from the medical system software developers who are domain experts. This was done in secret to promote objective answers to the validation and evaluation of Medical DLT system prototype. To reach consensus various parameters were considered, these parameters were usability, security and privacy, access control, authentication and authorization, interoperability and adherence to healthcare standards. The domain expert opinions were gathered and distilled using the structured and iterative Delphi technique. The results obtained from the delphi method are as shown in chapter 4 sections 4.5.4.

3.10 Ethical Considerations

During the data collection processes and the framework testing procedures, several ethical considerations were adhered to due to the sensitivity of both the patients' medical data and the medical systems that were involved in the development of the medical system prototype. The researcher adhered to all ethical requirements by the regulating authorities. Data was collected from the sampled medical software developers after seeking consent and approvals from the sampled institutions. This was done after obtaining an introductory letter from the institute of postgraduate studies of Kabarak University and also a research permit from the National Commission for Science Innovation and Technology (NACOSTI), as stated in Appendix 1. The information obtained from the respondents was treated with utmost confidentiality so as to uphold respondents' self-esteem and respect. Since patient's medical data is private and a proprietary, strict adherence to code of ethics in data management was also maintained.”

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents the findings of the study, analysis, interpretations and discussion of the findings, organized as per the research objectives and questions indicated in chapter one. It also presents the general information as provided through the domain experts' responses who were the medical systems software developers. The objective of this study was to bridge the gap between the pressing need for seamless data sharing throughout the healthcare ecosystems, and the quickly evolving field of medical technology. The study examines a wide range of security procedures, interoperability awareness and alignment with healthcare objectives concerns, in an effort to provide light to the complicated nature of secure medical system design.

The findings that relate to each of the four research objectives have been presented. Objective one sought to establish factors affecting secure interoperability of medical systems; objective two aimed to design an algorithm to enhance security of DL interoperability framework for medical systems; objective three sought to develop a secure DL interoperability framework for improving the security of medical data exchange between medical systems; while objective four aimed to validate the developed secure distributed ledger interoperability framework for secure medical data exchange have been presented.

4.1.1 General Information

A mixed research design incorporating systematic literature review, descriptive study, experimentation techniques and prototyping was employed in the study with the purpose of developing an enhanced secure distributed ledger interoperability framework for

medical systems. Descriptive survey was used to gather facts from the medical systems software developers who are domain experts involved in analyzing, designing and developing medical systems software, via online questionnaires and semi-structured interview schedule. To analyze the collected data IBM SPSS statistics version 28 and Microsoft Excel statistical tools were used. For qualitative data analysis MAXQDA tool was used to analyze data. The results are presented in tables, frequency tables, graphs and charts.

4.1.2 Systematic Literature Review Results

The study used systematic literature review research design to answer the first objective that sought to establish the factors affecting secure interoperability of medical systems.

4.1.2.1 Research Questions Addressed RQ

To conduct the systematic review the study formulated a research question “what are the factors that are affecting secure interoperability of medical systems at different interoperability levels?” that aided in understanding the subject matter.

4.1.2.2 Inclusion and Exclusion Criteria

This literature review only includes research that address the issue of interoperability of medical system at different interoperability levels. Additionally, studies on the application of DLTs by the medical systems in healthcare sector and the studies from the years 2017 to 2023 are the ones included for the review. Review type research, discussions, uses and applications of DLTs in other sectors, non-relevant publications and any work that are not empirical were excluded.

4.1.2.3 Data Sources

The literature review included the review of ten electronic databases and electronic libraries. The libraries reviewed include; IEEE Xplore, Google Scholar, PubMed –

NCBI, Elsevier Science Direct, Mendeley, PNAS, Springer link, Web of Science (WoS), Medline EBSCO, and ACM Digital Library. The researcher conducted the advanced search for the relevant publications from the electronic libraries and databases using the query string(s) defined: “(Distributed ledger OR Distributed Ledger Technologies OR “DLTs”) AND (medical systems OR healthcare OR eHealth OR e-health OR health* OR health systems* OR medical information systems OR *health information systems* OR medical)”.

The researcher constructed the search string based on the research domain and the defined research question. Due to a lack of advanced search options for some libraries and databases like Google Scholar, Mendeley, PNAS and Springer Link, they returned many non-related results that were not meeting the inclusion - exclusion criteria. Therefore, the researcher only included the first 100 most relevant results from these four databases. This search in the online digital libraries was conducted in January 2023. The researcher intentionally made the search query as broad as possible in order to consider as many results related to the systematic research questions as possible. The summary of the search in all databases and libraries returned 4777 results and the results returned for each database search are presented in Table 6.

Table 6*Summary of Search Results*

Database / Library	Number of Results	Number of results suitable after detailed screening
IEEE Xplore	17	10
Google Scholar	3562(100)	12
PubMed – NCBI	30	5
Elsevier Science Direct	18	8
Mendeley	167(100)	7
PNAS	202(100)	2
Springer link	745 (100)	1
Web of Science (WoS)	10	2
Medline EBSCO	20	4
ACM Digital Library	6	1

4.1.2.4 Selection of Studies

The selection process started with 501 publications gathered from online digital databases and digital libraries. Based on the inclusion-exclusion criteria, the publications were either included in the review or not and a total of 52 papers were reviewed. The researcher was interested in how the distributed ledger technology (DLT) is used in providing secure interoperability of medical systems in the healthcare sector and finding out the factors that affect secure interoperability of medical systems at different interoperability levels.

4.1.2.5 Systematic Literature Review Findings

The findings on factors affecting secure interoperability of medical systems in the healthcare sector revealed that structural, semantic, security and technical factors are among the factors affecting secure exchange of electronic medical records (EMRs) across different medical systems. The results are summarized in Table 7.

Table 7*Summary of Systematic Literature Review Results*

Broad Factors	Specific Factors	Literature Sources	
Structural Factors	Architecture of networks	(Rahmani et al., 2018),(Uddin et al., 2018) and (Budman, 2021)	
	Viability and scalability	(Mishra et al., 2023) and (Emergen Research, 2022)	
	Application programming interfaces (APIs) and data integration	(Torab-Miandoab et al., 2023),(Panda et al. 2023) and (Juárez et al., 2022)	
	Data protocols and standards	(A. Singh & Chatterjee, 2020) and(Acuña Ulloa &Cabanillas Castillo, 2022; AlQudah et al., 2021)	
	Data Policies and governance	(Truong et al., 2020), (Torab-Miandoab et al., 2023) and(Ajayi et al., 2020)	
	Infrastructure and hardware	(Andoni et al., 2019) and(Andrew et al., 2023).	
	Semantic Factors	Data formats and semantics standardization	(Mehta et al., 2020),(Kotey et al., 2023; Szarfman et al., 2022), (Colombo et al., 2020; Elvas et al., 2023), (Brogan et al., 2018; García et al., 2020), (Haque et al., 2022; N. Kuo, 2015; Moon et al., 2020) and (AlQudah et al., 2021; Institute, 2020; Muinga et al., 2020).
		Data mapping and ontology	(de Mello et al., 2022; Haque et al., 2022), (Belmonte & Ot, 2021; E. Li et al., 2021; Schulz et al., 2018) and(Belmonte & Ot, 2021; de Mello et al., 2022; Schulz et al., 2018; Torab-Miandoab et al., 2023).
		Semantic harmonization	(de Mello et al., 2022; Torab-Miandoab et al., 2023), standardization (Eklund, 2019; Health Act, 2017) and (Kim et al., 2020).
		Consents and permissions for data sharing	(Abernethy et al. 2022), (Truong et al., 2020; Zheng et al., 2018),(Savage & Savage, 2020; Torab-Miandoab et al., 2023) and (Belmonte & Ot, 2021; Katehakis & Kouroubali, 2019)
Cross-border communication		(Pawczuk et al., 2019), (Seaberg et al., 2021),(June Okal, 2018),(McGhin et al., 2019), (Kouroubali & Katehakis, 2019),	

		(Cohen 2020b), Durneva et al. (2020) and (Torab-Miandoab et al., 2023)
	Semantic risks and cybersecurity	(Dagher et al., 2018; Edemekong & Micelle, 2020), (IBM, 2021),(de Mello et al., 2022),(Yang et al., 2022),(Abernethy et al., 2022) and(Seaberg et al., 2021)
Security Factors	Data encryption	(Elvas et al., 2023) and Seh et al. (2020)
	Management of identity and access	(Arslan et al., 2020; Wang et al., 2022), (Accenture, 2019) and (Eunice et al., 2019)
	Consensus mechanisms in Blockchain	Ibanez and Rua that was published in 2023 and (Ibañez & Rua, 2023)
	Smart contracts and vulnerabilities	Quantstamp study in 2021 and(Dai et al., 2019; Saxena et al., 2021).
	Immutability and data integrity	(Urkude et al., 2021) and (Liang et al. 2023)
	Privacy preserving techniques	(Holweger et al., 2021),Deloitte report in 2021 and(Anthony Jnr, 2021)
	Frequent monitoring and auditing	(Xia et al., 2017) and (Sun et al., 2018)
Technical Factors	Blockchain structures and procedures	(Saeed et al., 2022)
	Mechanisms of consensus	(Hafid et al., 2020) and (Union et al., 2020).
	Solutions for data storage	HIMSS research in 2021, (Onik et al., 2019) and (M. Kim et al., 2020)
	Smart contract development	(Elvas et al., 2023) and (Budman, 2021)
	Standards for interoperability	(Clunie, 2021) and (Ulloa & Castillo 2022)
	Interfaces for application programming (APIs)	(Abernethy et al., 2022).
	Structure and network	(Australia, 2020) and (Anthony Jnr., 2023; Laroiya et al., 2020)

4.1.3 Response Rate

The effectiveness of the data collection strategy can be determined mainly by the response rate. Using a purposive sampling technique, a total of 17 medical systems software development companies involved in the design and development of medical systems were sampled and used for the study. Two medical system software experts

were sampled per company and issued with the online questionnaires. A total of twelve (12) companies with a total of 24 respondents from the 17 medical systems software development companies sampled filled and returned usable questionnaires to the researcher, giving a response rate of 70.6%. The high response rate signifies relevance of the research topic to the participants, and the success of the data collection processes. It also reveals a substantial degree of involvement and willingness of the respondents to participate in the study.

The major reasons for a high positive response by the respondents were attributed to the research questionnaire, which was accompanied with the research permit license number from NACOSTI, the research permission introduction letter by the Institute of Post-graduate studies of Kabarak University, the ethical letter from Kabarak ethics committee, the assurance by the researcher to maintain professionalism, privacy and confidentiality when working with responses from the respondents, the assurance and willingness by the researcher to share the findings and final report with the interested respondents, and the structure of the questionnaire, which was simple, professional and non-ambiguous. Additionally, the response rate provides context for the generalizability of the results to the broader population, and contributes to the overall validity of this study.

4.1.4 Medical System Software Developers Years of Experience

In response to the experience in designing medical systems, the dataset contains details on the respondents' years of expertise in medical system design. The respondents' degrees of experience ranged, with those with 1 to 5 years of experience making up the majority (50.0%), these findings revealed that most of the organizations targeted fresh graduates from various universities within and outside the country. Understanding the years of experience is vital as it helps in determining how it affects quality assurance, innovation and invention, and risk mitigation, this was explained by the need for the

development companies need for those with less engagements since the development of software requires those who are able to code for longer hours without distractions. This was followed by those with 6 to 10 years of experience (33.3%). Only 16.7% of respondents said they had between 11 and 15 years of experience in this field. This distribution shows that both the professionals in their early careers and those with greater experience contributed to the study. A fair representation of a wide range of experience levels among the respondents, was revealed by the findings.

This variability in experience shows that the study includes perspectives from both seasoned experts and up-and-coming experts in the field of medical system design. The range of experience levels produced a broad variety of viewpoints and ideas, adding to the general robustness of the study's findings. These observations assisted in putting the forthcoming studies of security procedures, interoperability, and practical difficulties into context. The detection of trends and correlations between experience and attitudes toward security, interoperability, and system design methods is also made possible by analyzing the respondents' degrees of experience. This link offered insightful information about how best practices change over time and how to adapt them to shifting technology environments.

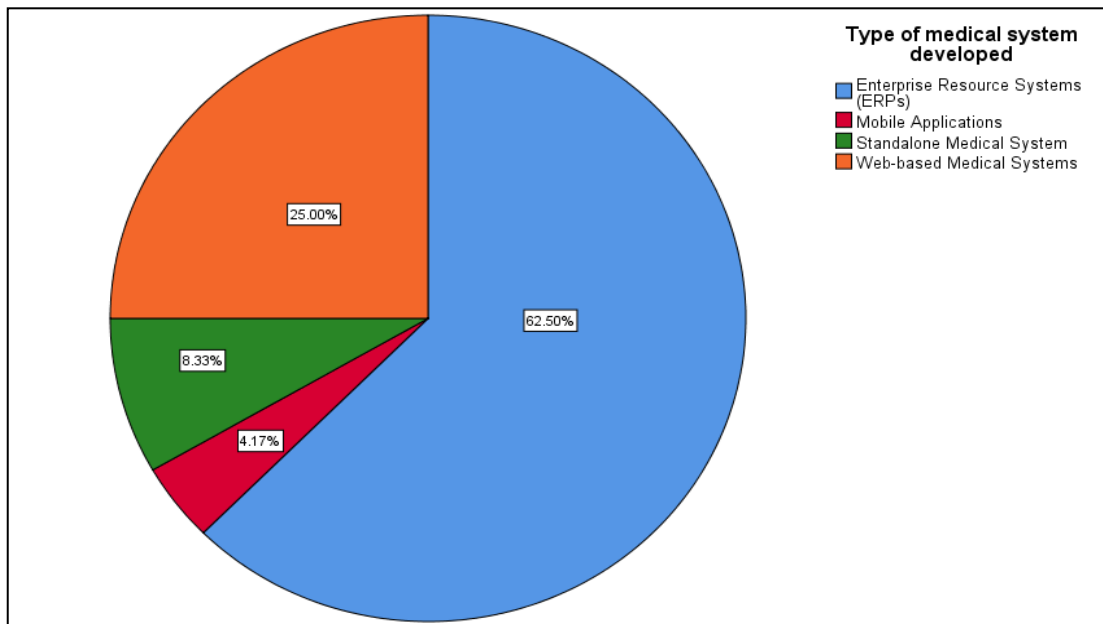
4.1.5 Type of Medical System Developed

The classification of the medical systems developed by the participating medical system software development companies offers insightful information about the emphasis and areas of expertise of the respondents. This information helped the researcher in contextualizing their responses, and to understand how different types of medical systems impact various aspects of design, security, and interoperability. Figure 13 shows some key findings based on the analysis of the type of medical system that was being

developed by medical systems software development companies that participated in the study.

Figure 13

Key findings based on the Analysis Showing Percentages of the type of Medical System Developed by the Medical Systems Software Development Companies



i. Enterprise Resource Systems (ERPs)

A significant portion of the respondents (62.5%) reported that their medical system software company was developing Enterprise Resource Systems (ERPs) in the medical domain. ERPs play a vital role in managing various aspects of healthcare organizations, such as patient records, billing, and inventory management. This indicates that a substantial number of respondents are involved in creating systems that streamline administrative and operational processes within healthcare settings.

ii. Web-based Medical Systems

25.0% of the respondents indicated that their company is involved in developing web-based medical systems. Web-based systems offer the advantage of accessibility and remote usage, allowing healthcare professionals and patients to interact with the system

from different locations. These systems often facilitate communication, data sharing, and patient engagement.

iii. Standalone Medical Systems

A smaller portion of respondents (8.33%) reported designing standalone medical systems. Standalone systems refer to software applications or devices that operate independently and are not necessarily connected to larger network infrastructures. These systems might serve specific medical functions or offer specialized tools. These kinds of systems include clinical decision support system and disease management system.

iv. Mobile Applications

4.17% of the respondents mentioned developing mobile applications tailored to the medical field. Mobile applications play an increasingly crucial role in healthcare by enabling patients and healthcare providers to access information and services on mobile devices. These systems include patient monitoring system, mobile telemedicine system, mhealth based systems among others.

Implications of the diversity in the types of medical systems developed by the respondents highlight the range of applications and functionalities within the medical domain. ERPs, web-based systems, standalone systems, and mobile applications each serve distinct purposes, suggesting that respondents have expertise in various segments of the healthcare technology landscape. Understanding the type of medical systems developed allows for targeted analyses in subsequent stages of the study. The knowledge of the type of the system developed gave the researchers a clear understanding of the security practices applied across different types of system designs, which laid the foundation of understanding the levels of interoperability and the challenges that hinder interoperability of different types of medical systems. By categorizing responses based

on the type of medical systems, the researcher was able to uncover nuances and trends that contribute to a more comprehensive understanding of the intersection between system design, security, interoperability, and practical challenges in the diverse landscape of medical technology.

4.1.6 Security as a Design Requirement

The study sort to explore whether security is considered a necessary requirement during the design phase by the developers. Examining whether security is considered a necessary requirement during the design phase of medical systems is crucial in understanding the approach and priorities of the respondents. Based on the analysis done, the following findings were discovered:

i. Security as a Necessary Requirement

Security is viewed as a vital criterion during the design phase of medical systems, according to the majority of respondents (91.67%). This broad agreement serves as a testament to the fact that security has been given paramount consideration in the design of medical systems. Sensitive medical data and system integrity can be protected and possible risks reduced by designing medical systems that emphasize on security, right from the initial stages.

ii. Security as Not a Necessary Requirement

Security is not seen as a necessary necessity throughout the design phase according to a lesser percentage of respondents (8.33%). It is important to keep in mind that this minority opinion may be impacted by elements such as the particular medical systems' structure, company culture, or perceived risk levels.

The implications of the responses indicate that the respondents' overwhelmingly agreement that security must be a priority during the design process as demonstrated in

their awareness of and attention to security-related issues. This adherence to security best practices is encouraging since it shows that many medical systems software development companies are actively addressing security concerns to protect patient data, adhere to legislation, and uphold system reliability. There may be a number of reasons for the relatively small percentage of respondents who said that security is not viewed as a necessary criterion. This minority response may reflect differing perspectives on security requirements, possible misconceptions about the potential threats, or the assumption that security measures can be effectively addressed post-design. Addressing the viewpoints of this subgroup could provide valuable insights into challenges related to security awareness and implementation. Overall, the findings indicate a strong commitment to integrating security considerations into the design process of medical systems. This commitment is reflective of the evolving landscape of data breaches and cyber threats, where the consequences of inadequate security can be detrimental to both patients and healthcare organizations. The broad recognition of security as a requirement bodes well for the overall security posture of the medical systems being developed by the participating companies.

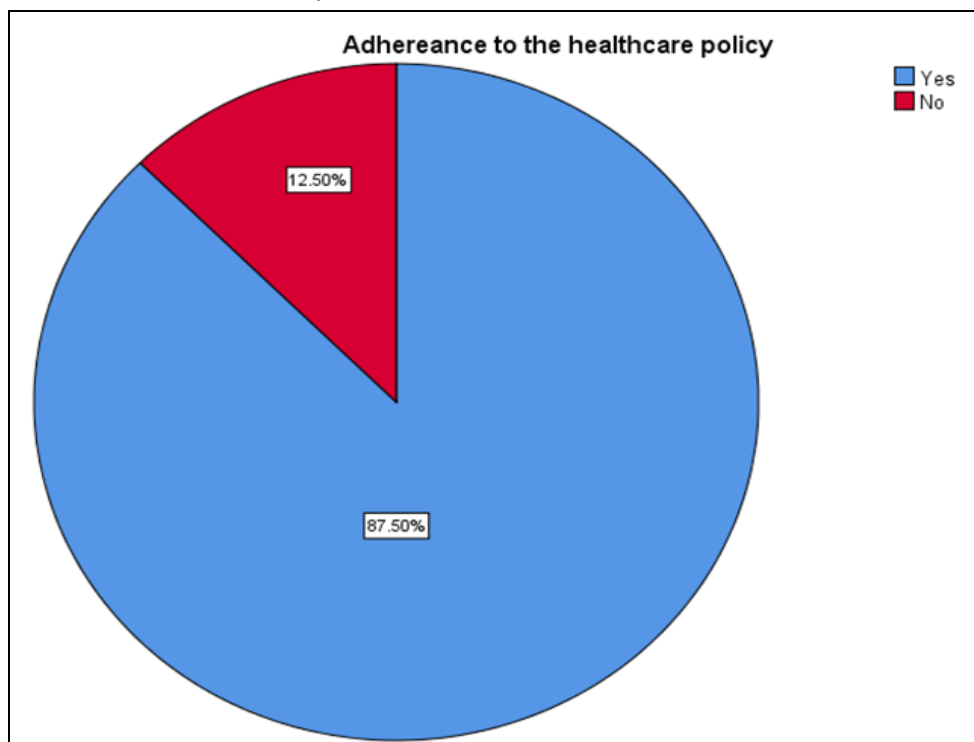
4.1.7 Adhering to Healthcare Design Policy

Understanding if the company adheres to specific healthcare design policies indicates respondents' commitment to industry standards. Exploring whether companies adhere to specific healthcare design policies provides insights into their commitment to industry standards and best practices. The study focused on understanding if the respondents were adhering to policies and standards like, the global data protection regulation (GDPR), Kenyan Data Protection Act of 2019, Health Insurance Portable and Accountable Act of 1996 (HIPAA), HL7 (Health Level Seven), DICOM (Digital Imaging and Communications in Medicine), FHIR (Fast Healthcare Interoperability Resources),

SNOMED CT (Systematized Nomenclature of Medicine - Clinical Terms), CCDA (Consolidated Clinical Document Architecture), OAuth (Open Authorization) and Open ID Connect, XDS (Cross-Enterprise Document Sharing), SMART on FHIR SMART (Substitutable Medical Applications, Reusable Technologies) and NCPDP (National Council for Prescription Drug Programs). This analysis offers valuable information about the extent to which organizations prioritize regulatory compliance and align their design practices with established guidelines. The study revealed the findings depicted in Figure 14.

Figure 14

Adherence to the Healthcare Policy



i. Adherence to Healthcare Design Policy

The data revealed that a significant majority of respondents (87.50%) indicated that their company adheres to healthcare design policies. This significant number shows that the participating businesses place a high value on adhering to rules, norms, and guidelines

specific to their industry. Adhering to healthcare design guidelines makes it possible to guarantee that the created systems meet recognized standards for quality, security, and patient safety.

ii. Non Adherence to Healthcare Design Policy

A lesser percentage of respondents (12.50%) claimed that their business did not follow healthcare design guidelines. This minority opinion may be the result of a number of variables, including organizational size, resource constraints, or particular contextual concerns. To have a thorough grasp of the difficulties and incentives associated with policy adherence, it is crucial to take into account the factors that led to this viewpoint.

The vast majority of respondents who said that their firms follow healthcare design regulations suggest that compliance with these policies indicates a strong commitment to upholding industry standards. This dedication is positive because it demonstrates a proactive approach to ensuring that the developed medical systems meet essential quality and safety requirements. The minority of companies who deviate from healthcare design principles might provide valuable insights into the factors behind this decision. Examining the elements that contribute to this attitude could reveal problems with how resources are allocated, opinions on how applicable the policy is, or possible conflicts between the policy's implementation and other organizational goals. When considering security protocols and interoperability levels with other elements, such as healthcare design policies, a complete grasp of how policy alignment impacts system design and development may be gained. Furthermore, comparing adherence rates across different medical system types and company sizes might reveal disparities within the industry. In summary, the findings emphasize how important it is to follow policy to guarantee that medical systems are designed with quality, safety, and regulatory compliance in mind. The large number of businesses that follow healthcare design guidelines shows a shared

dedication to industry norms and enhances the general legitimacy and dependability of the medical systems under development.

4.1.8 Correlational Analysis

A convincing understanding of the relationship between a company's adherence to healthcare design guidelines and its awareness of interoperability within the context of developing medical systems emerged from the data analysis. Table 8 shows the summary of the correlational analysis.

Table 8*Summary of the Correlation Analysis*

		Correlations				
		Adhering to healthcare design policy	Awareness to interoperability	Sharing information between different healthcare	System have architectural interoperability inbuilt capabilities	The level of interoperability align with the healthcare organizational needs
Adhering to healthcare design policy	Pearson Correlation	1	.655**	.589**	.737**	.507*
	Sig. (2-tailed)		.001	.002	.000	.011
	N	24	24	24	24	24
Awareness to interoperability	Pearson Correlation	.655**	1	.265	.415*	.258
	Sig. (2-tailed)	.001		.211	.044	.223
	N	24	24	24	24	24
Sharing information between different healthcare	Pearson Correlation	.589**	.265	1	.799**	.697**
	Sig. (2-tailed)	.002	.211		.000	.000
	N	24	24	24	24	24
System have architectural interoperability inbuilt capabilities	Pearson Correlation	.737**	.415*	.799**	1	.321
	Sig. (2-tailed)	.000	.044	.000		.126
	N	24	24	24	24	24
The level of interoperability align with the healthcare organizational needs	Pearson Correlation	.507*	.258	.697**	.321	1
	Sig. (2-tailed)	.011	.223	.000	.126	
	N	24	24	24	24	24

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

4.1.8.1 Adhering to Healthcare Design Policy and Awareness to Interoperability:

The statistical results showed a strong positive correlation between adhering to healthcare design policy and awareness to interoperability. These two variables recorded

($r = 0.655$, $p < 0.01$), indicating a meaningful and consistent link. This indicates that organizations that prioritize adherence to healthcare design guidelines often demonstrate a higher level of understanding of interoperability difficulties during the creation of their medical systems. The fact that there is a correlation between adherence to healthcare design policies and increased knowledge of interoperability issues has significant ramifications for the healthcare sector business. Healthcare organizations who prioritize adherence to these regulations not only show a dedication to healthcare industry standards, but also seem to be more aware of the changing interoperability landscape, possibly presenting themselves as industry leaders. The importance of fostering a culture of adherence to healthcare design policies as a means to promote better awareness and integration of interoperability standards within the domain of medical systems development is highlighted by this finding, which offers insightful information for both policymakers and industry stakeholders.

4.1.8.2 Awareness to Interoperability and Sharing Information

An intriguing association has been found between statistics on interoperability awareness and the inclination to share information among various healthcare systems. Although there is a positive correlation, it is only moderately significant ($r = 0.265$, $p < 0.05$), indicating that there is a relationship between these factors that is both discernible and not overly strong. This research suggests that healthcare organizations with stronger awareness of interoperability principles have a greater propensity to share information across various medical systems.

The significance of this link resides in the understanding it offers to the dynamics of information sharing and interoperability in the healthcare industry. Although not a strong association, it shows that healthcare organizations are more likely to appreciate the advantages of seamless information interchange among medical systems as they become

more aware of the complexities of interoperability. This insight might help the healthcare sector to collaborate more effectively, provide better patient care, and streamline procedures. Despite the fact that the association is not particularly strong, it emphasizes the value of fostering interoperability awareness as a first step toward attaining more effective information sharing procedures among healthcare systems.

4.1.7.3 Sharing Information and Architectural Interoperability

An extensive and highly significant association has been found between the examination of data on information exchange between different medical systems and the availability of architectural interoperability inherent features. In particular, there is a clear positive connection between these two variables ($r = 0.799$, $p < 0.01$). This finding highlights a strong correlation, indicating that healthcare organizations who are eager to share information across various medical systems are also more likely to build architectural interoperability right into their medical systems.

This association has important ramifications. It suggests that a healthcare company's tendency for information exchange and its approach to system design are strategically aligned. The creation of medical systems with built-in architectural interoperability elements is essentially a strategy employed by enterprises that prioritize seamless information interchange throughout the healthcare ecosystem. This alignment might be viewed as a good indication for the healthcare sector since it shows that these healthcare organizations are working together to improve the interoperability of their medical systems, which could result in more effective and integrated healthcare services.

In conclusion, healthcare organizations' strategic synergy is shown in the substantial positive association between information exchange and architectural interoperability. It implies that healthcare organizations are acknowledging the crucial connection between

these two elements and are acting proactively to promote interoperability by design. The advancement of interoperability efforts and, ultimately, an increase in patient care and healthcare system effectiveness are both potential benefits of this correlation.

4.1.8.4 Architectural Interoperability and Organizational Needs

An intriguing but not statistically significant association is found when the relationship between having architectural interoperability inherent capabilities, and the alignment of interoperability levels with healthcare organizational needs is examined. In particular, there is a positive association between these two variables ($r = 0.321$, $p > 0.05$), showing that healthcare organizations with architectural interoperability elements in their systems are likely to have a little better alignment of interoperability levels with their healthcare organizational goals. However, the extent of this correlation's strength is relatively moderate, and it is not statistically significant.

Nonetheless, it is still important to look into the correlation's implications even if it is not statistically significant. This finding suggests that there could be a relationship between medical systems' architectural design and their adherence to the specific needs of healthcare institutions. Investing in architectural interoperability aspects may somewhat boost a business's chances of meeting the interoperability requirements of its multiple healthcare organizations. This is because the absence of statistical significance raises the possibility that there are other variables at play, caution should be used while evaluating this relationship. This finding highlights the difficulty of precisely matching system design to organizational needs in terms of application. Architectural interoperability is one determining element, but it is not the only one, even if it might aid in this alignment. It's likely that there are more organizational, technological, and environmental factors. Consequently, healthcare organizations need to consider a comprehensive interoperability strategy that extends beyond system design. The association between

organizational needs alignment and architectural interoperability is not statistically significant despite optimistic findings, hence the need to address the interoperability problems in the healthcare sector, through more research and analysis of different components.

4.1.8.5 Adhering to Healthcare Design Policy and Organizational Needs

This study has shown a positive and statistically significant relationship between following healthcare design policy and matching interoperability levels to organizational requirements in the healthcare industry. Specifically, these two factors have a noteworthy positive correlation ($r = 0.507$, $p < 0.05$). This research indicates that medical systems that satisfy healthcare organizations' unique requirements and specifications are more likely to be found in companies that emphasize patient care and adhere to healthcare design principles.

This association illustrates the importance of following recognized healthcare design standards, frameworks, and guidelines while developing new medical systems. In addition to ensuring compliance with industry standards, healthcare companies prioritizing adherence to these standards and guidelines demonstrate a commitment to tailoring their medical systems to the unique needs of healthcare organizations. By connecting their medical systems with these requirements, healthcare organizations can enhance their medical systems' general efficacy and interoperability within the healthcare ecosystem.

This finding recommends that medical system developers and healthcare organizations should focus substantially on following medical system design regulations to align medical system design with organizational requirements better. More efficient and interoperable medical systems might be produced by taking a strategic approach to

medical system development that incorporates policy adherence and healthcare organizational requirements analysis. The relevance of policy compliance for attaining interoperability and system effectiveness in healthcare is shown by the positive and statistically significant correlation between following healthcare design policy and alignment with organizational requirements. It bolsters the idea that, in this case, developing a medical system involves a complete strategy that considers industry norms and organizational requirements.

4.2 Factors Affecting Secure Interoperability of Medical Systems

Interoperability is the ability of different medical systems' devices and applications to work together in exchanging and using data seamlessly within and across organizational boundaries to advance effective healthcare delivery for individuals and communities (Bokolo, 2022). Interoperability aids in improving healthcare delivery, patient outcomes, and overall efficiency in the healthcare industry. It enables healthcare providers to access and share patient information accurately and efficiently, leading to better-informed decisions and improved patient care. Poor interoperability between health information systems reduces the quality of healthcare provided to patients and wastes resources (HIMSS, 2022).

4.2.1 General Categories of the Factors Affecting Secure Interoperability of Medical Systems

Achieving seamless interoperability remains a complex challenge. This study sort to explore key factors affecting the interoperability of medical systems. The study revealed that some of the key factors that affect interoperability of medical systems can be categorized into technical, semantic, organizational, legal/regulatory, security and privacy, human, financial, and cultural aspects. Table 5 shows the categories of factors affecting the interoperability of medical systems.

Table 9*Categories of Factors Affecting the Interoperability of Medical Systems*

	Percent (%)
Valid Technical factors	32
Structural factors	11
Semantic factors	22
Organizational, Human & Cultural factors	05
Legal/Regulatory factors	10
Security & Privacy factors	12
Financial factors	08
Total	100

4.2.1 Results Analysis and Discussion of the Findings

According to this study, respondents rated technical factors as the most influential. 32% of the respondents consider technical factors to have the greatest impact on the interoperability of medical systems. This category encompasses crucial elements such as data standards, interoperability protocols, data integration, scalability, and technical infrastructure; all of which were identified as top contributors to the overall interoperability challenge. The study noted that the use of standardized data formats and coding systems, such as HL7, DICOM, SNOMED CT, is crucial for ensuring that data can be exchanged and interpreted consistently across different systems. Medical systems often use proprietary data formats, making it difficult for different systems to communicate effectively. Establishing and adhering to industry-standard data formats, for example, HL7, FHIR, is crucial for achieving interoperability.

It was also noted that the choice of communication protocols (e.g., FHIR, CDA) and interfaces for data exchange is important to establishing seamless connections between systems. Additionally, the ability to integrate data from various sources (e.g., EMRs,

medical devices, laboratories) is vital for a comprehensive patient record; and hence systems should be designed to scale with increasing data volumes and user demands. Also, managing inconsistent information across multiple network sources is a huge challenge, particularly for healthcare IT vendors who service large health networks. Many healthcare organizations still rely on enterprise systems that are not designed with interoperability in mind. These older systems may lack the necessary APIs and interfaces to integrate with modern systems, creating compatibility issues. Effective interoperability often requires the use of integration middleware, such as service-oriented architecture (SOA) or healthcare information exchange (HIE) platforms.

Selecting and implementing the appropriate middleware is critical in ensuring seamless data exchange between different systems. Lastly, the study revealed that technical infrastructural factors like network connectivity, data storage and management are also crucial for the success of medical systems interoperability. This implies that reliable and secure network infrastructure is essential for data transmission and exchange between medical systems; and efficient data storage, backup, and management systems are needed to handle the volume of data generated in healthcare sector. These results are consistent with the already existing literature (Yang et al., 2022), (Clunie, 2021) and (Albouq et al., 2022).

Semantic factors were rated the second most influential factors with 22% of the respondents indicating terminology and vocabulary, data mapping and ontologies as the main elements. This implies that consistent use of medical terminology and coding systems ensures that data has a shared meaning across systems. Correspondingly, establishing mappings between different coding systems or vocabularies helps in translating data between systems with varying terminologies and using ontologies and knowledge graphs can help in representing complex medical concepts and relationships,

thereby aiding semantic interoperability. These results align with the existing literature (Patange et al., 2021), (Torab-Miandoab et al., 2023) and (de Mello et al., 2022).

Furthermore, the survey revealed that security and privacy concerns were recognized as impediments to medical system interoperability. 12% of the respondents highlighted the significance of robust data security measures which includes encryption, access controls, and audit trails, as essential to protecting patient data during exchange. Additionally, the importance of patient consent and privacy emerged as vital factors, emphasizing the need to secure patient consent for data sharing and to ensure compliance with privacy regulations for maintaining trust. These elements were highlighted for their pivotal roles in addressing these challenges. These results are in line with the reviewed literature (Durneva et al., 2020).

Structural factors were also considered to be hindering interoperability of medical systems with 11% of the respondents citing it as an impediment. In the healthcare industry, structural elements are a major determinant of medical system interoperability. The level of structural interoperability establishes the structure, syntax, and format of data that is sent between systems, making sure that the data remains coherent and comprehensible to the systems that receive it. Structural interoperability, for example, makes sure that vital medical data, like test results or patient record, is sent in an orderly and consistent way, allowing for easy data interpretation and interchange between various healthcare information systems. Structural variables improve the consistency, correctness, and dependability of information provided amongst healthcare professionals by creating a uniform framework for data interchange. This improves patient outcomes, decision-making, and care coordination. Furthermore, following structural interoperability guidelines encourages data integrity, lowers errors, and facilitates the effective integration of medical information systems, ultimately enhancing the quality

and effectiveness of healthcare delivery. These results are in line with the reviewed literature (Persons et al., 2020). Legal and regulatory factors were identified as another impediment to the achievement of medical system interoperability, as indicated by 10% of the respondents. Healthcare regulations, exemplified by HIPAA in healthcare sector, impose stringent demands concerning the storage and sharing of patient data. Regulatory bodies may lag behind in establishing clear standards for interoperability. The absence of such standards can hinder innovation and create uncertainty for healthcare organizations. Diverse regulations across regions and countries create compliance complexities, thereby hindering data sharing.

Hence, striking a delicate balance between ensuring compliance with these regulations and promoting interoperability becomes a crucial challenge in the achievement of medical systems interoperability. Collaboration among healthcare IT vendors, standards development organizations, and government agencies can foster development and adoption of interoperability standards and best practices to aid in medical systems interoperability. This implies that lack of interoperability standards or poorly enforced standards can obstruct seamless medical data exchange by complicating transactions and complicating the coordination of care across various medical settings. The findings are in line with the information that is already in literature (Persons et al., 2020).

Financial considerations, highlighted by 08% of the respondents as a concern, also emerged as a hindrance to medical system interoperability. The financial ramifications of establishing and sustaining interoperable systems can be substantial, encompassing initial expenditures, continuous maintenance costs, and the potential for vendor lock-in. Further, the demonstration of a favorable Return on Investment (ROI) can serve as a pivotal motivator for healthcare organizations to invest in such systems.

Organizational, human, and cultural factors, all accounting for 5% of responses, were identified as significant influences on medical system interoperability. Organizational aspects encompass healthcare policies and regulations, which necessitate compliance with healthcare regulations such as HIPAA and ISO, as well as industry standards, can impact the sharing of patient data between organizations. Workflow integration, another organizational factor, involves aligning system workflows with clinical processes and practices to enhance user acceptance and system usability. Additionally, governance and leadership were highlighted; indicating that strong leadership and governance structures can stimulate interoperability initiatives and establish guidelines for data sharing.

Among human factors, user training emerged as a crucial element, emphasizing the need for adequate training for healthcare professionals and IT staff to enhance effective utilization and troubleshooting of interoperable systems. User acceptance was another human factor, which plays a pivotal role in the success of interoperable systems, as resistance to change can impede adoption.

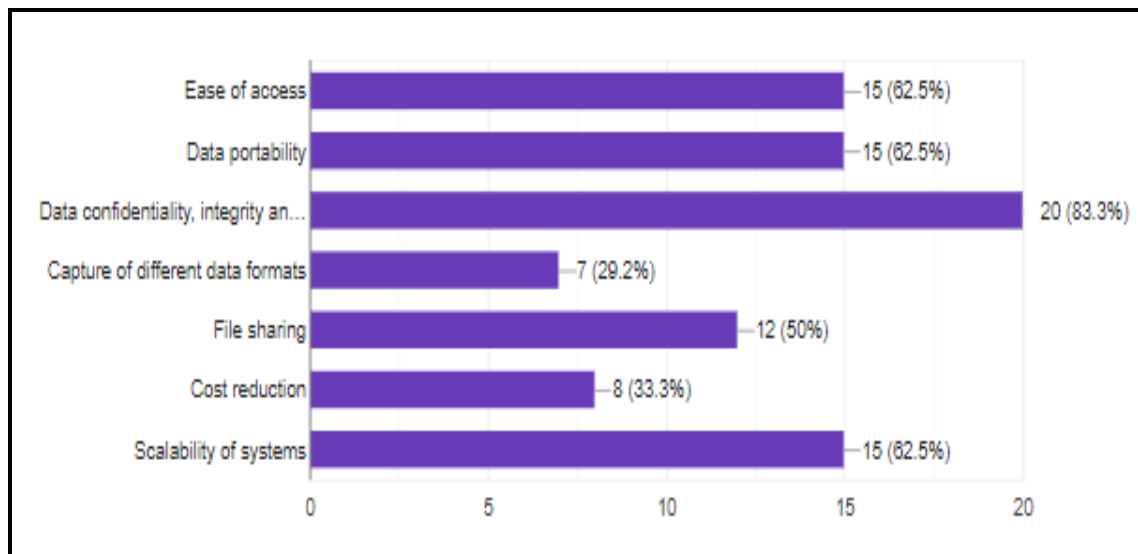
Cultural factors which accounted for the final 5%, comprise resistance to change, which is prevalent in the healthcare industry due to its traditional conservatism, potentially hindering the adoption of new technologies and interoperable systems. Healthcare professionals may exhibit hesitancy towards embracing change, even when it promises benefits. The siloed mindset, historically predominant in healthcare organizations with limited collaboration between departments or institutions, necessitates a cultural shift towards a more collaborative approach to promote interoperability.

4.2.2 Specific Barriers to Secure Interoperability of Medical Systems under Technical, Semantic and Security Factors

The study further sort to understand the specific barriers to interoperability of medical system under the categories labelled technical, semantic and security factors, which were identified in section 4.2.1. The respondents were asked to indicate the specific barriers under technical, semantic and security factors. Figure 15 gives the summary of the specific barriers to interoperability of medical systems as answered by the respondents. The discussion of the findings on barriers hindering secure interoperability of medical systems under the technical, semantic and security factors are discussed in the subsequent sections.

Figure 15

Summary of the Barriers to Interoperability of Medical Systems



4.2.2.1 Results Analysis and Discussion of the Findings

Ease of access of medical systems is mentioned as one of the barriers under the technical factors that hinder interoperability. 62.5% of respondents believed that accessibility of data was a barrier to interoperability, hence highlighting it a serious problem that faces medical systems. These findings are in line with more general debates in the healthcare

sector, where data accessibility has long been a source of worry. In order to deliver timely and effective patient care, it is critical to ensure simple and safe access to medical data across various systems, according to a paper by the Healthcare Information and Management Systems Society(HIMSS, 2022). The respondents may have pointed out data silos, proprietary data formats, or access control restrictions as technical obstacles to the free flow of information across healthcare organizations.

The fact that a large majority of respondents acknowledge that removing these barriers is difficult is a further indication of the pressing need for solutions because achieving interoperability necessitates doing so. The World Health Organization report on Israel's venture to advance interoperability and data sharing in the health system(World Health Organization [WHO], 2021)also emphasizes the necessity of interoperability for global health activities, and the importance of resolving access concerns in order to accomplish this goal. As a result, the survey results do not just reflect the respondents' opinions; rather they reflect the industry's acknowledgment of the significance of addressing data accessibility as a key component of the technical factors affecting and hindering attainment of seamless interoperability in medical systems.

Data Portability is also recorded as a barrier under technical factors affecting interoperability of medical system. 62.5% of respondents citing data portability as a barrier to interoperability, thereby revealing a pervasive worry in the world of medical systems in the healthcare sector. The seamless interchange of information between healthcare organizations, which is essential for coordinated patient care and effective healthcare delivery, is impacted by the issue of data portability, making it a significant factor. This finding is consistent with talks in the healthcare IT industry, as cited in a paper by Torab and others (Torab-Miandoab et al., 2023),noting that it has been difficult to make sure that medical data can be easily transported and shared among medical

systems. Additionally, one of the essential elements of interoperability, according to a report released by the Office of the National Coordinator for Health Information Technology (ONC) (U.S. Department of Health & Human Services, 2023), and a paper by Savage and Savage (Savage & Savage, 2020), is data portability. No matter the technologies in use, data portability underlines the necessity for healthcare companies to be able to access, retrieve, and securely communicate patient data across many platforms. The overwhelming majority of survey participants who see data portability as a problem emphasize how urgent it is for healthcare institutions and policymakers to deal with this issue.

The World Health Organization (WHO)(World Health Organization [WHO], 2020) also underlines the importance of data portability in international data exchange and global health efforts, in addition to its importance at the national level. This observation stresses importance of data portability in addressing impediments to interoperability, both inside local medical systems and globally. Finally, the significant proportion of respondents who identified data portability as a challenge highlights the urgent need for coordinated efforts in the healthcare industry to develop standards and solutions that enable easy transfer of data between various systems, ultimately enhancing interoperability and, by extension, the caliber of healthcare services offered to patients.

Data confidentiality, integrity and security was also indicated to be a security factor that is hindering interoperability of medical systems. The startling agreement among 83.3% of respondents who cited data confidentiality, integrity and security as major obstacles to interoperability reflected the supreme significance of security and medical data quality in the context of medical systems. This discovery reveals a widespread worry about the security and reliability of patient medical data and information in the healthcare sector. Medical systems are built on the core tenets of data integrity and confidentiality. The

systems are essential to maintaining the authenticity of medical records, protecting patient privacy, and guaranteeing dependability of healthcare data for clinical decision-making (Pillai et al., 2020). The importance of these problems in healthcare information technology is highlighted by the fact that a sizable majority of research participants identified security and reliability as barriers to interoperability. Strong security measures that include confidentiality, privacy, integrity and data quality requirements are required, according to many sources in the healthcare sector. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States establishes stringent rules for the confidentiality and integrity of medical data (Duggineni, 2023).

To secure confidentiality and integrity of data, international standards like ISO 27001 (ISO/IEC, 2020) offer recommendations for information security management systems. Additionally, research by the Healthcare Information and Management Systems Society (HIMSS) emphasizes that data security lapses can have serious repercussions, including monetary fines, reputational harm to an organization, and, most importantly, compromised patient care as discussed by Yeo and Banfield (Yeo & Banfield, 2022). The overwhelming level of worry shown by poll participants highlights how urgent it is to address these issues in their entirety. In conclusion, there is a clear call to action given the overwhelming consensus among respondents that data confidentiality, integrity and security hinder interoperability. In order to achieve smooth interoperability, the study stresses the need for healthcare organizations to give strong security measures and data quality initiatives top priority. By addressing these issues, data privacy is improved and medical systems are made more trustworthy and reliable, thus improving patient care and outcomes.

Different data formats which were stated as a technical and semantic factor was also deemed to be a barrier to interoperability of medical systems. The findings indicated that

29.2% of respondents believe that diverse data formats are a barrier to interoperability highlights a significant yet underappreciated component of interoperability issues in the field of medical systems. Fundamentally, interoperability depends on the capacity of various systems to comprehend and utilize data from one another. Data format compatibility is an important component of interoperability. It can be very difficult to share data seamlessly when medical systems employ different data formats to store and exchange information (Yang et al., 2022). Due to a wide variety of software and medical systems used in healthcare sector, from electronic medical records (EMRs) to medical imaging technologies, this difficulty is accentuated.

It may be challenging to integrate and communicate data across healthcare ecosystem since each of these medical systems may choose to use a different data format. Nearly 30% of respondents acknowledged this difficulty, highlighting the necessity of standardized data formats and interoperability protocols in the healthcare sector. By defining common data exchange standards and profiles, standardization initiatives, such as those promoted by groups like Health Level Seven International (HL7)(STU, 2018) and Integrating the Healthcare Enterprise (IHE), seek to specifically address these problems.

The seamless sharing of healthcare data between various systems is made possible by these standards (Saripalle, 2019). Additionally, Lehne et al., (2019)suggests and emphasizes in his research how crucial standardizing data formats is to achieve true interoperability of medical systems. Consequently, ensuring reliable data interchange, requires standard formats which make it possible to create interoperable software that can access and use data from a variety of sources. In conclusion, the problem of data formats is a significant a barrier to interoperability. Standardization initiatives and adoption of standard data formats and protocols in medical systems are required to

address this issue, which ultimately boost interoperability and result in more effective healthcare delivery.

Sharing files across different medical systems was also cited as a barrier to interoperability. Findings indicated that 50% of respondents believed file sharing to be a barrier to interoperability ,emphasizing the significance of efficient data exchange technologies for interoperability in healthcare sector. Transparent file and data transfer is essential for healthcare systems. Effective information exchange is crucial for delivering high-quality care, from sharing patient records among healthcare providers to transmitting diagnostic images and test results (M. Kim et al., 2020).

The fact that 50% of respondents considered file sharing a severe problem, highlights the complex nature of medical information, which manifest in a range of file types, including text-based records, high-resolution medical images, and videos. It is a challenging undertaking to make sure that these varied data formats can be transferred and understood correctly by multiple systems (Torab-Miandoab et al., 2023).Data Privacy and Security has also been considered a challenge. Sharing healthcare data requires strong security measures to preserve patient confidentiality and data integrity because the information is highly sensitive. Sharing files securely and in accordance with healthcare standards is also a challenge (Denecke, 2021).

In addition, file sharing standardization is posed to be a challenge. Lack of established standards for file sharing can make medical systems less compatible. Data loss, corruption, or misinterpretation might result from separate systems sharing files in different ways and formats (Chenthara et al., 2020). Lastly, medical system integration efforts have been faced with a big opposition. To enable file sharing between their medical systems, healthcare firms frequently invest in integration solutions (Bakibinga et

al., 2020). However, these initiatives could need a lot of resources and might not cover all the required endpoints, leaving gaps in interoperability. Healthcare organizations and technology suppliers must concentrate on creating standardized file-sharing protocols, guaranteeing strong security procedures, and pushing interoperability projects that take into account the many kinds of data used in healthcare settings, so as to address the ensuing issues. Additionally, implementing health information exchange (HIE) technologies and standards can significantly improve interoperability throughout the healthcare ecosystem by easing file sharing. In conclusion, the fact that 50% of respondents cited file sharing as a barrier to interoperability of medical systems highlights the urgent need for healthcare organizations and stakeholders to give top priority to solutions that allow for effective, secure, and standardized file sharing in order to enhance overall healthcare interoperability and patient care outcomes.

Cost reduction of developing, adopting and integration technologies that could allow sharing of information and electronic medical records (EMRs) across medical systems was also cited to be a barrier to interoperability of medical systems. The result of this study shows that 33.3% of respondents consider cost reduction to be a potential barrier to interoperability. This brings to light the intricate financial issues that can influence efforts to improve healthcare system compatibility. Several cost-related variables are relevant in the context of healthcare interoperability including the initial cost of development and installation of medical systems.

Putting in place interoperable systems frequently necessitates a sizable upfront cost. This includes expenses for staff training, replacing outdated systems, and purchasing new technologies. This upfront cost may be a deterrent for certain healthcare institutions, particularly smaller ones, with tighter budgets (Renukappa et al., 2022). Secondly, maintenance cost was also considered a challenge hindering interoperability of medical

systems. Maintaining interoperable systems entails continual expenses for technical assistance, hardware upkeep, and software updates. If not effectively managed, these charges may put a burden on finances (Nagasubramanian et al., 2020). Additionally, data integration cost incurred by combining data from many systems can be difficult and expensive. To help with data integration initiatives, healthcare institutions may need to hire professionals or consultants, thereby raising overall costs as noted by Li et al. (2021) and Kuo & Kuo (2017).

Compliance costs incurred when ensuring that interoperable systems abide with healthcare standards and laws may result in extra costs. Penalties or fines for non-compliance might further strain the budget (E. Li et al., 2022). Lastly, return on investment (ROI) uncertainty was indicated as a challenge to interoperability of medical systems. Although it is anticipated that interoperability would have long-term advantages, figuring out the return on investment (ROI) can be difficult. Due to uncertainties over the financial rewards, some firms could be hesitant to invest in interoperability initiatives (Torab-Miandoab et al., 2023).

Healthcare organizations and governments can take into account a number of measures to address these issues and lessen the possible impact of cost reduction. Budget Planning in healthcare organizations can better manage resources by creating a detailed budget plan that takes expenses of interoperability projects into account. The financial burden can be alleviated by healthcare organizations seeking grants and financing, especially smaller healthcare providers. Collaboration of healthcare organizations forming regional health information exchanges (HIEs) or collaborating with other healthcare institutions through adoption of medical systems that support interoperability can assist spread the expense of interoperability infrastructure and upkeep. Efficiency gains which should add emphases on the long-term cost savings and efficiency improves interoperability, which

could justify the initial investment. Standardization of medical systems implies that fostering adoption of interoperability standards can lower the price of bespoke integrations and advance interoperability throughout the sector (Albouq et al., 2022). While one-third of the respondents believe cost reduction to be a potential barrier to interoperability, it is crucial to understand that strategic planning, collaboration, and a focus on long-term benefits can assist healthcare organizations in navigating the financial aspects of achieving interoperability (E. Li et al., 2022). In the end, it's important to make sure that financial considerations don't get in the way of providing patients with coordinated, high-quality care.

Scalability of systems is a significant barrier to interoperability, according to 62.5% of respondents, which highlights the significance of tackling the problem of scalability in the context of medical systems. The ability of a system to handle more users, data, or tasks while maintaining good performance is referred to as scalability (Al-mutar et al., 2022). For several reasons, scalability is crucial in the healthcare sector. Healthcare organizations produce a vast amount of data, including patient information, imaging results, and clinical notes, which are generated every day by healthcare companies. To efficiently handle this influx of data, systems must grow as the volume of healthcare data increases (Yadav et al., 2020).

Expanding healthcare services to cover all the medical services may also result to scalability challenges. New services, specialties, and treatment techniques constantly appear in the fast-changing healthcare industry. Without interfering with current operations, scalable systems may adjust to these changes and facilitate the inclusion of new services or departments (Kim et al., 2020). Patient volume is on the rise (Lorenzen & Schwartz, 2021) resulting to the need for medical systems that can handle demand spikes when patient volumes change, as they do during pandemics or abrupt

emergencies. Scalability guarantees that healthcare professionals can continue to give high-quality care under even when patient volumes spike. Interoperability can be achieved by establishing connections with external healthcare systems, such as those of other providers, laboratories, and insurers. These connections can be facilitated by scalable systems, thus enabling frictionless data transfer.

To overcome the challenge of scalability in attaining interoperability, the healthcare sector should take into account techniques, scalable infrastructure achieved by investing in cloud-based services, and scalable hardware that can grow or shrink in response to demand. With this strategy, there is less need for significant up-front investments, and businesses may only pay for the resources they really utilize (Esposito et al., 2018). Healthcare sector should adopt interoperability standards and frameworks that encourage scalability (AlQudah et al., 2021). Scalability is a key consideration in the design of standards like HL7 FHIR and Fast Healthcare Interoperability Resources. Another technique that aims to improve system performance as patient data volume rises is patient data management. Implementation of effective data management techniques, such as data archiving, compression, and indexing (Kruse et al., 2018) improves system performance.

Additionally, regular assessments of the medical systems are crucial in the attainment of scalability. Medical organizations should perform routine evaluations of medical system scalability and performance to spot any potential bottlenecks or constraints (Szarfman et al., 2022). Healthcare organizations may solve scalability concerns before they have a negative impact on operations of medical systems. Collaboration among healthcare organizations where different vendors or developers of medical systems work with other vendors and technology partners who focus on scalable healthcare solutions and systems (Sater, 2018). Partnerships between medical vendors may give access to resources and

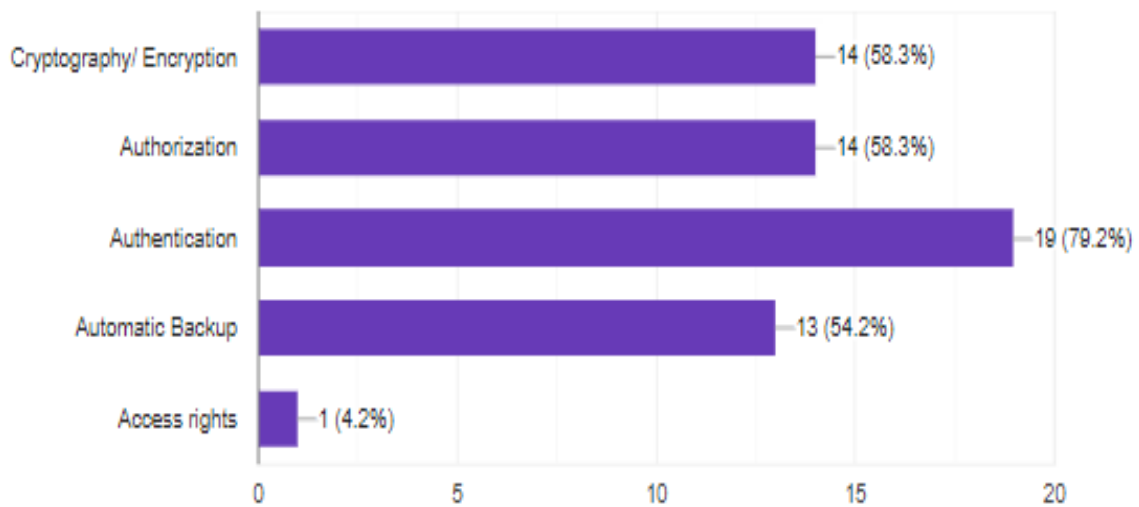
knowledge for tackling scale issues. A significant number of respondents perceived system scalability as a barrier to interoperability, which underscores the significance of scalability in healthcare technology. To ensure that their medical systems can adapt to the changing requirements of the healthcare sector while retaining security, interoperability and data exchange capabilities, healthcare organizations must invest in scalable infrastructure and technology.

4.2.3 Type of Security Incorporated in the Developed Medical Systems

To uncover the factors affecting interoperability of medical systems, the study sort to explore the type of security measures that were incorporated by the participating medical system software development companies. Understanding the types of security measures integrated into medical systems provided valuable insights into the security practices applied by the participating medical system software development companies. This analysis helped uncover the specific security technologies and strategies employed to safeguard sensitive patient data stored in the electronic medical records (EMRs) and maintain the integrity of the medical systems. Figure 16 shows the key findings on security incorporated in developed medical system.

Figure 16

Type of Security Incorporated in the developed Medical Systems



4.2.3.1 Results Analysis and Discussion of the Findings

Cryptography/Encryption: 58.3% of the respondents reported incorporating cryptography and encryption as a security measure in their medical systems. Cryptography and encryption play a crucial role in protecting data privacy by converting sensitive information into unreadable formats that can only be deciphered by authorized parties. This high adoption rate indicates a strong emphasis on data confidentiality within the design and development process.

Authentication: A significant majority of respondents (79.2%) mentioned incorporating authentication mechanisms into their medical systems. Authentication ensures that only authorized users can access the system, preventing unauthorized access and unauthorized changes to sensitive data. This security measure is essential for maintaining system integrity and controlling access to critical functionalities.

Authorization: More than half of the respondents (58.3%) indicated incorporating authorization as a security measure. Authorization defines what actions data specific users are permitted to access and manipulate within the system. This measure helps

prevent unauthorized actions and ensures that users can only perform tasks relevant to their roles.

Automatic Backup: A good number of respondents (54.2%) reported incorporating automatic backup mechanisms into their medical systems. Automatic backups are essential for data recovery in case of system failures, data corruption, or cyber-attacks. This measure contributes to maintaining data availability and system continuity.

Access Rights: A small proportion of respondents (4.2%) mentioned integrating access control levels into their medical systems. Access control levels dictate the permissions granted to different user roles, and ensuring that users can only access the information and functionalities relevant to their responsibilities.

These findings on the types of security being incorporated in a medical system shows that adoption of multiple security measures, such as cryptography, authentication, authorization, and access control, reflects a comprehensive approach to system security. The high percentage of companies incorporating these measures indicates a concerted effort to protect patient data, prevent unauthorized access, and maintain overall system integrity. The integration of security measures is aligned with best practices for designing secure medical systems, demonstrating an awareness of the unique security challenges and risks within the healthcare domain. The diversity in the types of security measures employed also suggests a nuanced understanding of the multifaceted nature of security requirements.

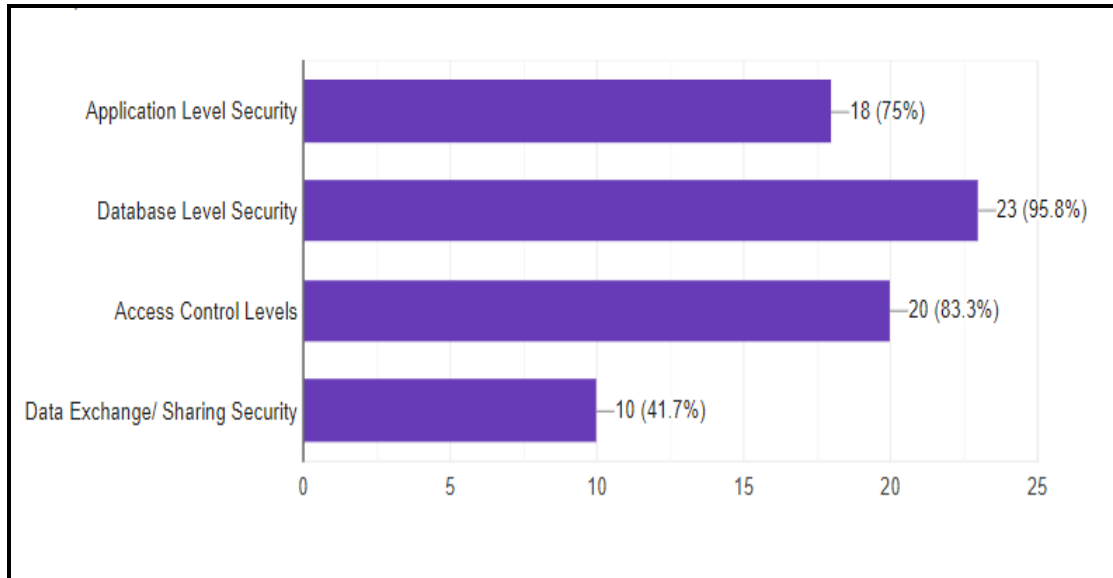
4.2.4 Level of Security used in the Medical Systems

Participants were questioned regarding the various security measures incorporated into the medical systems they created. This question gauges the perceived level of security in

the designed medical systems. Multiple responses were permitted to the question. Figure 17 shows a summary of the level of security used in the Medical Systems.

Figure 17

Level of Security used in the Medical Systems



4.2.4.1 Results Analysis and Discussion of the Findings

According to the findings, it is clear that the respondents incorporate a number of security features into their medical system designs. The most often incorporated security measure is at "Database Level," which was mentioned by 95.8% of respondents. 75.0% of the respondents indicated that the medical systems they develop incorporates security at the Application Level. According to 83.3% of respondents, Access Control Levels are important for limiting system access. It is interesting to note that 41.7% of the medical systems have Data Sharing security checked, underscoring the importance of security in data sharing. These results highlight the thorough method used by respondents to address security issues in the medical systems they build. This could involve securing data as it is exchanged between different systems or organizations, thus ensuring that data remains protected during transfer. In conclusion, the findings highlight the importance of a

layered and holistic approach to security within medical systems. The incorporation of various security measures showcases the dedication of companies to ensuring data privacy, system reliability, and compliance with regulatory standards.

4.2.5 Security Standards and Policies

The study sort to explore the awareness levels and applied security standards by the domain experts. Medical standards and policies play a crucial role in ensuring security, privacy and interoperability of medical systems.

4.2.5.1 Awareness of Medical Design

The degree to which participants are knowledgeable about the security factors, standards, and best practices involved in creating secure and interoperable medical systems can be determined by evaluating the respondents' awareness on the design principles for medical systems. This analysis aids in determining the respondents' level of knowledge and skill in the field. The responses obtained from the participants are shown in Table 6, and the discussion of the findings presented in the subsequent sections.

Table 10

Level of Awareness of Medical System Design

		Awareness of Medical System Design			Cumulative
		Frequency	Percent	Valid Percent	Percent
Valid	Yes	18	75.0	75.0	75.0
	No	6	25.0	25.0	100.0
Total		24	100.0	100.0	

The majority of respondents (75%) stated that they were highly aware of the security principles governing medical system design. This shows that the respondents are knowledgeable about the complexities involved in creating medical systems that adhere

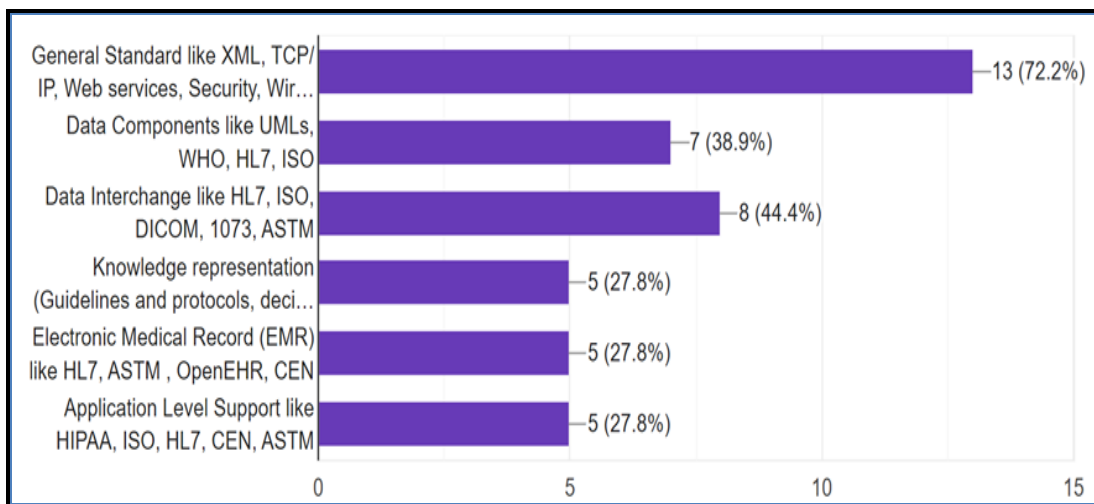
to standards of security, interoperability, and other pertinent considerations. However, some respondents (25%) said they were unaware of the security concepts underlying medical system design. This implies that a majority of the medical system software developers are cognizant of the security principles that can be incorporated into their medical system designs as they develop the medical systems.

4.2.5.2 Applied Security Standards

The study examined the perspective of various security levels of design considerations within medical systems among the individuals who were knowledgeable in medical system design. The applied security standards are as shown in Figure 18.

Figure 18

Security Standards Applied in the Medical Systems



Different perceptions of varied security levels of design considerations within medical systems were displayed by the domain experts who were knowledgeable of how medical systems are designed. The findings revealed that on application-Level Support, 27.8% of the respondents were aware that the design of medical systems takes into account application-level support standards, such as HIPAA, ISO, HL7, CEN, and ASTM. For Electronic Medical Record (EMR) Level, 27.8% of participants indicated that they were

aware of HL7, ASTM, Open EHR, and CEN as Electronic Medical Record (EMR) standards that should be taken into account when designing EMR systems. On Knowledge Representation Level, approximately 27.8% of the respondents were aware of the design principles governing knowledge representation, such as rules, protocols, and decision-support algorithms, which are frequently governed by HL7 and ASTM standards. Data Interchange Level showed that 44.4% of the participants said they were aware that the design process incorporates data interchange standards like HL7, ISO, DICOM, and ASTM, thus allowing for easy data flow between systems.

For Data Components Level, 38.9% of respondents knew that data components like UMLs, WHO, HL7, and ISO were integrated into medical systems and contributed to their overall design. On General Standards Level, a significant portion of respondents (72.2%), acknowledged the usage of general standards in the design of medical systems, including XML, TCP/IP, Web services, security protocols, wireless technologies, HL7 and IEEE standards, as well as XML, TCP/IP, and Web services. The effectiveness, security, and interoperability of medical systems are ensured by combining many design factors and standards, as shown by these research findings.

4.2.6 Interoperability of Medical Systems

Interoperability refers to the ability of medical systems in healthcare sector to seamlessly and securely exchange and use electronic medical records (EMRs), and the patient personal health information (PHI) across different medical systems, devices and applications (Bokolo, 2022). This study sort to examine the awareness levels of the respondents in developing interoperable medical systems. Responses to the questions on interoperability are discussed in the subsequent sections.

4.2.6.1 Awareness of Interoperability of Medical System

The respondents' familiarity with the idea of interoperability was examined. Participants were questioned about their knowledge of interoperability problems as they relate to medical systems. Table 11 highlights the summary of the responses on the awareness of interoperability.

Table 11

Summary of the Awareness of Interoperability of Medical Systems

		Awareness to Interoperability			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	18	75.0	75.0	75.0
	No	6	25.0	25.0	100.0
Total		24	100.0	100.0	

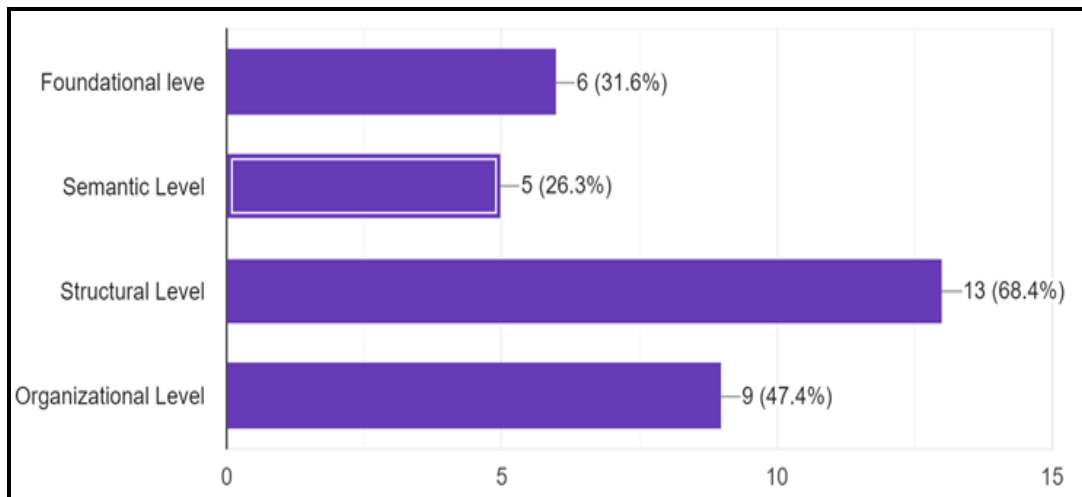
75% percent of the 24 respondents said they were aware of interoperability problems in the context of medical systems. This shows that a sizeable majority of the participants were aware of the difficulties and advantages of integrating various medical systems successfully. In contrast, 25.0% of the respondents said they were not aware of interoperability problems. The significance of interoperability and its ramifications for the integration of medical systems may not be fully understood, as this finding might suggest. The finding implies that participants' observed levels of awareness are a reflection of the different levels of their exposure to and knowledge about interoperability of medical systems, which may have an impact on how they see medical system design, development, and collaboration with other healthcare organizations.

4.2.6.2 Levels of Interoperability

The study then looked into the levels of interoperability within the medical systems. Participants who were aware of interoperability of medical systems were further asked to elaborate on how interoperable medical systems they designed and used were. Different opinions on the various levels of interoperability in the medical systems arose among the 75% of the respondents who were aware of interoperability issues. The results were graphed as shown in Figure 19.

Figure 19

Levels of Medical Systems Interoperability



4.2.6.3 Results Analysis and Discussion of the Findings

Foundational Level: 31.6% of the respondents who were surveyed indicated that medical systems are interoperable on a fundamental level. This implies a fundamental degree or basic level of interoperability and compatibility that allows different medical systems to exchange patients' data and information, but may not ensure seamless integration or full usability of the exchanged data. It is also known as simple transport level. This level establishes the inter-connectivity design requirements needed for one medical system or medical application to securely communicate patients' data to and receive patients' data

from another medical system. It establishes building blocks where medical systems can exchange data but with human intervention. The medical systems can send and receive data across healthcare organizations, but they cannot interpret the patients' data without human assistance or other assistance from other technologies. Some of the key characteristics of the foundational level of interoperability includes; patient data exchange, which enables medical systems to send and receive patients' data between each other, often using standardized formats and protocols; basic communication, where medical systems can establish connections and transmit patients' data, but they may not fully understand the data or be able to act on it without manual or human intervention; Data Standards, where patient' data may be in a common format, but it may not be fully structured or semantically meaningful; and limited security, in which basic security measures like user authentication may be in place, but security may not be robust.

Structure Level of interoperability: The majority of respondents (68.4%) believed that structural interconnection exists in their medical systems. This level implies that systems can interchange data without information being lost, and while maintaining the data's intended meaning. Since structural interoperability builds upon foundational interoperability by ensuring that the data exchanged between systems follows a common structure and can be readily interpreted. Some of the key characteristics of structural level of interoperability includes standardized data formats, in which patients' data is exchanged using standardized and well-defined formats, schemas, and data models as defined by the medical regulating bodies; Data Mapping where medical systems can map data fields and elements from one medical system to another, making it easier to understand and use; data validation where the patients' data exchanged adheres to predefined medical standards and validation rules; and enhanced security which implies

that more robust security measures are typically in place to protect data during transmission and storage.

Semantic Level: 26.3% of participants said that semantic interoperability exists in their medical systems. This suggests a deeper level of data comprehension and interpretation across many medical systems, thus facilitating valuable information interchange. Semantic interoperability takes interoperability to a higher level by ensuring that data exchanged between medical systems is not just structurally compatible but also carries a shared meaning and context. Some of the key characteristics of semantic level of interoperability includes Common Terminologies in which medical systems use standardized clinical vocabularies, ontologies, and terminologies to represent and interpret data consistently; Data Semantics which implies patients' data exchanged has a shared understanding of its meaning and context, enabling automatic interpretation and integration; Clinical Decision Support which describes medical systems ability to exchange data for clinical decision support, making it more actionable for healthcare providers; and lastly the enhanced clinical workflows, where patients' data can flow seamlessly across different medical systems, improving the efficiency and quality of care.

Organizational Level: According to 47.4% of the participants, healthcare organizations exhibit organizational interoperability. Organizational interoperability level represents the integration of medical systems, processes, and policies across different healthcare organizations, such as hospitals, clinics, and laboratories. This level suggests that the systems are able to cooperate and work together as part of a bigger healthcare ecosystem. Some of the key characteristics of the organizational level of interoperability includes Cross-Organizational Data Sharing, where data can be shared securely and seamlessly among different healthcare organizations; Integrated Care Coordination, which implies

that healthcare providers across organizations can collaborate effectively, ensuring coordinated patient care; Patient-Centric Focus, in which patient data and processes are organized around the patient's needs, leading to improved patient-centered care; and Comprehensive Health Information Exchange, in which a comprehensive health information exchange infrastructure may be in place to support data sharing on a regional or national level.

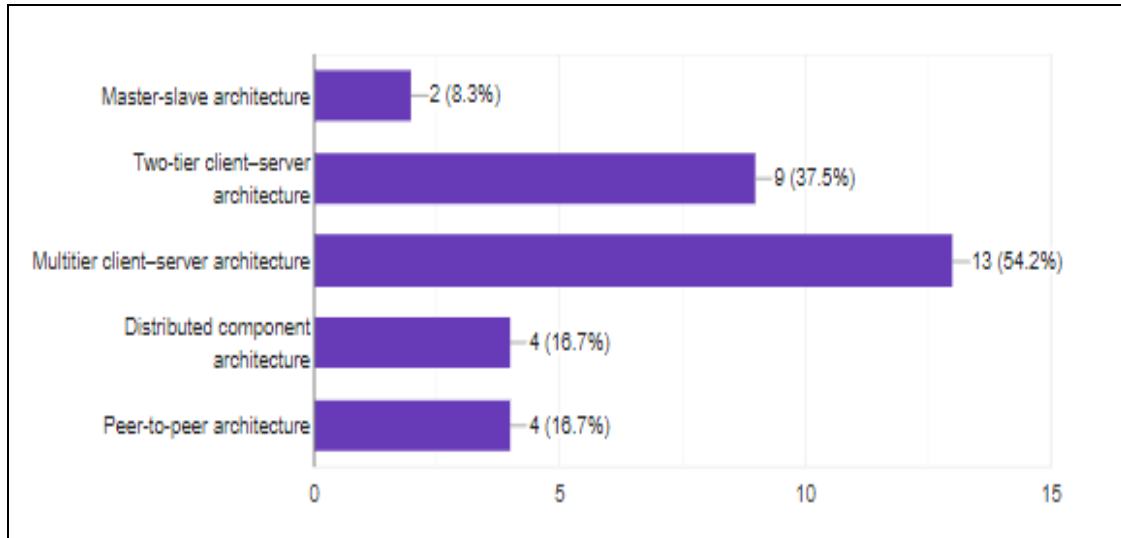
These findings show the complexity of interoperability and the various techniques necessary to accomplish seamless integration and data interchange among medical systems. This complexity is highlighted by disparate perceptions from the domain experts that responded to the study. Achieving higher levels of interoperability, particularly semantic and organizational interoperability, is a significant challenge in healthcare sector due to the complexity of medical systems, diverse data sources, and the need for strict security and privacy measures. However, these levels of interoperability are essential for improving patient care, reducing medical errors, and enabling more efficient and data-driven healthcare delivery.

4.2.7 Architectures and Information Sharing

The study allowed the respondents to give multiple responses on the architectures employed in sharing of information. Learning about the architectural approaches used in developing medical systems was vital. Examining the architectural methods used to create medical systems informed the study by giving insights into fundamental design ideas and tactics used by businesses. Understanding the variety of approaches and their potential effects on system functionality and interoperability is made easier by this examination. The analysis on architectural approaches used in developing medical systems for data sharing is shown in Figure 20.

Figure 20

Architectural Approaches Used in Developing Medical Systems for Data Sharing



4.2.7.1 Results Analysis and Discussion of the Findings

Master-slave architecture. Only 8.3% of the respondents reported the use of master-slave architecture. A single master component serves as the coordinator and controller for several slave components in this arrangement. Although careful synchronization may be needed, master-slave architecture can be effective for controlling distributed systems

Two tier client-server architecture: The use of a two-tier client-server architecture was mentioned by 37.5% of the respondents. The client layer and the server layer are the two primary layers of the system in this method. Despite the fact that this architecture can make the design simpler, compared to multitier systems, it may have scaling and concern separation issues.

Multi-client server architecture: 54.2% of the respondents used the multi-client server architecture in designing medical systems, a number of responses indicated the use of multitier client-server architecture. With this strategy, the system is divided into various levels, each of which is in charge of particular duties. This architecture enables scaling, effective resource use, and concern separation.

The distributed component architecture: The usage of distributed component architecture was mentioned by 16.7% of the respondents. With this strategy, the system is divided into modular parts that can communicate with one another across a network. Using a distributed component architecture can increase system scalability and flexibility.

Peer-to-peer architecture, or P2P architecture was mentioned by 16.7% of the respondents. This method eliminates the need for a centralized server by allowing systems to connect with one another directly. Although peer-to-peer architecture might encourage decentralization and direct data transmission, it may also present problems with data security and consistency. To address the data insecurity problem of the peer-to-peer architecture it is necessary to implement encryption, authentication, access control, authorization and integrity mechanisms.

These results show a variety of architectural strategies were used in developing medical systems. The architecture chosen can have a big impact on things like resource usage, scalability, data sharing, and system complexity. Multitier client-server architectures appear to be in demand due to their ability to balance scalability and concern separation. Knowing the architectural decisions might help reveal the business's top design priorities. For instance, the usage of distributed component design shows a focus on modularity and flexibility, but the adoption of peer-to-peer architecture may indicate a preference for decentralized communication. The results demonstrate a range of architectural strategies applied in the creation of medical systems. These architectural approaches inform the necessity of having medical systems that capture different levels of architectures to ensure secure and interoperable functionalities are realized.

4.2.8 Results from the Interview Schedules and Discussions of the Findings

Important new information on distributed ledger technology (DLT) security and interoperability in medical systems has been obtained via conversations with software developers of medical systems. Firstly, the range of medical procedures that developers work on shows that there are many potential applications in the healthcare sector. Second, developers agree that cooperative information sharing within the healthcare ecosystem is beneficial and that connectivity between medical systems from various medical software providers is vital. These medical systems must transmit critical healthcare data, such as prescription drugs, treatment plans, and medical records.

One significant finding is the identification of communication failures in medical systems, which prompted the creation of several distinct medical systems. The level of pleasure that developers have with different approaches varies. Some, however, are not satisfied with them and are willing to attempt different approaches. Software developers for medical systems are also searching for solutions to facilitate communication without having an immediate detrimental effect on their systems. This choice shows a significant desire to keep things compatible with the least disruption to how things are now done in medicine.

The components that make up the varied architecture of the medical information technology landscape have been revealed by investigations into the many applications of medical systems in various hospitals or healthcare institutions. The medical system software makers shared insights into how their systems manage and retain patient treatment information, demonstrating a commitment to effective record-keeping for follow-up care prescriptions or treatments. The handling of prescription data during patient transfers between healthcare institutions was also discussed, considering the use of portable media and internet exchanges.

The findings of the interview schedule demonstrated that, while building and developing their medical systems, medical systems software engineers had a thorough awareness of healthcare standards, laws, protocols, and architectures. The software developers of medical systems expressed their desire to integrate the standards into their systems and comply with medical systems requirements during a discussion on adherence to standards such as FHIR and others. The interview schedule also looked at how the current laws affected the development process, highlighting data security, privacy, and sharing issues. The purpose of the interview schedule was to provide medical system software developers with a forum to discuss important topics that impact the development of reliable, safe, and compatible medical systems in the ever-changing environment of stringent healthcare standards and laws.

Healthcare criteria for the National Strategy of Universal Healthcare Coverage and its implementation was thoroughly discussed throughout the interviews. Medical system software developers showed their dedication to data security and privacy by discussing how they safeguard patient medical data inside their medical systems. Based on the National Strategy for Universal Healthcare Coverage, preferences for peer-to-peer, and distributed data-sharing models were investigated. The results of these interviews provide a thorough grasp of the issues, remedies, factors, and concerns that medical system software developers would take into account with regard to implementing distributed ledger technology's security and compatibility with medical systems.

4.3 Algorithm to Enhance Security of Distributed Ledger (DL) Interoperability Framework for Medical Systems

In order to design an algorithm that would enhance security of distributed ledger interoperability across various medical systems, the study first designed an enhanced secure distributed ledger framework in form of an architectural layout. The enhanced

secure distributed ledger interoperability framework for medical systems is discussed in the subsequent sections.

This study designed an architectural layout for an enhanced secure medical distributed ledger interoperability framework in a multifaceted process through planning and consideration, with an aim to achieve security, confidentiality, integrity, availability, authentication, access control, scalability, interoperability of medical systems. Understanding the needs of different stakeholders, including patients, healthcare providers, and system administrators, was crucial in shaping the architectural layout design. Moreover, compliance with healthcare regulations, like Health Insurance Portability and Accountability Act (HIPAA), general data protection regulation (GDPR) and other Data Protection Acts, were factored into the design to ensure data privacy and security.

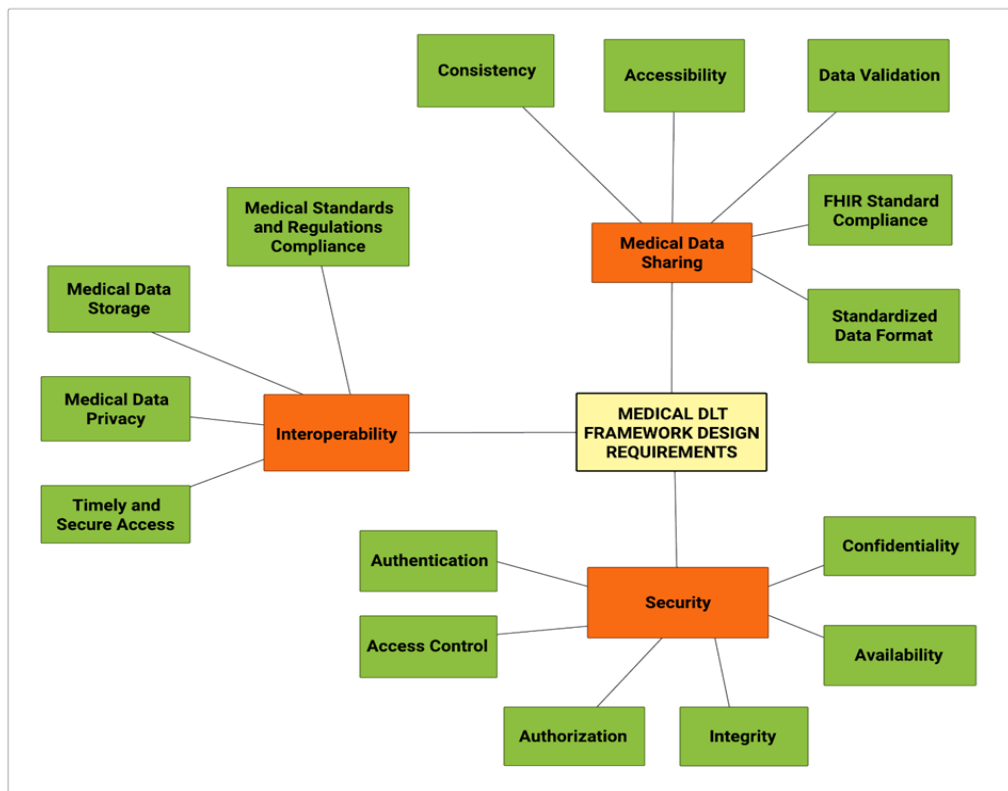
4.3.1 Secure Medical DLT Interoperability Architectural Framework Design Requirements

Designing an enhanced secure medical DLT interoperability framework calls for careful considerations of various requirements that aim at enhancing confidentiality, authentication, access control, integrity and availability of electronic medical records and medical systems. Some of the medical DLT system design requirements are interoperability, security and data sharing on the interoperability design requirement, the Medical DLT framework adheres to timely and secure access, adherence to the medical standards and regulations like HIPAA and HL7 FHIR standards, medical data storage regulations and medical data privacy. To achieve security as a requirement, the Medical DLT framework ensures confidentiality by encrypting medical records, authentication by implementing several layers of user authentication in order to access the patient electronic medical records (EMRs); authorization by enacting mechanisms for assigning

Medical DLT system user roles based on what they are authorized to access; integrity by ensuring that all electronic medical records are hashed before sharing and storage; access control by ensuring that all users are assigned a unique user name and password; and availability of electronic medical records via the Medical DLT System without considering where those patients' medical records were uploaded from. Lastly the medical data sharing requirement that encompasses data consistency, accessibility, data validation, HL7 FHIR data standardization and standardized of data formats and protocols was observed. All these design requirements are aimed at enhancing security and interoperability of medical systems. The medical DLT framework design requirements are as illustrated in Figure 21.

Figure 21

Secure Medical DLT Interoperability Architectural Framework Design Requirements



4.3.2 The Medical DLT Interoperability Framework Architectural Design Tools and Technologies Used

The enhanced secure distributed ledger interoperability framework architectural design layout implements a decentralized and secure electronic medical record (EMR) system. The secure medical DLT interoperability architectural design leverages various technologies, including Ethereum, InterPlanetary File System (IPFS), Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR) standard, and cryptographic encryption techniques such as Advanced Encryption Standard (AES), Diffie-Hellman Key Exchange (DHKE) and Elliptic Curve Cryptography (ECC).

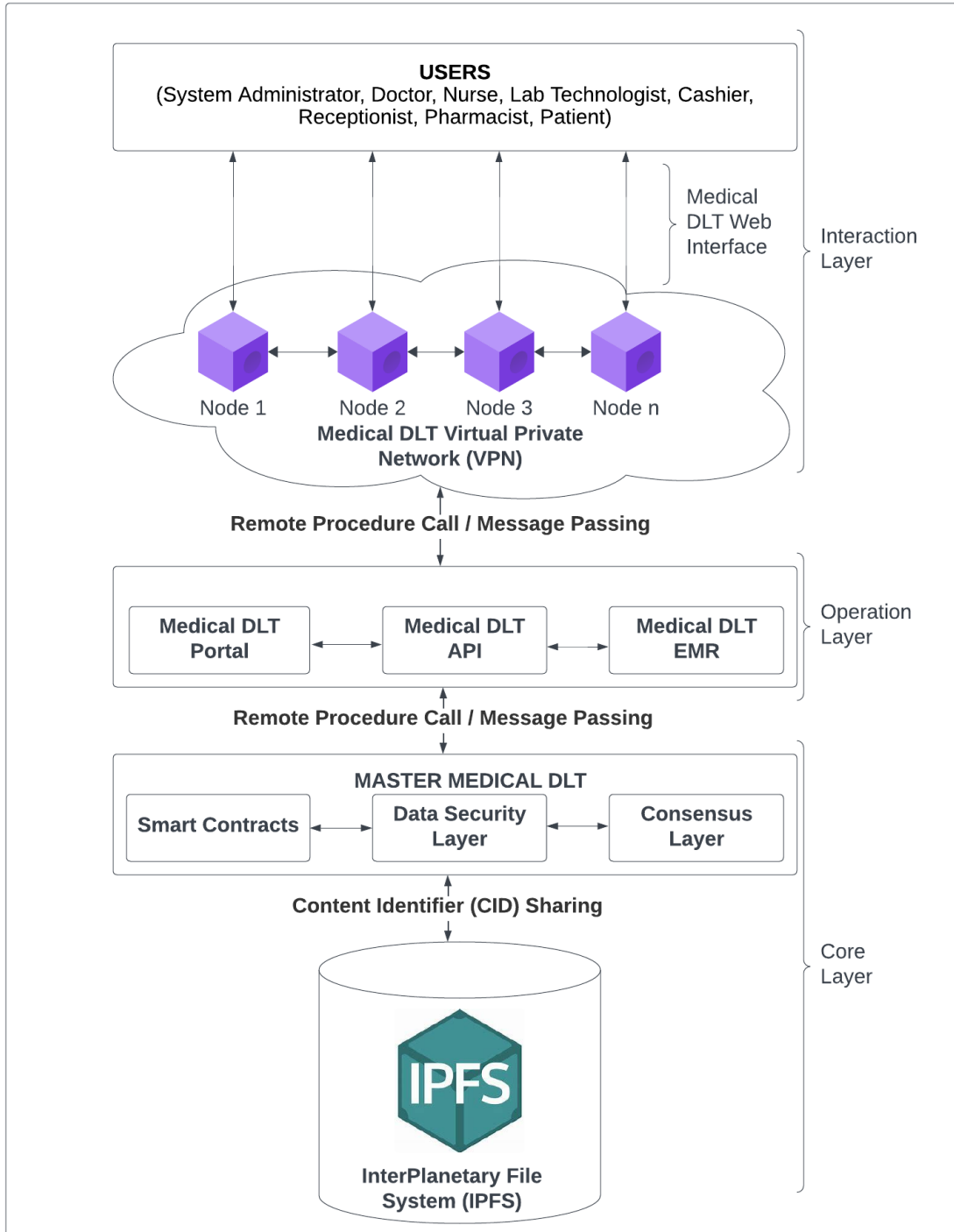
A distributed ledger technology (DLT) is employed to create an immutable record of EMRs, maintaining the integrity and security of patients' medical information. Patients, Hospital System Administrators and other healthcare providers like Doctors, Nurses, Lab Technologists and Pharmacists generate their wallets using MetaMask. The Medical DLT system also supports non-medical workers like the Cashier who is responsible for billing the patients, the insurance agents who are responsible for supporting the patients access and benefit from the insurance companies. Hospitals acts as the nodes in the proposed medical DLT Network.

4.3.3 The Enhanced Secure Distributed Ledger Interoperability Framework Architectural Layout

The enhanced secure medical distributed ledger interoperability framework architectural layout design is made up of core layer, operational layer and interaction layer as shown in Figure 22, and its description discussed in the subsequent sections.

Figure 22

The Enhanced Secure Distributed Ledger Interoperability Framework Architectural Layout



i. Core / Technical Layer

This layer is made up of the InterPlanetary File System (IPFS) and the Master Medical DLT which encompasses the smart contracts, data security layer and consensus layer.

a) InterPlanetary File System (IPFS)

InterPlanetary File System (IPFS) is a protocol and network intended to create a peer-to-peer method of storing and sharing files and hypermedia in a distributed ledger network. It applies a content addressing mechanism to uniquely identify and retrieve files based on their content rather than relying on their tradition storage location-based address. Each file is assigned a cryptographic hash to ensure integrity and to be tamper resistant. IPFS utilizes the MerkleDag data structure and a caching mechanism, hence optimizing on its efficiency and enabling seamless content identification and discovery.

To address the data insecurity concerns of using the peer-to-peer architecture IPFS incorporates encryption mechanisms to protect data in transit and at rest within the peer-to-peer network. It also implements authentication, access control and authorization mechanisms to authenticate participants and enforce access control policies and authorization mechanisms to restrict unauthorized access to sensitive data and resources within the P2P network. IPFS finds applications in various domains, from sharing large files to supporting the development of decentralized applications (dApps), offering a strong and censorship-resistant approach to data storage and distribution. In the Medical DLT System, the IPFS stores the actual Patient files and then generates Content Identifier (CID). The CID is added to the Medical DLT, and the transaction ID is returned to Patients Wallet for future reference.

b) Master Medical DLT

Master Medical DLT layer hosts the master healthcare administrator module that allows the healthcare regulating bodies to create and accredit health facilities (nodes) to join the Medical DLT Network. The Master Medical DLT layer is also made up of the smart contracts, data security layer and the consensus layer as discussed in the subsequent sections.

i. Smart Contracts

Smart Contracts are self-executing contract code that has terms of agreements to be executed between participating parties. In the Medical DLT framework, smart contracts layer governs the rules for data sharing and access control. The Smart contract properties represent a data schema that is used in the entire Medical DLT system. Smart contracts enable participating parties in the distributed ledger network to gain trust without any interventions from third parties or intermediaries.

ii. Data Security Layer

Data Security Layer achieves security via applying several layers of cryptographic mechanisms and techniques. This aims to ensure confidentiality, privacy, integrity, authentication, authorization, access control, and availability of the patients' electronic medical records has been achieved. Data security ensures that the data created, shared and stored in EMRs adhere to the data protection standards and regulations supported by the healthcare sector. This layer defines the data security structure of the enhanced secure DL interoperability framework for medical systems. Medical DLT system supports data encryption using Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) encryption algorithms. For secure key exchange between nodes (health facilities) in the distributed ledger network, Diffie-Hellman Key Exchange

(DHKE) algorithm is used. To achieve integrity, keccak256 hashing algorithm has been deployed into the Medical DLT System.

To ensure the Electronic Medical Records (EMRs) adhere to globally accepted standards and regulations, the Medical DLT System uses Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR) standard to ensure medical data standardization. Patient medical data is encrypted before storage and before sharing it to ensure confidentiality and privacy is achieved. To allow the patient to sign their electronic medical records (EMRs) before updating them to the Medical DLT Elliptic Curve, Digital Signature Algorithm (ECDSA) is used for generating the digital signature. This enables each patient to generate their private digital signature stored in the patient wallet, and other participants in the Medical DLT can verify the signature using the associated patient public key. A distributed ledger technology (DLT) is employed to create an immutable record of EMRs that can be referenced in future.

iii. Consensus Layer

Consensus Layer is responsible for reaching consensus on the validity of transactions and maintaining the integrity of the Medical DLT network. This layer is responsible for achieving agreement among participating nodes (health facilities) in the Medical DLT network. It also aids the nodes in achieving consistency and shared view, preventing malicious activities and updates. Unlike in Bitcoin that applies Proof of Work and Proof of State consensus algorithms and others, the Medical DLT applies Proof of Authentication (PoA) consensus algorithms to authenticate the authorized users (participants) in the Medical DLT network.

ii. **Operational Layer**

This layer encompasses the Medical DLT Portal, Medical DLT API and Medical DLT EMR. The description of each of these modules is as discussed in the subsequent sections.

a) **Medical DLT Portal**

Medical DLT Portal is a web interface that links the medical DLT API to the MetaMask to allow users such as patients to generate their wallets. It also links the Medical DLT system to the Medical DLT API to allow the execution on smart contracts, encryption, hashing and signing of patients' medical files before adding them to the Master Medical DLT System or fetching the patients' electronic medical records (EMR) from the Master Medical DLT.

Medical DLT also allows each health facility (hospital) system administrator to create a health facility (hospital) wallet that in turn is used to generate the Content Identifier (CID) to be used by patients to identify authorized health facilities (hospital). Each health facility (hospital) has a system administrator who generates a health facility (hospital) wallet which is localized to the hospital. The health facility (hospital) system administrator activates the Medical-DLT Virtual Private Network (VPN), for example, using WireGuard for their specific health facility (hospital), using the accredited login credentials. The health facility (hospital) system administrator then creates the administrator (Admin) wallet using MetaMask to be used to link the health facility (hospital) to the Master Medical DLT, Medical DLT Portal and Medical DLT EMR in conjunction with the health facility (hospital) wallet.

b) Medical DLT API

The Medical DLT API (Backend) is an abstract layer that has no Graphical User Interface (GUI). The medical DLT Application Programming Interface (API) serves as a crucial intermediary that allows the Medical DLT and the Medical EMR to communicate, exchange data and seamlessly integrate with one another. It facilitates the sharing of medical information across the medical systems hence enhancing interoperability and enables the creation of a connected healthcare ecosystem.

Medical DLT API enables the Medical DLT EMR system to exchange patient data securely, while allowing medical practitioners and healthcare providers to access up-to-date and accurate information across different healthcare facilities.

Medical DLT API also integrates with other information systems that support service delivery to patients like the insurance systems and the financial billing systems. Medical DLT API allows and supports integration with other third-party services that enhance the overall functionality and capabilities of the medical systems. To provide interoperable and standardized medical systems, Medical DLT API plays a key role in improving the efficiency of healthcare operations, thus ensuring data accuracy and better patient care. The utilization of a medical DLT system API exemplifies the power of distributed ledger technology in creating a more interconnected and collaborative healthcare environment.

c) Medical DLT EMR

A Medical DLT Electronic Medical Record (EMR) is a digital repository that stores comprehensive and real-time patient medical information, replacing the traditional paper-based records. The medical DLT EMR plays a very crucial role in enhancing interoperability of medical systems by providing a standardized electronic format for creating, capturing, processing, managing, and sharing patient data across various healthcare facilities that are using different medical systems that have been developed by

different vendors. Medical DLT EMR stores patient medical data that cuts across demographic data, consultation data, treatment data, diagnosis data, laboratory tests data, medical history data and medications among others. Interoperability is achieved through the capability of Medical DLT EMR to integrate with other medical systems, such as the medical laboratory systems, radiology systems, and finance billing systems. The medical DLT supports standardization of patients' medical data by integrating Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR) standards and Clinical Data Interchange Standards Consortium (CDISC) for standardization of data for laboratory tests and clinical trials.

Additionally, it makes use of the international categorization of Diseases (ICD), a worldwide categorization system for illnesses, medical disorders, and associated data. ICD-10 and ICD-11 are two classifications in ICD. While ICD-11 is the most recent version which offers a more intricate and contemporary coding system, ICD-10 is still commonly utilized for diagnosing conditions. The Medical DLT EMR also the Logical Observation Identifiers Names and Codes (LOINC), a standard for identifying health measurements like the patient vitals, observations, and documents. It standardizes the names and codes used in laboratory tests, making it easier to exchange and integrate laboratory data across different medical systems. The Medical DLT also integrates Systematized Nomenclature of Medicine - Clinical Terms (SNOMED CT) which is a comprehensive clinical terminology system used to capture and represent clinical information in electronic medical records (EMR). SNOMED CT offers a consistent representation of clinical ideas, which improves the interoperability of medical systems. Healthcare providers are able to access a comprehensive view of a patient's medical history, which facilitates better decision-making, streamline workflows, and improve continuity of care.

Lastly the Medical DLT EMR incorporates the Digital Imaging and Communications in Medicine (DICOM) a standard that is responsible for transmitting, storing, and sharing patient medical images, including those that are generated by diagnostic imaging equipment like the X-Rays, Computed Tomography (CT) scan, Ultrasound and Magnetic Resonance Imaging (MRI) among others. This promotes interoperability in the field of medical imaging by integrating the Medical DLT system to the medical Imaging systems. Interoperability of medical systems is made possible by the enhanced secure Medical DLT interoperability framework's design, which makes the Medical DLT EMR global, decentralized, and accessible to all accredited medical facilities. The medical DLT's adoption is a critical step towards creating a more integrated and cooperative healthcare ecosystem that improves patient outcomes by encouraging improved communication among medical practitioners.

iii. Interaction/ Application Layer

This layer includes the Medical DLT web user interface and application logic layer for accessing and sharing patient EMRs. It also encompasses the Virtual Private Network (VPN) and the Remote Procedure Calls (RPC) for message-passing.

a) Medical DLT User Application Layer

The Medical DLT web-based user application layer represents the top layer in the medical DLT system architecture layout and it provides the interface for the users to interact with different Medical DLT system functionalities. This layer encompasses an interface to the medical DLT EMR that is used by the healthcare providers to manage patient's data, appointments, remote consultations, patient scheduling applications and patient web portals. This layer offers the medical system administrator a platform to add other health workers and users to the Medical DLT System. It offers a graphical user interface that can be used by healthcare professionals, medical system administrators and

the patient a seamless experience when interacting with the Medical DLT System. It facilitates health practitioners to perform tasks such updating patient electronic medical records, accessing patients' diagnostic reports, managing appointments and sharing or communicating with other healthcare professionals securely. The Medical DLT user application layer complies with the software design principles of user interface (UI) and user experience (UX) for usability, efficiency and accessibility, usability and efficiency, to ensure effectiveness and interoperability of the enhanced Medical DLT web-based system. The medical DLT user application layer supports a variety of user interfaces that supports users and user interfaces such as the health facility (hospital) system administrator (admin), medical practitioners, patient and other healthcare facility workers/staff like the cashier. The specific subsections of the enhanced interoperability Medical DLT user application layer is discussed in the following sections.

i. System Administrator (Admin) module

This module allows the healthcare facility (hospital) medical system administrator to create and add different medical user, roles to the Medical DLT system and Portal. These user roles give the users operational access permission levels when using the Medical DLT System. This aids in the authentication and authorization of the medical healthcare professionals as users in the system. The medical system administrator uses MetaMask to generate and create the health facility (hospital) administrator wallet. Medical system administrator has login credentials and password to aid them to access the medical DLT system, and the medical system administrator wallet, which has the Public Key (Pu), Private Key (Pr) used to encrypt the healthcare facility private information.

ii. Patient Wallet Module

The patients' wallet module uses MetaMask to allow patients to create a patients' wallet. It allows the patient to generate a pair of Keys, Public Key (Pu), Private Key (Pr) used

for encrypting patients' electronic medical records (EMRs), additional Symmetric Key (SK) that is used by the patient to sign and authorize the medical practitioners in a given healthcare facility (hospital) to add and view their historical patients' electronic medical records (EMRs). Secondly, the Patient Symmetric Key (SK) is also used by the patient to sign, authenticate and verify their electronic medical records (EMRs), before the Doctor is allowed to add new medical records into the Master Medical DLT.

iii. Medical Practitioners Module

It allows authorized Medical Practitioners to create their wallets (Individualized). Each medical practitioner is expected to generate their wallet using MetaMask, which has a pair of Public Key(Pu) and Private Key (Pr) to be used in the Medical DLT System especially when adding or referencing/fetching the patient electronic medical records. Additionally, the medical practitioners or healthcare workers, like Doctors, Nurses, Receptionists, Lab Technologists, Pharmacists and Cashiers are also system users with different roles, hence requiring to be authenticated to use the Medical DLT System effectively.

iv. Remote Procedure Calls (RPC) or Message passing

Remote Procedure Calls (RPC) or message passing are communication protocols that enables the medical DLT program in one health facility to execute procedures or functions on another healthcare facility address space (commonly on a remote server) as if those procedures and functions were local procedures. This implies that RPC allows a program from a remote machine in a healthcare facility to request a service from another medical program located on another computer of a different healthcare facility as if it were a local function call within the same local area network. RPC are a crucial pillar supporting interoperability of medical systems by supporting seamless communication and data exchange between different medical system software from different vendors,

and using different devices. RPC acts as the interlink between the Master DLT, InterPlanetary File System (IPFS), Medical DLT Portal, Medical DLT API, Medical DLT EMR and the Medical DLT web-based user interface.

v. Medical DLT Virtual Private Network (VPN)

The medical DLT virtual private network (VPN), also known as Medical DLT Interlink Network, support Remote Procedure Calls (RPC) and aids different medical facilities to link to the Master Medical DLT, Medical DLT Portal, Medical DLT EMR and InterPlanetary File System (IPFS). It spans the transport layer and the application layer of the network communication across the distributed ledger network. This layer also provides a link between the Medical DLT and the Nodes (health facilities /hospitals) via a secure virtual private network (VPN). It also establishes a secure and trusted medical environment or ecosystem for all communicating nodes, hence providing secure interoperability of medical systems. The developed peer-to-peer network architecture utilizes role-based access control (RBAC), access tokens, or cryptographic keys to control access permissions and ensure that only authorized peers can access or modify data. It also implements data validation and integrity checks mechanisms to verify the accuracy, completeness, and consistency of data exchanged between peers. Uses checksums, cryptographic hash functions, or digital signatures to detect data tampering, corruption, or unauthorized modifications during transmission or storage in the P2P network.

4.3.4 Patient Hospital Visit Instance Workflow

a. Patients Module

Patients visit any approved healthcare institutions like a hospital of their choice to seek treatment. Upon arrival to the hospital the patient is expected to have generated the patients' wallet that stores their Public Key (Pu), Private Key (Pr) for encryption of their

patients' medical data, also known as patients' personal health information (PHI), and Symmetric Key that is used as a session Key (K) when signing their patients' electronic medical records (EMRs) before saving and updating them on the medical DLT EMR. The patient also uses the Symmetric key to authorize access to their historical patients' electronic medical records by the authorized medical practitioner.

b. Hospital Medical System Administrator (Admin) Module

Each hospital is expected to have a medical system administrator whose mandate is to install and setup the medical DLT System to their specific hospital. Additionally, the medical system administrator is expected to generate the hospital wallet that has the hospital Public Key (Pu) and Private Key (Pr). Further, the medical systems administrator also creates different system users and defining their roles into the Medical DLT System. Some roles of these users include Receptionist, Nurses, Doctors, Lab Technologists, pharmacists and Cashier. These roles define the operational permission levels of the users when using medical DLT system.

c. Receptionist

The receptionist logs into the Medical DLT System using their approved user name and password. Then, they identify and register the patients into the Medical DLT system using their approved credentials, which in turn initiates the hospital visit workflow. If the patients already exist in the medical DLT system, the receptionist only initiate a new hospital visit instance.

d. Nurse at Triage

The Nurse serving patients at the triage logs into the Medical DLT system using their username and password, after which they take and record the patients' vitals details into the medical DLT system.

e. Consultation Doctor

The Doctor logs into the Medical DLT System using their username and password. The Doctor then seeks consent from the patients to allow access of historical patients' electronic medical records. Upon accepting to give consent, the patients use their patients' wallet which stores their Public Key (Pu), Private Key (Pr) and symmetric key (K) to sign and authenticate the Doctor to access and update their electronic medical records (EMRs). The Doctor reviews the historical EMRs and the patient's progress, then sends the patient for lab investigations.

f. Lab Technologists

The lab Technologists then logs into the Medical DLT System using their user name and password. The lab technologists then conducts medical lab investigations and test as recommended by the consulted Doctor. The Lab Technologists then records lab investigation reports into the system to be accessed by the Consultation Doctor.

g. Consultation Doctor

The Consultation Doctor then signs into the Medical DLT system to access the Lab Technologist investigation reports. Then prescribes the treatment and updates the patient's electronic medical records on the Medical DLT System and refers the patients to the pharmacists.

h. Pharmacists

The Pharmacists signs into the Medical DLT System using their username and password. Then adds the drugs and other hospital receivables to update the stock-in module. The Pharmacist then adds the drugs dispensed to the patient to the Medical DLT System, and refers the patient to the Cashier.

i. **Cashier**

The Cashier logs into the system using their username and password into the Medical DLT System. Then bills the patients and closes the patients' hospital visit instance upon receiving the patients bill payment.

j. **Hospital Medical System Administrator (Admin) Module**

Upon closure of the patient's hospital visit instance, the admin pushes the patient FHIR compliant Encrypted, Hashed and Signed Electronic Medical Record event to the Medical DLT System which only stores the Content Identifier (CID) generated by the InterPlanetary File System (IPFS).

k. **InterPlanetary File System (IPFS) Module**

This module stores the actual patients' medical files and then generates content identifier (CID) for each Patient Medical File stored and maps the CID to the Medical DLT for storage. The patients' medical data saved into the medical files is encrypted, hashed and signed using the Patients Wallet details before storage into the IPFS.

l. **Master Medical DLT System**

The Master Medical DLT System stores the patient's content identifier (CID) and updates patients' wallets for future reference.

4.3.5 High level Workflow Design for Patient Hospital Visit Instance

The high-level algorithm that shows and explains the architectural workflow for a patient hospital visit instances from when a patient gets to the hospital until when the instance is closed.

Step 1: Patient Visits Hospital

- The patient arrives at the hospital to seek medical care.

Step 2: Generate Patient Wallet

- A patient wallet is generated to securely store the patient's health records and keys.

Step 3: Hospital Receptionist Identifies & Registers Patient

- The hospital receptionist identifies and registers the patient in the hospital's system.
- The patient's registration is linked to their Patient Wallet and the Hospital Wallet.

Step 4: Nurse at Triage Takes & Records Patient Vitals

- The nurse at triage takes and records the patient's vital signs.
- The data is recorded and associated with the patient's Public Key (Pu) and Symmetric Key (SK).

Step 5: Consultation with Doctor

- The patient consults with a doctor.
- The doctor adds the consultation record to the Medical Distributed Ledger Technology (DLT) Electronic Medical Record (EMR) using their Doctor Public Key (Pu), the Patient Public Key (Pu), and the Patient Symmetric Key (SK).

Step 6: Lab Technologist Conducts Lab Investigation

- The lab technologist carries out lab investigations and adds the investigation report using their Lab Technologist Public Key (Pu), the Patient Public Key (Pu), and the Patient Symmetric Key (SK).

Step 7: Consultation with Doctor (Lab Report Interpretation)

- The doctor reads and interprets the lab test report.
- The doctor adds the treatment plan to the Medical DLT EMR using their Doctor Public Key (Pu), the Patient Public Key (Pu), and the Patient Symmetric Key (SK).

Step 8: Pharmacists Dispenses Medication

- The pharmacist adds the dispensed drugs to the patient's records using their Pharmacist Public Key (Pu), the Patient Public Key (Pu), and the Patient Symmetric Key (SK).

Step 9: Cashier Bills the Patient

- The cashier calculates the bill for the patient's visit and closes the patient's visit instance.

Step 10: Hospital Admin Pushes Patient FHIR-Compliant EMR to Medical DLT

- The hospital administrator pushes the patient's FHIR-compliant Electronic Medical Record (EMR) event to the Medical DLT.
- The EMR event is encrypted, hashed, and signed for security.

Step 11: InterPlanetary File System (IPFS) Generates Content Identifier (CID)

- IPFS generates a Content Identifier (CID) for each patient file stored on the distributed file system.

Step 12: Map CID to Medical DLT

- The generated CID is mapped to the Medical DLT for storage and future reference.

Step 13: Medical DLT Stores Patients' CIDs

- The Medical DLT securely stores the Patients' CIDs for future reference and data retrieval.

End of patient hospital visit instance

4.3.6 A Detailed High-Level Explanation of the Enhance Secure Distributed Ledger

Interoperability Framework Algorithm

Enhancing the security of patients' medical data and information when using medical systems and the electronic medical records (EMRs) is paramount and a regulatory requirement by the healthcare regulating bodies. To achieve the security of patients' medical data and protect sensitive patients' medical data while ensuring integrity of transactions across multiple medical systems, an enhanced secure Distributed Ledger (DL) Interoperability Framework for medical systems is of utmost importance. To achieve secure interoperability of medical systems, the developed Medical DLT

interoperability framework is further expounded and explained in an algorithmic form. The designed algorithm is made up of steps that outline the approach taken by the enhanced secure DL interoperability framework, to achieve the security of patients' medical data in medical systems. The algorithm focuses on steps, which include definition of requirements, implementation of robust access control mechanisms, secure communication, consensus management, data encryption, privacy preserving techniques, immutable audit trails, data validation, data ownership and consent, storage backup and recovery, and Regular updates and path management.

A detailed high-level explanation of each step followed in generating the algorithms is discussed systematically in the subsequent section.

a. Define Security Objectives / Requirements

The study began by clearly defining the security objectives and requirements necessary for achieving secure DL interoperability framework. The study identified confidentiality, integrity, authenticity, access control, regulatory compliance and availability of medical data to be key requirements in achieving secure interoperability of medical systems.

b. Implement Robust Access Control Mechanisms

The study then designed a Medical DLT Interoperability Framework that implements robust access control mechanisms to restrict access to authorized users and nodes. The framework requires every user to create a user login account that has username and password in order to access the Medical DLT system and Medical DLT EMR. Additionally, each user is required to create user wallet that utilizes cryptographic keys (Public Key and Private Key) and digital signatures for authentication. The framework also allows the medical DLT administrator to define role-based access control and

permissions. Lastly, it ensures that only authorized nodes and users can read or write to the medical DLT ledger.

c. Secure Communication Channel

The developed Medical DLT Interoperability Framework ensures secure communication channels between ledger nodes. The use of Transport Layer Security (TLS) for encryption and secure socket communication has been achieved. The framework also implements message-level encryption, message authentication via use of digital signatures and hashing of data to prevent unauthorized data tampering and ensure data integrity.

d. Apply the Proof of Authentication (PoA) Consensus Mechanism

The Medical DLT Interoperability Framework applies Proof of Authentication (PoA) consensus algorithm that aligns with the desired level of security. This consensus algorithm aids in authenticating and validating the nodes and ensuring that only validated transactions are added to the ledger. Patients hold the authority to authenticate the medical practitioners who access and modify their medical records within the medical DLT and Medical DLT EMRs by use of their symmetric key.

e. Encryption Data Before Storing

The developed Medical DLT Interoperability Framework encrypts sensitive patients' data before storing it in the ledger. It utilizes robust encryption algorithms and key management systems to protect patient electronic medical records (EMRs).

f. Implement Privacy-Preserving Techniques

The Medical DLT Interoperability Framework implements privacy-preserving techniques such as zero-knowledge proofs, homomorphic encryption, multi-party computations or confidential transactions to protect sensitive patients' medical data when

sharing medical data without revealing the actual information while maintaining interoperability.

g. Maintain Immutable Audit Trail

The Medical DLT Interoperability Framework maintains an immutable audit trail of all transactions which includes the history of access and modifications on the Medical DLT ledger. It also implements versioning and time stamping which enables accountability and traceability.

h. Perform Data Validation

The Medical DLT Interoperability Framework uses smart contracts to validate incoming data and ensure it adheres to predefined healthcare HL7 FHIR standards and data formats.

i. Implement Data Ownership and Consent

The Medical DLT Interoperability Framework implements a consent based electronic medical record (EMR) management system that allows patients to control access to their medical data. It implements a patient-controlled consent model, which has a granular consent settings and logging of patient approvals by using an extra layer of security where patients authorize access and update their medical data using a symmetric key known to the patient only.

j. Implement A Robust Storage, Backup and Recovery Measures

The Medical DLT Interoperability Framework implements a robust storage, backup and recovery measures to ensure that patient medical data can be stored for future reference and restored in case of data tampering or loss. This framework implements InterPlanetary File System (IPFS) that stores the patient files, then in turn creates a

Content Identifier (CID). This CID is subsequently incorporated into the Medical DLT, and the transaction ID is provided to the patient's wallet for future reference.

k. Regular Updates and System Security Patch Management

The Medical DLT Interoperability Framework keeps all components of the interoperability up-to-date with the system security patches and updates to mitigate known security vulnerabilities and threats.

4.3.7 Notations adopted in the Enhanced Secure Distributed Ledger Interoperability Framework Algorithm for Medical Systems

To expound on the security and interoperability of the medical systems, this study developed more specific and detailed algorithms to illustrate how to enhance secure distributed ledger interoperability framework algorithms works, the resulting specific algorithms are as discussed in the subsequent sections. The developed enhanced secure distributed ledger interoperability framework algorithms for medical systems used various notations as shown in Table 12.

Table 12*Summary of the Notations used in the Developed Framework Algorithms*

Symbol	Description
N	Node (N) which represents a health facility / hospital
ID _N	An identification (ID) informs of content identifiers (CIDs) assigned to a Node (N)
ID _P	Identification assigned to a random patient attending any registered Node for treatment
ID _W	Identification assigned to an authorized staff / worker at a Node
B _E	An encrypted block
B _D	A decrypted block of random Patient (P)
B _S	A signed block
B _H	A hashed block
B _P	An encrypted, signed and hashed block created or appended to existing block of random Patient (P)
PU _P	Public Key of a Patient (P)
PR _P	Private Key of Patient (P)
SK _P	Symmetric Key of Patient (P)
PIN	Patient PIN

4.3.8 Proof of Authentication (PoA) Algorithm

This algorithm shows the process that the patient uses to authenticate the Node_i representing the healthcare facility (hospital) in order to allow the health facility health professionals to offer medical services to the patient. It is also used by the Patient to authenticate the medical practitioners who are authorized by the health facility to add or retrieve the patients' EMRs to the medical DLT. The proof of authentication algorithm uses different variable parameters, such as Hid to represent Hospital ID, Pid to represent Patient ID and Wid to represent Worker ID.

Algorithm: Proof of Authentication

Input: ID_N, ID_P, ID_W

Output: B_P // Encrypted, signed and hashed random patient (P) clock

Step 1: Register Node N (ID_N) to DLT Block

Step 2: If Success (Node N) == True {

For Worker in Node N

If exists (worker) == True

Error {Worker already registered}

Else

Register Worker (ID_W)

}

Step 3: Worker Login

Step 4: If Authentication Worker (ID_W) == True

Grant Login;

Else

Reject Login;

Step 5: If True in Step 4

If exists (Patient (ID_P)) == True

Error {Patient Exists}

Else

Register Patient;

Step 6: If Register (Patient (ID_P)) == True

Activate (Patient)

Step 7: If Exists (Record) == True

Fetch Record ()

Else

Create Record ()

Step 8: If success in Step 7

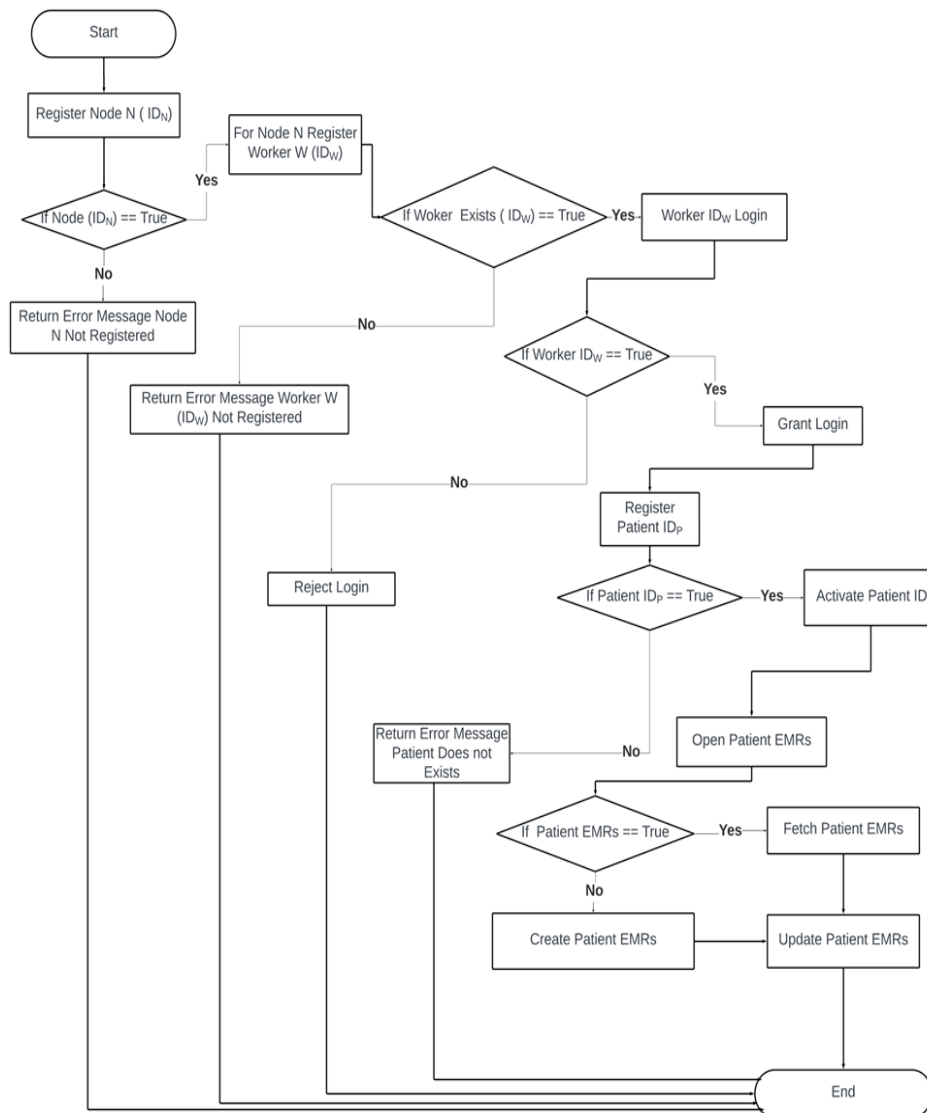
Update Medical DLT

Step 9: End

The proof of authentication algorithm is further represented in a flowchart as shown in Figure 23.

Figure 23

Fetch Record Algorithm Flowchart



4.3.9 Fetch Record Algorithm

The Fetch Record Algorithm is used to show how healthcare professional (Doctor) is going to retrieve the patient historical electronic medical records (EMRs) from the medical DLT, regardless of which health facility entered them to the Medical DLT system. The Fetch Records Algorithm uses patient Id to search for the patient historical electronic medical records (EMRs) and then uses the symmetric key to sign the consent of accepting the EMRs to be retrieved and accessed by the authorized healthcare professional (Doctor).

Algorithm: FetchRecord

Input: ID_P , SK_P , ID_N

Output: B_P // An encrypted signed and hashed block created or appended to existing block of random Patient (P)

Step 1: Start

Step 2: For ID_P in ID_N : //Loop through CIDs to check the patients in Node N Block

If Success (SK_P)==True

Return B_P ;

Else

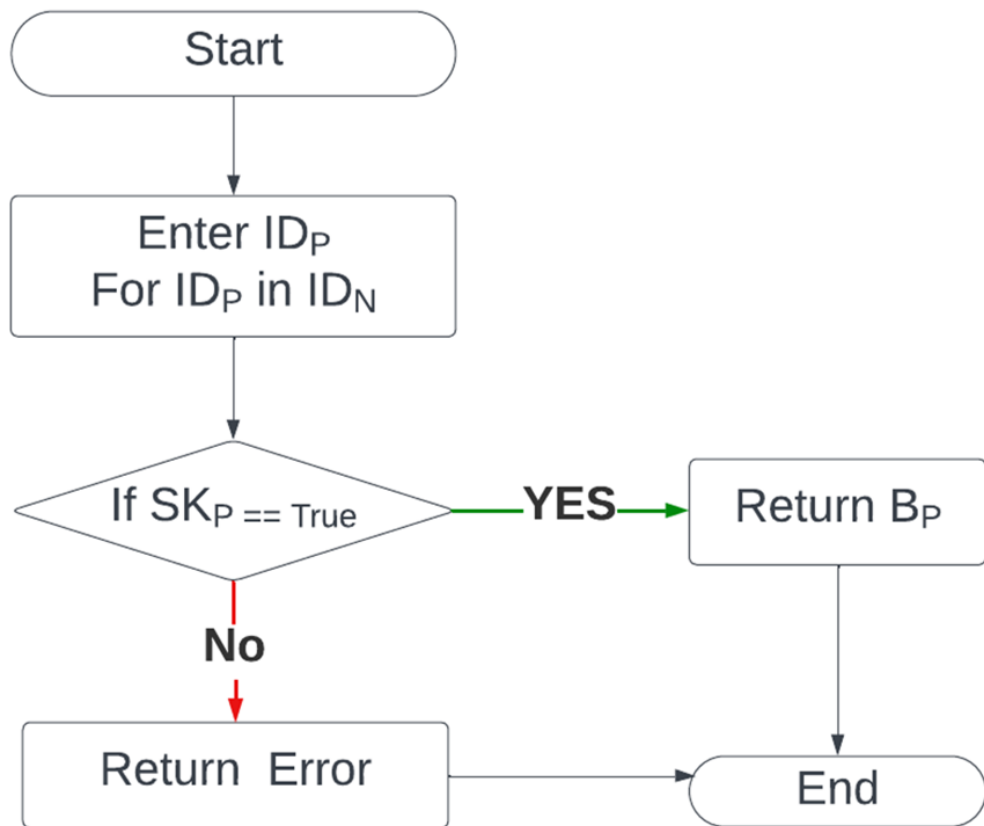
Return Error;

Step 3: End

The Fetch Record algorithm is further represented in a flowchart as shown in Figure 24.

Figure 24

Fetch Record Algorithm Flowchart



4.3.10 Create Record Algorithm

The Create Record Algorithm is used to show the process that is taken by the authorized healthcare professional (Doctor) to create and add new patient electronic medical record (EMR) to the Medical DLT System. The algorithm uses Patient ID variable to identify and verify the patient, and uses the symmetric Key for the patient to authenticate the healthcare professional (Doctor) and give consent to allow them create a new patient electronic medical record and add it to the Medical DLT System.

Algorithm: Create Record

Input: ID_P, SK_P

Output: B_P

Step 1 Start

Step 2: For ID_P in ID_N

 Enter SK_P

 If $SK_P == True$

 Return B_P

 Else Return Error {Patient Wrong Symmetric Key En-

tered}

Step 3: Push B_P to ID_N // Medical DLT Ledger

Step 4: Generate Patient Record CID

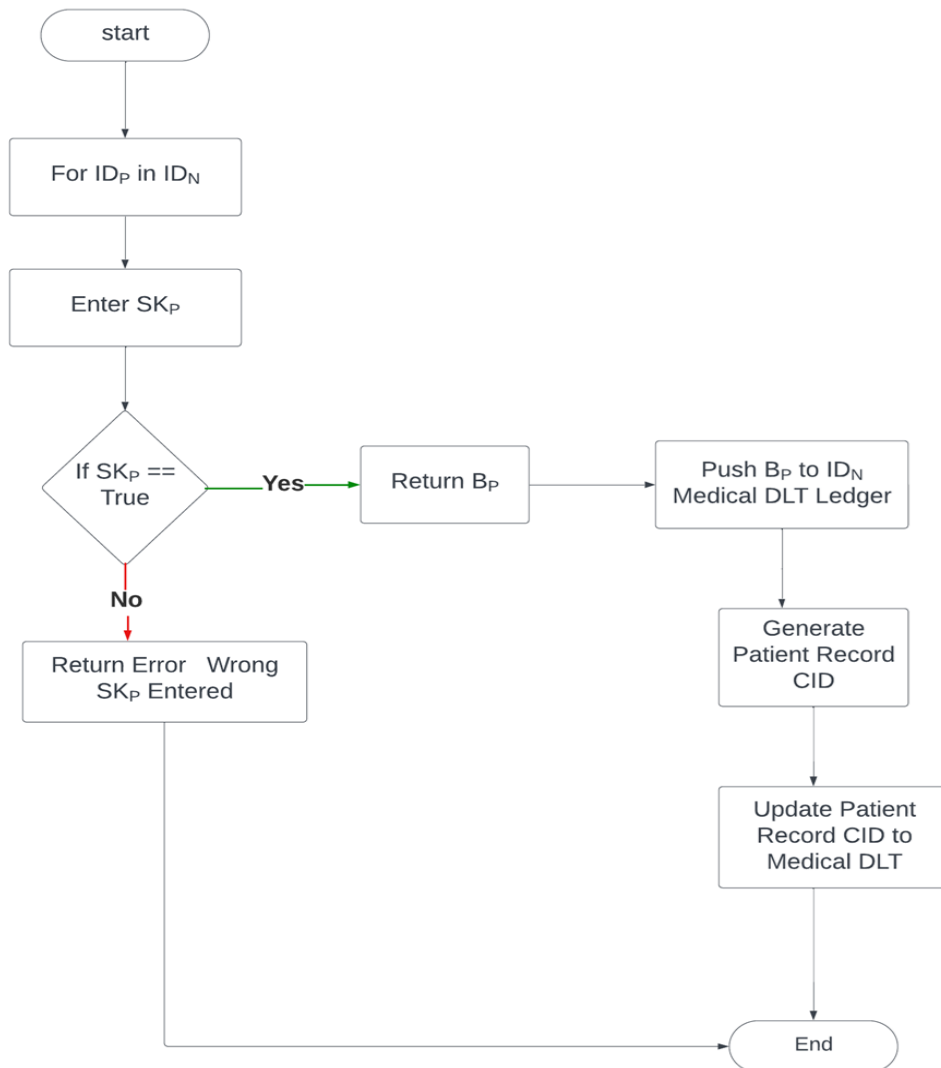
Step 5: Update Patient Record CID to Medical DLT

Step 6: End

The Create Record algorithm is further represented in a flowchart as shown in Figure 25.

Figure 25

Create Record Algorithm Flowchart



4.3.11 Create Patient Wallet Algorithm

The create-patient wallet algorithm shows the process that is taken to aid the patient to create the patient wallet that has the Public Key (Pu_P), Private Key (PR_P) and Symmetric Key (SK_P). The process relies on patient ID which can be the patient username used for identification and the patient PIN which is used for authenticating the patient when accessing the wallet.

Algorithm: Create Patient Wallet

Input: ID_P and Patient PIN

Output: Wallet $\{PU_P + PR_P + SK_P\}$

Step 1: Start

For ID_P and Patient PIN in Wallet

Enter ID_P and Patient PIN

if Correct ($ID_P + PatientPIN$) == True

Return $\{PU_P + PR_P + SK_P\}$

Else

Return Error

Step 2: Generate Patient Wallet ($PU_P + PR_P + SK_P$)

Step 3: Retrieve Patient Wallet Private Key

If (Patient Wallet PIN) == True

Return {Patient PR_P }

Else

Return Error (Wrong PIN)

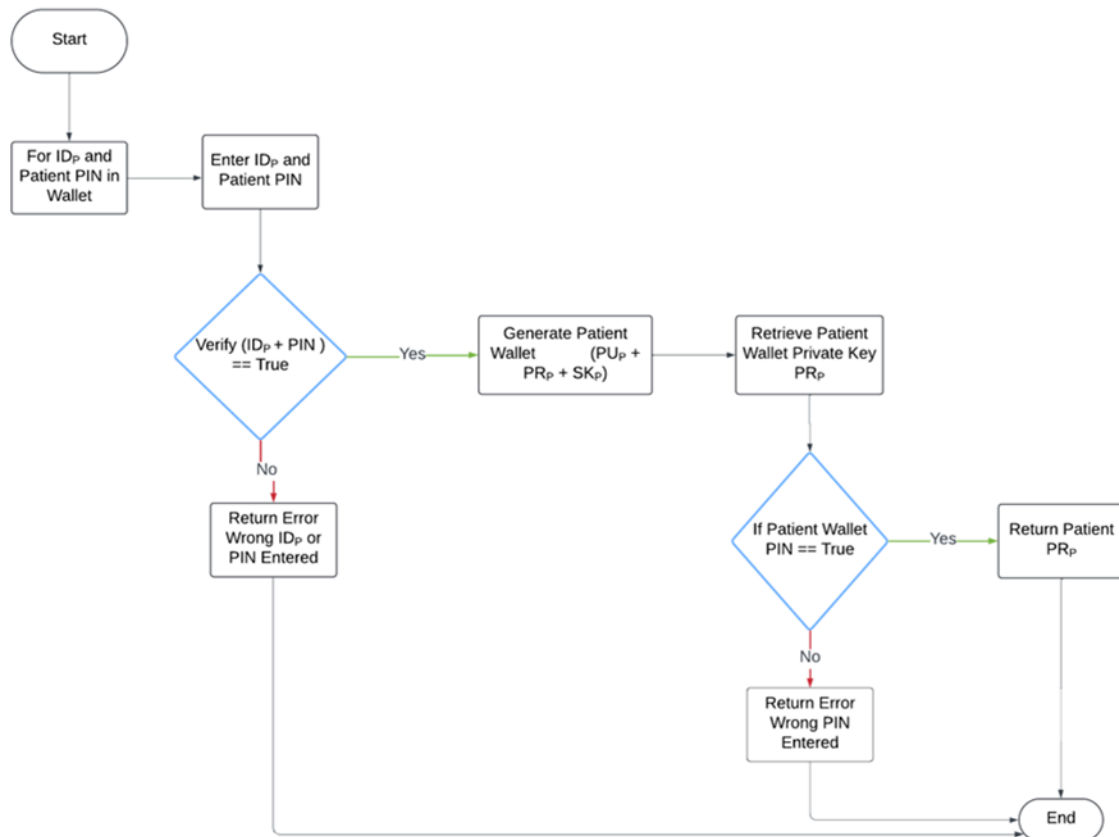
Step 4: End

The Create Patient Wallet algorithm is further represented in a flowchart as shown in

Figure 26.

Figure 26

Create Patient Wallet Algorithm Flowchart



4.3.12 Generate and Store Symmetric Key (SK) Algorithm

This algorithm demonstrates the process that the patient uses to generate and store the symmetric key that is used to authenticate the authorized healthcare professional (Doctor), and also to grant or revoke access to the accredited health facility. The patient generates the symmetric key after authenticating that they are the owners of the Patient wallet by providing a valid PIN and other wallet details, that is, the Public Key (PU_p) and Private Key (PR_p).

Algorithm: GenerateandStoreSymmetricKey

Input: Pin, PU_p, PR_p

Output: SK_p

Step 1: Start

Step 2: Enter Patient PIN // Generate Patient Symmetric Key

If Success (PIN)==True

Return Confirm PIN

Else

Return wrong PIN entered

Step 3: Reenter PIN + PU_P + PR_P

If Success (PIN + PU_P + PR_P) == True

Return Symmetric Key (SK_P) // (store patient symmetric key

(SK_P))to the Patient wallet

Else

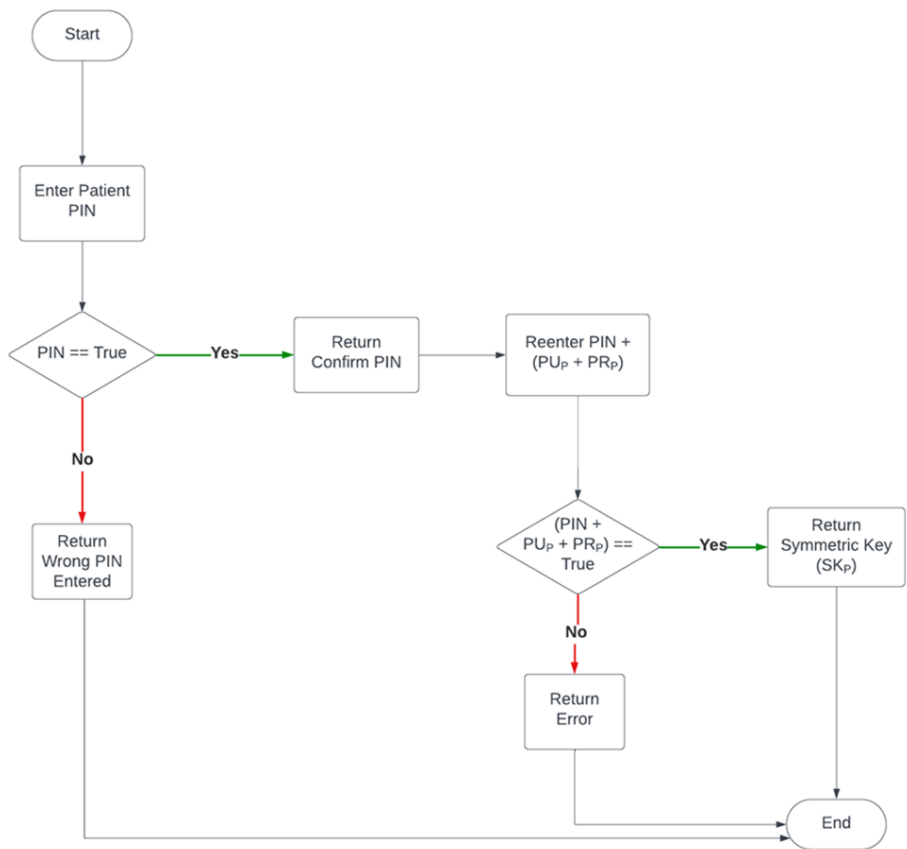
Return Error Message

Step 4: End

The Generate and Store Symmetric Key (SK) Algorithm is further represented in a flow-chart as shown in Figure 27.

Figure 27

Generate and Store Symmetric Key (SK) Algorithm Flowchart



4.3.13 Retrieve Symmetric Key (Sk) Algorithm

The retrieve symmetric key algorithm illustrates the process of retrieving the symmetric key when a patient forgets their symmetric key that was used to sign, hash and encrypt their electronic medical records in a different healthcare facility (hospital). The patient is required to enter their valid PIN to open their patient wallet and also their passphrase which is a security group of words known only to the patient, to authenticate that the patient is the legitimate owner of the patient wallet and that the historical electronic medical records (EMRs) belong to them. The patient is also required to enter their Public Key (Pu) and Private Key details as captured in their patient wallet.

Algorithm: RetrieveSymmetricKey

Input: PIN, PU_P, PR_P, Passphrase

Output: SK_P

Step 1: Start //Retrieve Symmetric Key (Sk)

Step 2: Enter PIN+ Passphrase

 If Success (Pin + Passphrase)==True

 Return Confirm PIN

 Else

 Return wrong PIN entered

Step 3: Reenter PIN + PU_P + PR_P

 If Success (PIN + PU_P + PR_P) == True

 Return Symmetric Key (SK_P)

 Else

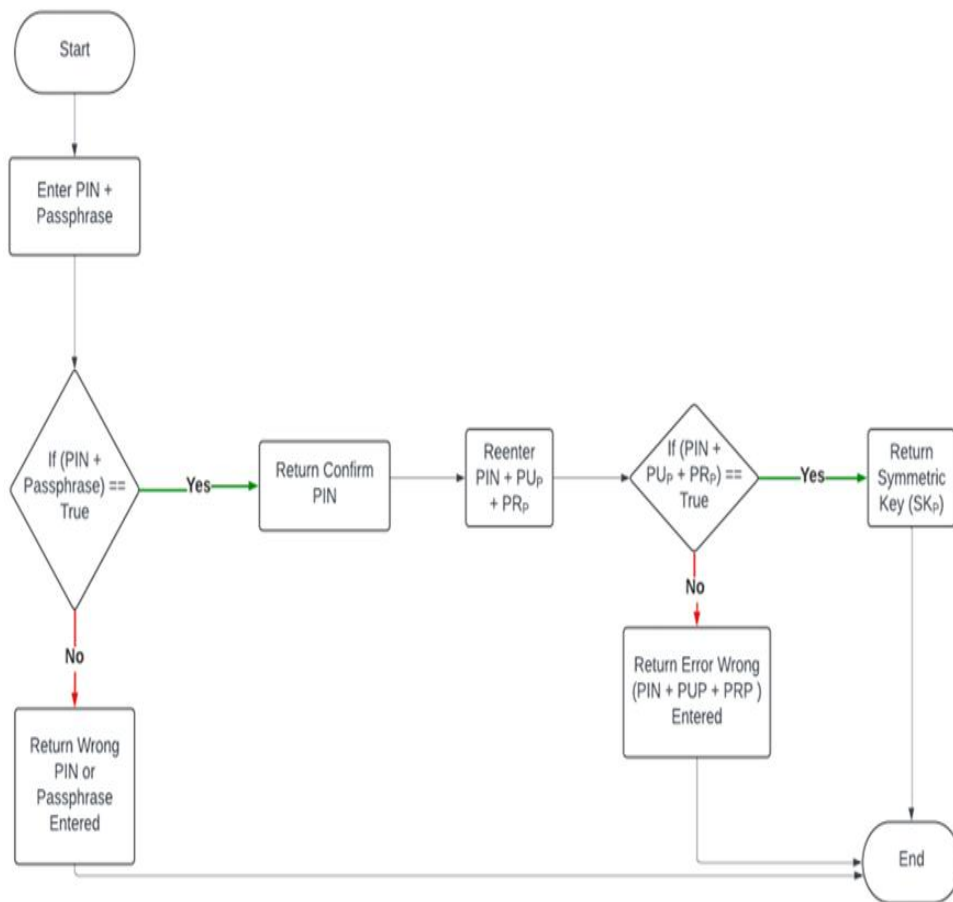
 Return Error Message

Step 4: End

The Retrieve Symmetric Key (Sk) Algorithm is further represented in a flowchart as shown in Figure 28.

Figure 28

Retrieve Symmetric Key (Sk) Algorithm Flowchart



4.3.14 Sign Patient EMR Plaintext Algorithm

The sign patient electronic medical records (EMRs) algorithm shows the process used by the patient to sign and authenticate that the new EMRs are correct and can be added to the Medical DLT system by the healthcare professional (Doctor). This is done once a patient visits any accredited health facility to seek treatment. Every new record needs to be signed before hashing using the patient symmetric key.

Algorithm: SignPatientEMR

Input: Pin,Sk

Output: B_S

Step 1: Start // Sign Patient EMR (Symmetric Key (SK_p))

Step 2: Enter PIN

If Success (PIN) == True

Return Enter Symmetric Key (SK_P)

Else

Return Wrong Pin Entered Message

Step 3 Enter Symmetric Key (SK_P)

If Success Symmetric Key (SK_P) == True

ReturnBS //Signed PatientEMR Plaintextusing Patient SK_P

Else

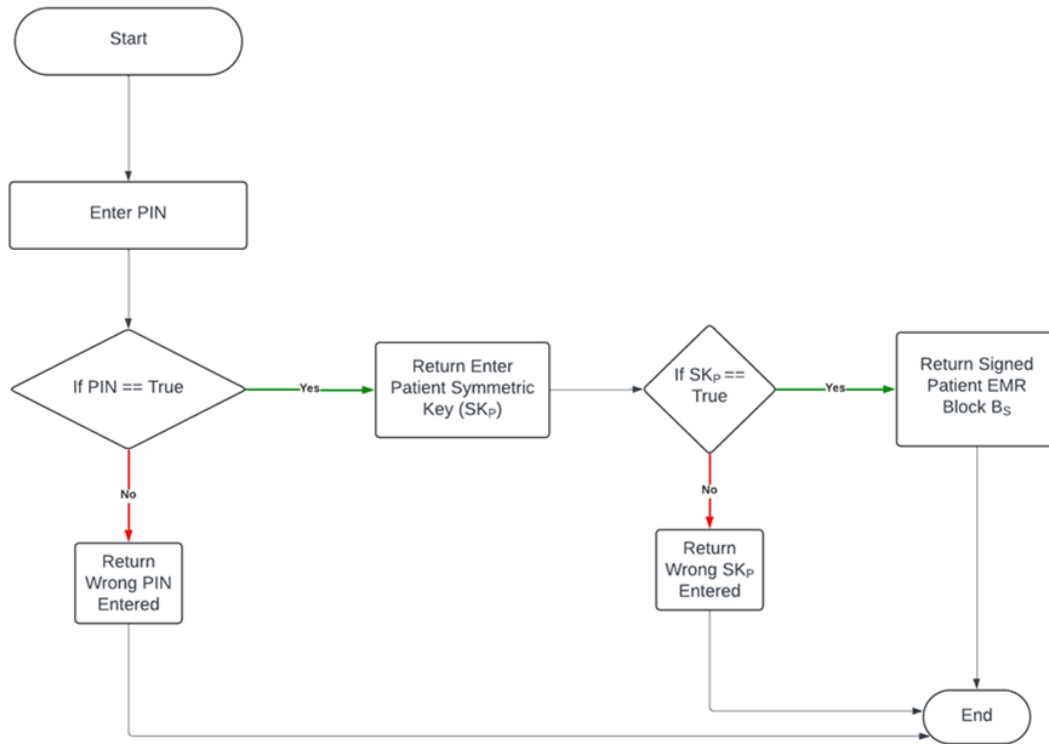
Return wrong Symmetric Key (SK) entered

Step 4: End

The Sign Patient EMR Plaintext Algorithm is further represented in a flowchart as shown in Figure 29.

Figure 29

Sign Patient EMR Plaintext Algorithm Flowchart



4.3.15 Hash Patient EMR Plaintext Algorithm

The Hash Patient EMR Plaintext Algorithm demonstrates the process of hashing the patient electronic medical records (EMRs). This is achieved by the patient entering their patient wallet PIN to authenticate ownership and the symmetric to allow signing of the records in order to give and bind the electronic medical records (EMRs) identity to the patient. Once the patient wallet PIN is correct and the symmetric key (Sk) provided is correct, then the patient electronic medical records (EMRs) are signed to wait for encryption process to take place.

Algorithm: HashPatientEMR

Input: PIN, SK_P

Output: B_H

Step 1: Start // Hash Patient EMR (Symmetric Key (SK_P))

Step 2: Enter PIN //Patient Pin

If Success (PIN) == True

Return Enter SK_P // Patient Symmetric Key (SK_P)

Else

Return Wrong Pin Entered Message

Step 3: Enter Symmetric Key (SK_P)

If Success Symmetric (SK_P) == True

Return B_H // HashedPatient EMR Plaintext via Symmetric Key (Sk))

Else

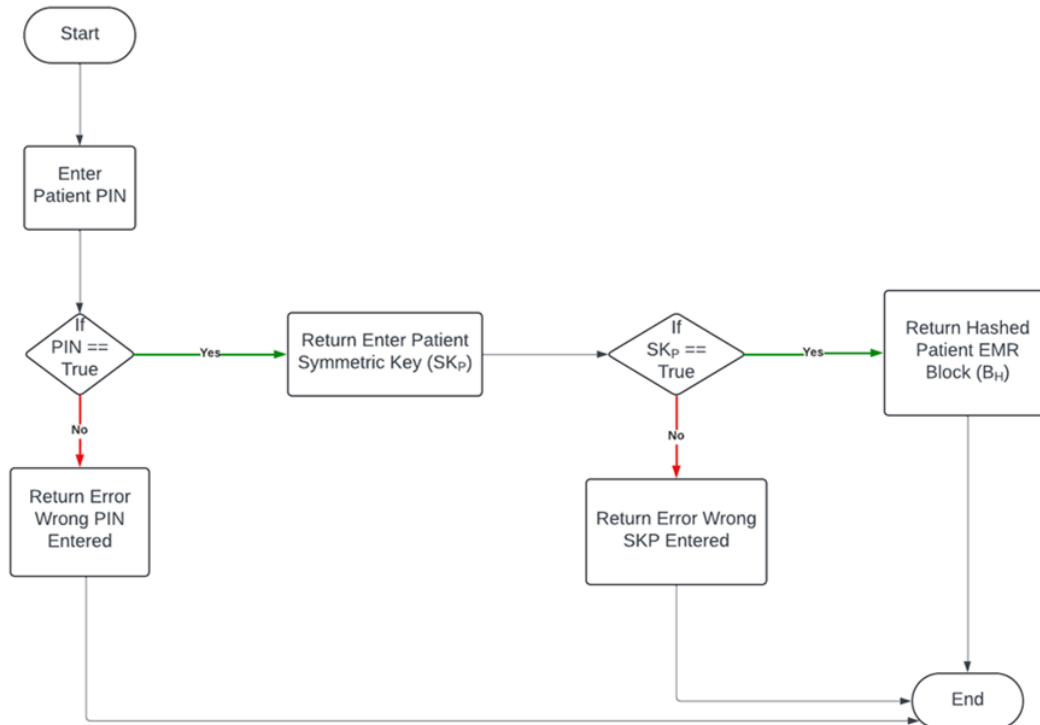
Return Error Message

Step 4: End

The Hash Patient EMR Plaintext Algorithm is further represented in a flowchart as shown in Figure 30.

Figure 30

Hash Patient EMR Plaintext Algorithm Flowchart



4.3.16 Encrypt Patient EMR Plaintext Algorithm

The Encrypt Patient EMR Plaintext Algorithm shows the process used by the healthcare professional (Doctor) to encrypt new patient electronic medical records (EMRs) before it is added or updated or uploaded to the Medical DLT system. The patient is required to authenticate a healthcare professional (Doctor) using their patient wallet details beginning from entering the correct PIN, Public Key (Pu), Private Key (Pr) and Symmetric Key (Sk). Once the patient's electronic medical records are signed, hashed and encrypted they are updated to the Medical DLT system for future reference either by the same healthcare facility or a different one, hence providing secure interoperability medical system.

Algorithm: EncryptPatientEMR

Input: Pin, PU_P , PR_P , SK_P

Output: B_E // Encrypted Patient EMR (Patient EMR Ciphertext)

Step 1: Start // Encrypt Patient EMR using patient Symmetric Key (SK_P)

Step 2: Enter Patient PIN

 If Success (PIN) == True

 Return Enter $PU_P + PR_P + SK_P$

 Else

 Return Wrong Pin Entered Message

Step 3: Enter Patient Public Key (PU_P) + Private Key (PR_P) + Symmetric Key (SK_P)

 If Success $PU_P + PR_P + SK_P ==$ True

 Return B_E // Encrypted Patient EMR Ciphertext

 Else

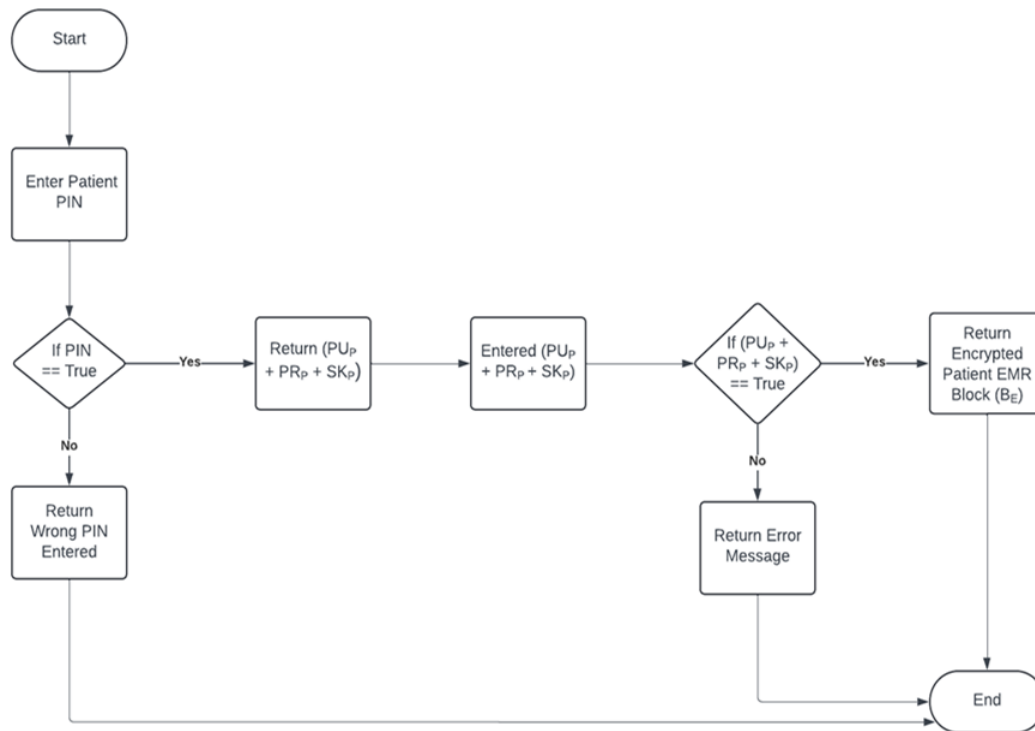
 Return Error Message (Patient Public Key (PU_P) or Private Key (PR_P) or Symmetric Key (SK_P) Don't Match)

Step 4: End

The Encrypt Patient EMR Plaintext Algorithm is further represented in a flowchart as shown in Figure 31.

Figure 31

Encrypt Patient EMR Plaintext Algorithm Flowchart



4.3.17 Decrypt Patient EMR Cipher Algorithm

The Decrypt Patient EMR Cipher Algorithm is used to show the process that is used by the doctor to decrypt the patient historical signed, hashed and encrypted electronic medical records (EMRs). This process requires the patient to enter their patient wallet valid PIN and then the Public Key (Pu), Private Key (Pr) and Symmetric Key (Sk) to be authenticated as the legitimate owner of the historical EMRs. This allows the doctor to decrypt the patient historical signed, hashed and encrypted electronic medical records (EMRs) even if they were uploaded to the Medical DLT from a different accredited healthcare facility.

Algorithm: DecryptPatientEMR

Input: PIN, PU_P, PR_P, SK_P

Output: B_D // Decrypted Patient EMR (Patient EMR Plaintext)

Step 1: Start // Decrypt Patient EMR using (Symmetric Key (SK_P))

Step 2: Enter Patient PIN

 If Success (PIN) == True

 Return Enter $PU_P + PR_P + SK_P$

 Else

 Return Wrong Pin Entered Message

Step 3: Enter $PU_P + PR_P + SK_P$

 If Success ($PU_P + PR_P + SK_P$) == True

 Return B_D // Decrypted Patient EMR Plaintext (Decrypted Patient EMR

 Ciphertext)

 Else

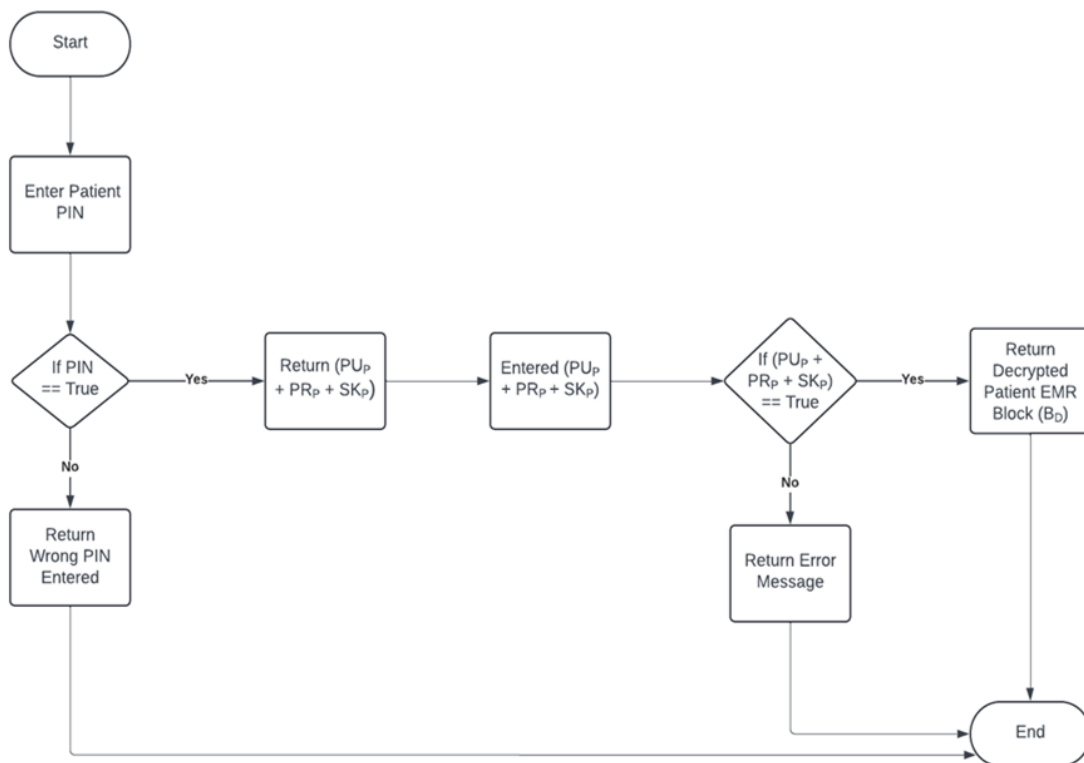
 Return Error Message (Patient Public Key (PU_P) or Private Key (PR_P) or Symmetric
Key (SK_P) Don't Match)

Step 4: End

The Decrypt Patient EMR Ciphertext Algorithm is further represented in a flowchart as shown in Figure 32.

Figure 32

Decrypt Patient EMR Plaintext Algorithm Flowchart



4.4 Validation of the Developed Enhanced Secure Distributed Ledger Interoperability Framework for Secure Medical Data Exchange

To validate the developed enhanced secure distributed ledger interoperability framework proof of concept method using a prototype of Medical DLT system was developed. The proof-of-concept prototype is used to demonstrate the functionality of interoperability of medical systems. The proof of concept method allows breaking of the prototype of medical systems into sub modules (Prasanna et al., 2021), that underpin the systems overall functionality, emphasizing on DLT based solutions to enhance security and promote seamless interoperability. Simulated data gathered from delphi method was used to test the functionality and interoperability of the Medical DLT System prototype. The prototype was also used to implement and evaluate the suitability of the designed algorithms that implement the enhanced secure distributed ledger interoperability

framework for medical systems. The prototype was sub divided into several sub modules, which are; Medical DLT (Web Interface), Medical DLT API (Backend), Medical DLT EMR (Backend), Medical DLT Portal, Medical DLT Smart Contract, Patient wallets interface, IPFS, WireGuard (Virtual Private Network (VPN)).

4.4.1 Medical DLT Virtual Private Network (VPN) Module

Medical DLT node networking is isolated from the public through a De-Militarized Zone (DMZ) approach such that only Health facility/Hospital/member Nodes with a public-private key networking information can participate and are authorized. This implementation is enhanced by WireGuard tool, a modern cryptographic Virtual Private Networking (VPN) approach, which allows for robust, fast, reliable and secure logical network or virtual LANs on top of a public network. Figure 20 is an example of a network definition for a Health facility or Hospital Node.

Figure 33

Medical DLT Virtual Private Network (VPN)

```
[Interface]
PrivateKey = 8LOu2ynWJLXtEPv9Ea0X3GRzHlqclPqWz3lfikhVtEM=
Address = 10.101.0.10/32, 4246:4206:9753:2021::a/128
DNS = 143.244.208.17y
MTU = 1280

[Peer]
PublicKey = LCnKM4eZrJZ9B4NzPFInu4TQEJSAmIRIhe/QnMfjbzc=
AllowedIPs = 10.101.0.0/24, 4246:4206:9753:2021::/64, 0.0.0.0/0
Endpoint = 159.223.200.xx:51822
PersistentKeepalive = 20
```

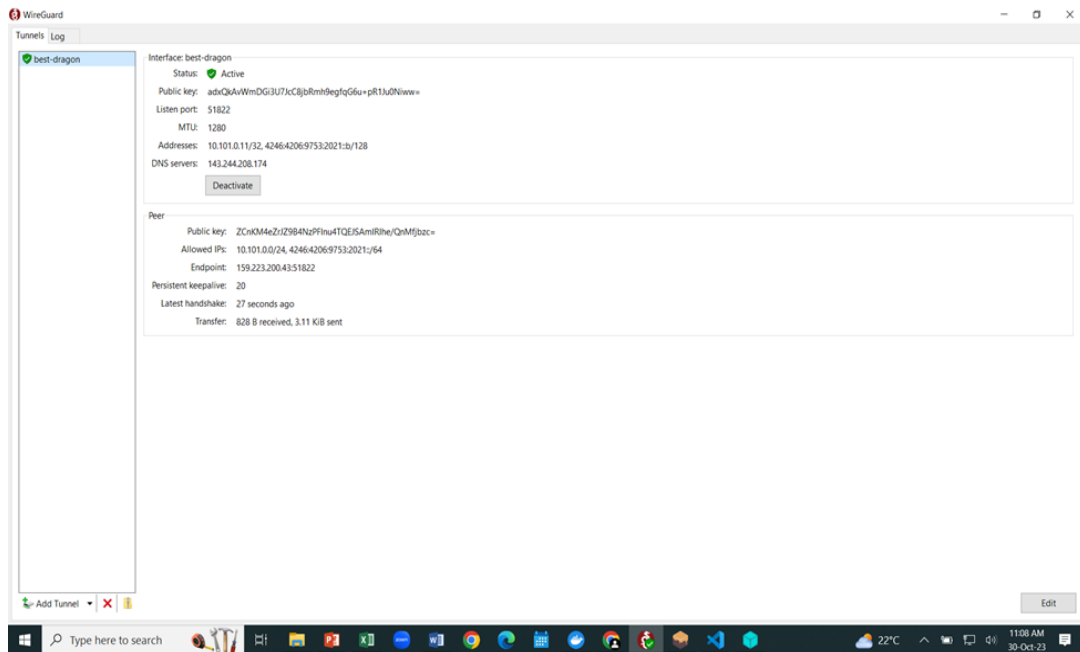
This configuration sets up the server it runs on, a network interface identified by Node IP *10.101.0.10* which it uses to securely communicate with other Health facilities or

Hospital Nodes, even on a public network. This is achieved through securely encrypting traffic between nodes with their public-private keys.

In DLT implementation, the Network latency, robustness, security and stability are emphasized as the immutability aspect, and distribution of Nodes relies on that private network to internetwork. Electronic Medical Records (EMRs) which are written to comply with HL7 FHIR standards can securely relay events to the Medical DLT Smart Contract. The Medical DLT VPN using WireGuard is as shown in Figure 34.

Figure 34

The Medical DLT VPN using WireGuard



To an average user, the experience feels the same as a traditional healthcare system; however, the underlying implementation handles technicalities such as permissioning, data storage, event communication, and encryption.

Patient EMRs are standard HL7 FHIR resources that are interoperable across health facilities or hospitals in the network. This study outlines how patient EMR record is processed and stored on InterPlanetary File System (IPFS), and then to the Medical DLT.

The Medical DLT EMR source code was written using Solidity, tested using Ganache during development and production setup or chestration using Ethereum based technology, and HyperledgerBesu for live network of Nodes. The choice of the base platform for the Medical DLT was based on the following reasons:

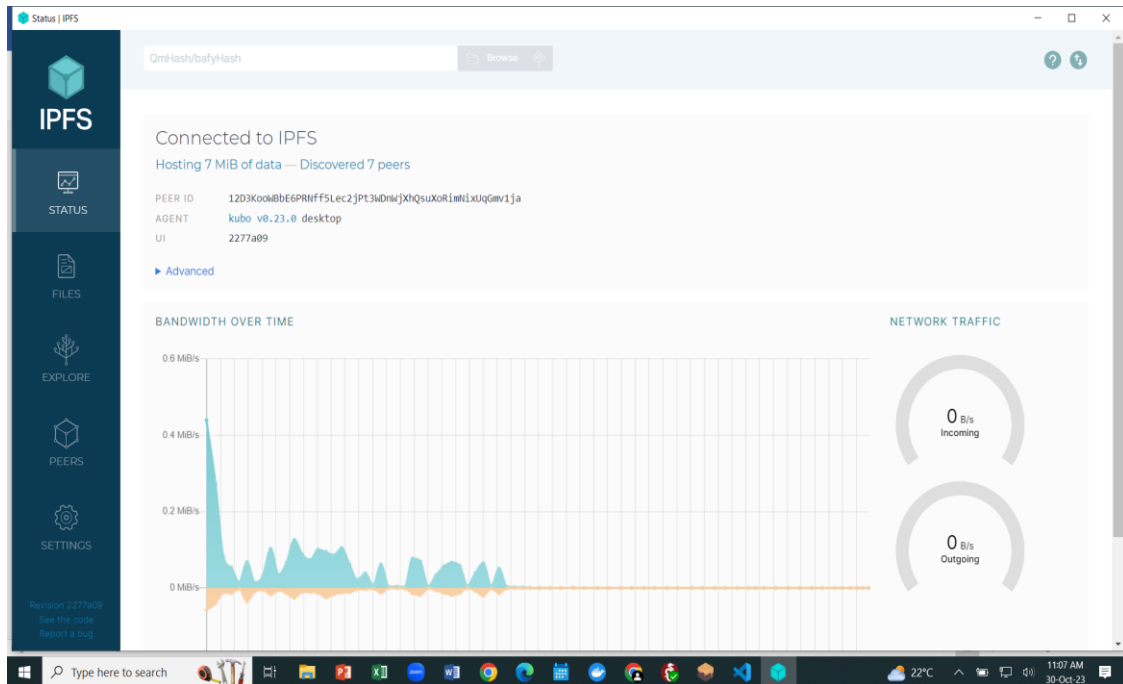
- Unlike main Ethereum, the study tried to avoid limitations and concerns of the Crypto Currency issues, as the study sort to develop a medical ledger system that does not concern such particulars.
- The HyperledgerBesu allows choice and fine-grained control of the private Ethereum network setup that has different configuration that allows advanced modelling of Smart Contracts based on Ethereum Virtual Machine (EVM), and without consensus algorithms constraints, but having access to all Ethereum technology benefits for a non-finance industry.

4.4.2 Medical DLT Interplanetary File System (IPFS) Module

To cater for storage concerns, the Medical DLT system uses Interplanetary File System (IPFS), a peer-to-peer distribute hypermedia protocol for data storage layer and distribution across Nodes. A record in IPFS is identified by a hash of the data known as Content-Identifier (CID). This helps the Medical DLT system to isolate data storage to a more robust and secure approach and implementation. All data in IPFS is immutable, encrypted and redundant across all health facilities nodes, or participating nodes in the Medical DLT Network. Figure 35 shows the Medical DLT InterPlanetary File System (IPFS) Module running.

Figure 35

Medical DLT InterPlanetary File System (IPFS) Module

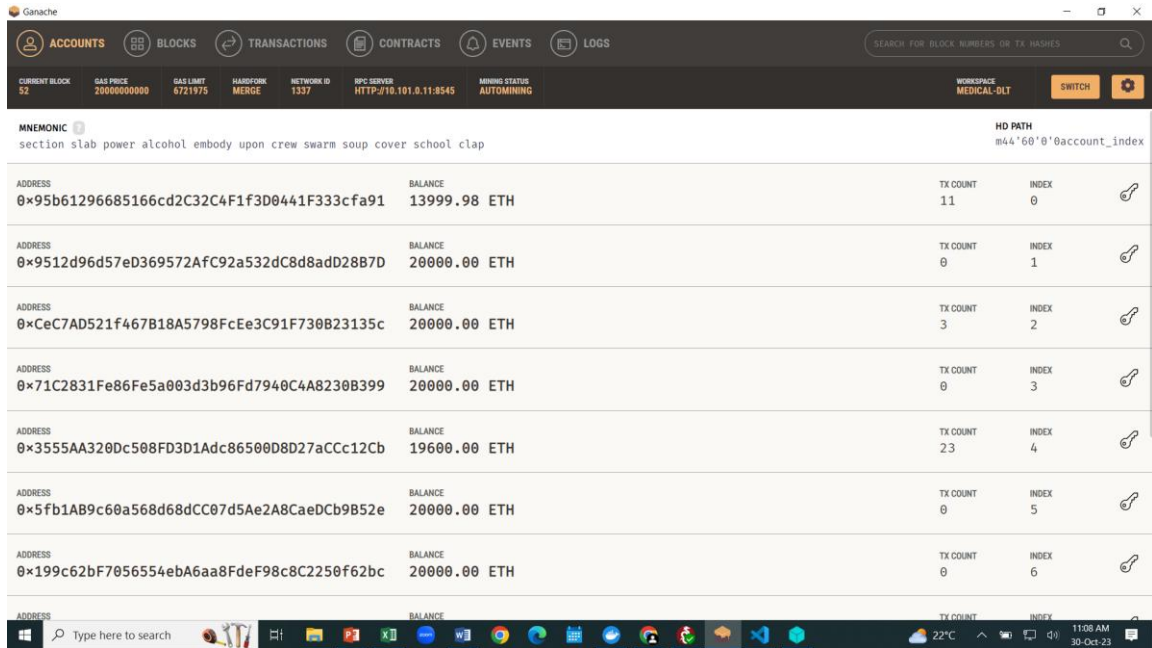


4.4.3 Medical DLT Smart Contract Module

This Smart Contract defines how the Medical DLT system organizes its data across Nodes (health facilities). It lives within Ethereum Virtual Machine(EVM) environment based on Ethereum platform to control immutability, additional security, audit traceability and verification management for advanced privacy that healthcare ecosystem deserves. Figure 36 shows the Ganache Ethereum that is supporting the Master DLT System.

Figure 36

Medical DLT Smart Contract Module



The Medical DLT smart contract acts as a decentralized electronic medical record system on the network of health facility or hospital nodes. It creates an accessible, secure, and immutable ledger of medical records, user accounts, and access requests. It is created using the Solidity programming language and built upon Open Zeppelin's Access Control contract to manage user roles and access permissions.

Steps followed when setting up the Smart Contracts

The steps followed when setting up the Medical DLT System Smart Contract are discussed in the subsequent sections.

a. Conditions and Contract Formation

This contract requires Solidity 0.8.0 or later to utilize. Import the contract from the OpenZeppelin library at first. A basic level of access control capability is provided by this contract, which manages several roles (such as administrator, patient, hospital, practitioner, and insurance provider) and their corresponding rights inside the system.

b. Setting up the Roles

Determining the different roles within the system comes next after putting up the smart contract. Roles are established by using the keccak256 hashing technique and consistent hash values. These jobs include administrative, patient, hospital, practitioner, and insurance provider functions. An essential component of any safe, decentralized application is the way this configuration guarantees that various users within the medical DLT system have varying degrees of access and capabilities.

c. Awareness of the Data Structures

Numerous intricate data structures, like as arrays, structs, mappings, and enumerations, are included in this smart contract. The Request Status enumeration is a crucial component that monitors the progress of access requests to a patient's data.

Within the system, many entities and actions are represented by structures. The User, Hospital, Record, Access Request, and Event structs are among these. The corresponding data for every person and hospital is stored in user and hospital structs. Patient record data is stored in the Record struct, and requests to see a patient's information are tracked by the AccessRequeststruct. The system records various occurrences into the Event struct. Mappings and arrays serve as the primary data storage in the contract, tracking users, hospitals, patient records, access requests, events, etc. These state variables are private to maintain data privacy and can be accessed through various getter functions.

d. Event Logging

Events are crucial in any distributed smart contract as they provide a way of triggering actions and recording activities on the ledger. In this smart contract, there are several events to track activities, like when a new patient record is added, a new access request is

created or updated, a new hospital is added, a new user is added, and a new event is logged.

e. Initialization and Role Assignment

In the contract initialization function, the deployer of the contract is assigned the ADMIN_ROLE. This function is typically only called once, right after the contract has been deployed to the network. This ensures that the initial setup is in the hands of a trusted entity, which is critical in a sensitive system such as a medical records platform.

f. Manipulating and Accessing the Data

The contract includes numerous functions to interact with and manipulate data. They include getter functions to retrieve details about users, hospitals, records, requests, and events. The medical DLT system also has functions to add new entities to the system. These functions ensure that only users with the appropriate roles can perform certain actions, maintaining the system's integrity and security. When a new health facility (hospital), user, or patient record is added, the relevant event is emitted, marking the action on the distributed ledger.

Access requests to patient records are handled through three functions; namely, request Access, approve Request, and deny Request. These functions allow practitioners or insurance providers to request access to a patient's records, and the patients to approve or deny such requests using their symmetric Key.

The logEvent function enables the system to log various significant events, providing a useful trail of actions taken in the medical DLT system.

The Medical DLT smart contract demonstrates a strong foundation for a secure, decentralized medical records ledger. It emphasizes data privacy and integrity through

robust access control measures, using the immutability and transparency of the distributed ledger technology to ensure that all activities are recorded and verifiable.

4.4.4 The Master Medical DLT Module

This section presents a detailed guide to understanding the implementation of a decentralized and secure electronic medical record (EMR) system. This system leverages various technologies including distributed ledger technologies like Ethereum, InterPlanetary File System (IPFS), Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR), and cryptographic encryption techniques such as Diffie-Hellman Key Exchange (DHKE) and Elliptic Curve Cryptography (ECC). A distributed ledger technology (DLT) is employed to create an immutable record of EMRs, maintaining the integrity and security of patients' medical information. The master Medical DLT implements several security elements which includes interoperability and standardization, distributed ledger technology, medical record generation and management, permissioning and access control, and the data security component that deals with encryption, decryption and key management as discussed in the subsequent sections.

a. Interoperability and Standardization Element

To ensure interoperability, standardization and data consistency in the way Electronic Medical Records (EMRs) are handled across different medical systems, the enhanced secure distributed ledger interoperability framework for medical system design follows the HL7 FHIR standard and other healthcare regulations like Health Insurance Portability and Accountability Act (HIPAA). This framework offers a set of standards for exchanging healthcare information electronically, including guidelines for representing, storing, and transmitting medical data.

b. Distributed Ledger Technology Element

The Medical DLT system uses a custom DLT, often referred to as blockchain, to create a decentralized and secure platform for handling Electronic Medical Records (EMRs). The Medical DLT comprises of nodes represented by participating healthcare facilities (hospitals), with each node having a copy of the complete ledger.

c. Medical Record Generation and Management Element

The medical records are generated by a regular EMR system, and standardized using HL7 FHIR. The EMRs are stored on the IPFS - a distributed system for storing and accessing files, websites, applications, and data. Instead of using traditional location-based addressing as used in HTTP, IPFS employs content-based addressing. This means that each file and all of the blocks within it are given a unique finger print called a cryptographic hash.

d. Permissioning and Access Control Element

The enhanced secure distributed ledger interoperability framework design ensures that only authorized parties can access a patient's EMRs. The medical DLT system uses Diffie-Hellman Key Exchange (DHKE) for permissioning access to the records. Each user, represented by a patient or a health facility (hospital), has a unique pair of private and public keys. When a patient visits a hospital, a shared secret key is established using DHKE. The patient then uses this key to allow the hospital access their records or to revoke access to their medical records.

e. Data Security Component that deals with Encryption, Decryption and Key Management Element

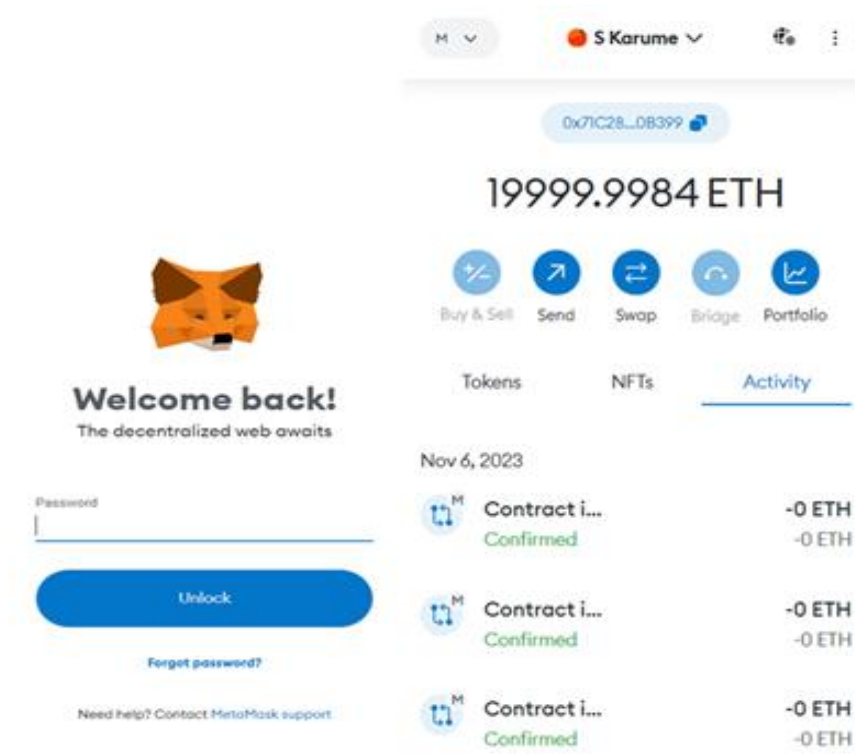
To maintain confidentiality and ensure data privacy, the medical DLT system utilizes Elliptic Curve Cryptography (ECC) to encrypt the EMRs. ECC is a public key encryption technique based on the algebraic structure of elliptic curves over finite fields.

4.4.5 The Patient Wallet Module

Medical DLT system envisages that patient create their own patient wallet using MetaMask. MetaMask is a popular browser extension that allows users to manage their Ethereum-based assets and interact with decentralized applications (DApps). Patient wallet requires the patient to keep their wallet secure using a PIN, password and seed phrase which should never be shared with anybody. If the Patient loses their patient wallet, then they need to use the seed phrase to recover and gain access to their wallet. Figure 37 shows the patient wallet of a patient by name S. Karume, who is registered into the Medical DLT System Network.

Figure 37

The Patient Wallet Module

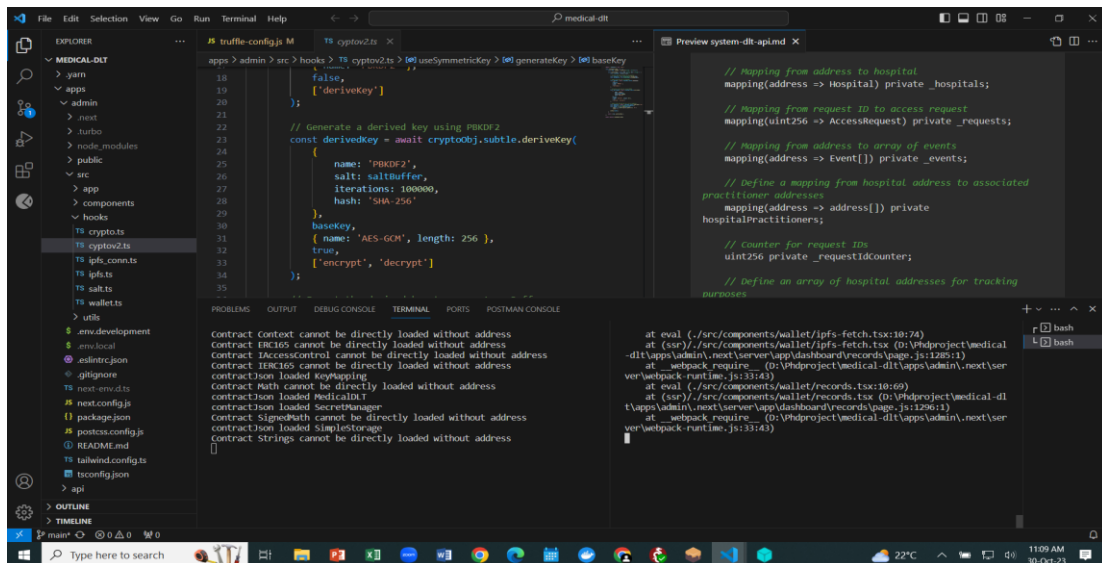


4.4.6 Medical DLT API Modules

The medical DLT System Application Programming Interface (API) is an abstract layer that has no Graphical User Interface (GUI), but links and enables seamless communication and data exchange between medical DLT and the Medical DLT EMR within the healthcare ecosystem. It also facilitates interoperability by allowing different medical systems from different nodes (health facilities) to exchange data and functionality cohesively. Patient medical data exchange via APIs contributes to a more comprehensive and accurate patient overview. Figure 38 shows the two APIs terminals that run to support medical DLT system interoperability, these two terminal interfaces of the Medical DLT API are the medical DLT System API and the Medical DLT Admin.

Figure 38

Medical Distributed Ledger Technology (DLT) Application Programming Interface (API) Modules

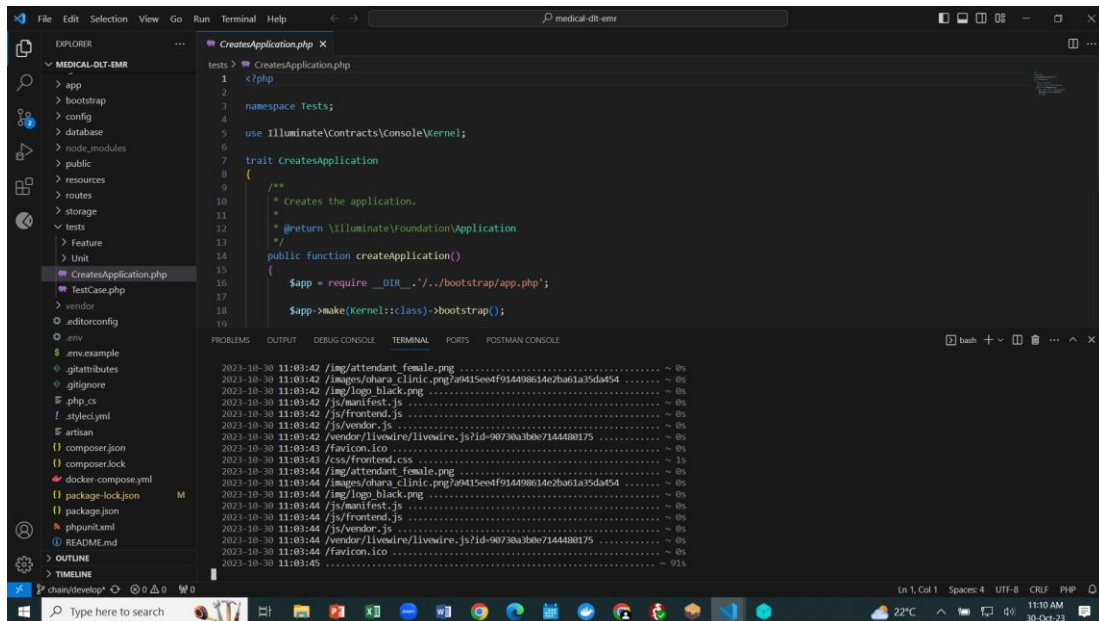


4.4.8 Medical DLT EMR (Backend) Module

The medical DLT EMR (backend) has no graphical user interface. It has been programmed using PHP and follows the healthcare sector standards and regulations which enhance good security practices among the developed medical systems. Figure 39 shows the Medical DLT EMR Backend Module.

Figure 39

Medical DLT Electronic Medical Records (EMR) Backend Module



4.4.8 Medical DLT System (Web Interface) Module

The medical DLT system web interface serves as a frontend interface that allows healthcare facility staff like hospital medical system administrator, Cashiers and other healthcare professionals like Doctors, Nurses, Lab technologists and Pharmacists to interact with the digital component of the medical system. The Medical DLT system web interface supports various aspects of healthcare service delivery, administration, and communication between the healthcare practitioners. It enhances security, efficiency, access controls, accuracy, authentication and collaboration within the medical system, while prioritizing patient-centered care. The medical systems administrators of the approved and licensed medical facilities in the healthcare sector is required to install the Medical DLT web interface in order to link to the secure master Medical DLT network. Figure 40 shows the Medical DLT System web interface for Hospital 1 and Hospital 2.

Figure 40

Medical DLT System web interface for Hospital 1 and Hospital 2

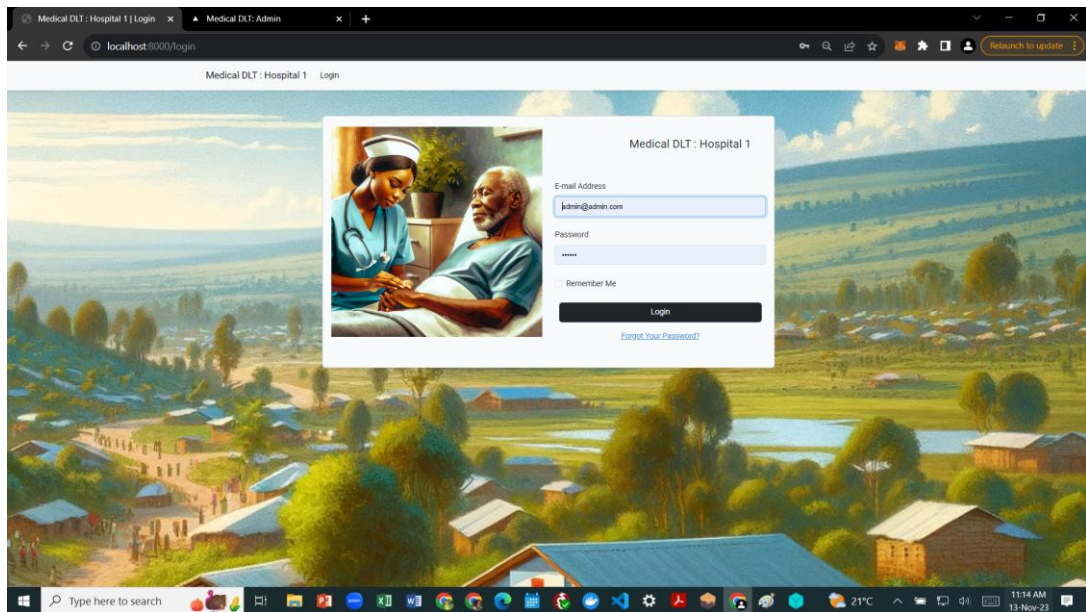


4.4.8.1 Medical DLT System Login Interface

The login interface for the medical DLT system is the initial point of access for authorized users. It provides the first level of authentication of user to protect sensitive patient's medical information. This interface ensures that only authorized and authenticated administrators, healthcare professionals, and healthcare staff have access to the Medical DLT system dashboard and other system functionalities. Medical DLT system user authentication involves a secure user name which is the users email address and a password that follows all the rules of a strong and secure password, ensuring compliance with the data protection healthcare standards and regulations; hence, contributing to the overall security and trustworthiness of the medical system. The login interface fosters a user-friendly interface that links users to the Medical DLT system dashboard. The Figure 41 shows the Medical DLT system Login interface.

Figure 41

Medical DLT System Login Interface

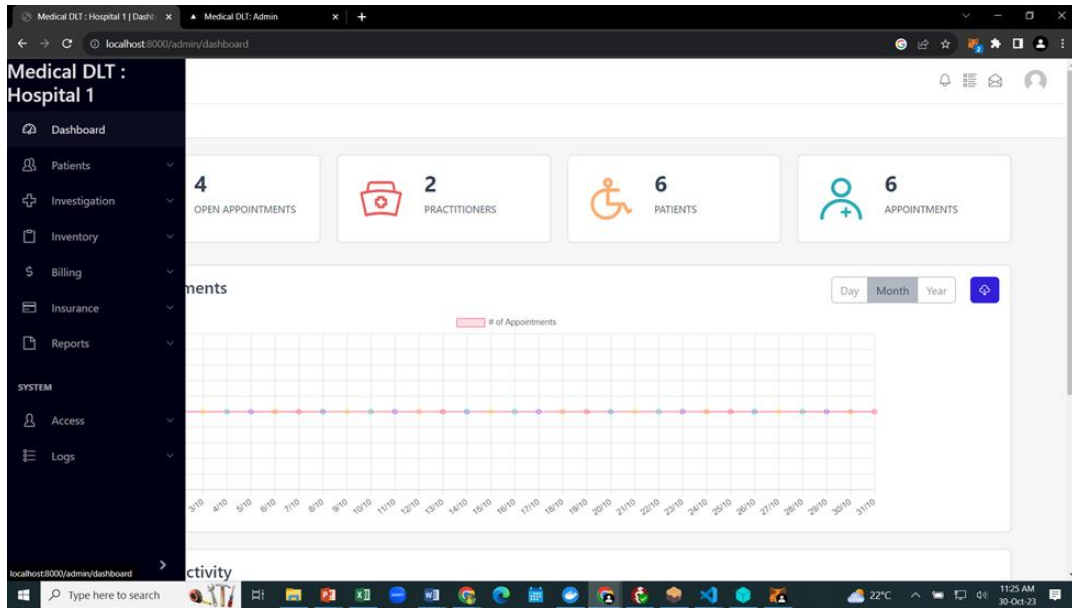


4.4.8.2 Medical DLT System Dashboard

The Medical DLT system dashboard serves as a visual representation of critical medical services, information and key performance indicators within the healthcare organizations. It provides the administrator and healthcare practitioners with various aspects of the Medical DLT system based on their user access privilege levels. This implies that different users have different dashboard items. The aspects captured in the Medical DLT system dashboard includes: patient's appointments, stock inventory, billing, insurance details data, reports, logs and access, which entails user and role management. The Medical DLT system dashboard enhances decision making process by offering an overview of the entire medical system and promoting data-driven actions hence improving efficiency and effectiveness of the healthcare operations. Figure 42 shows Medical DLT system Dashboard

Figure 42

Medical DLT system Dashboard

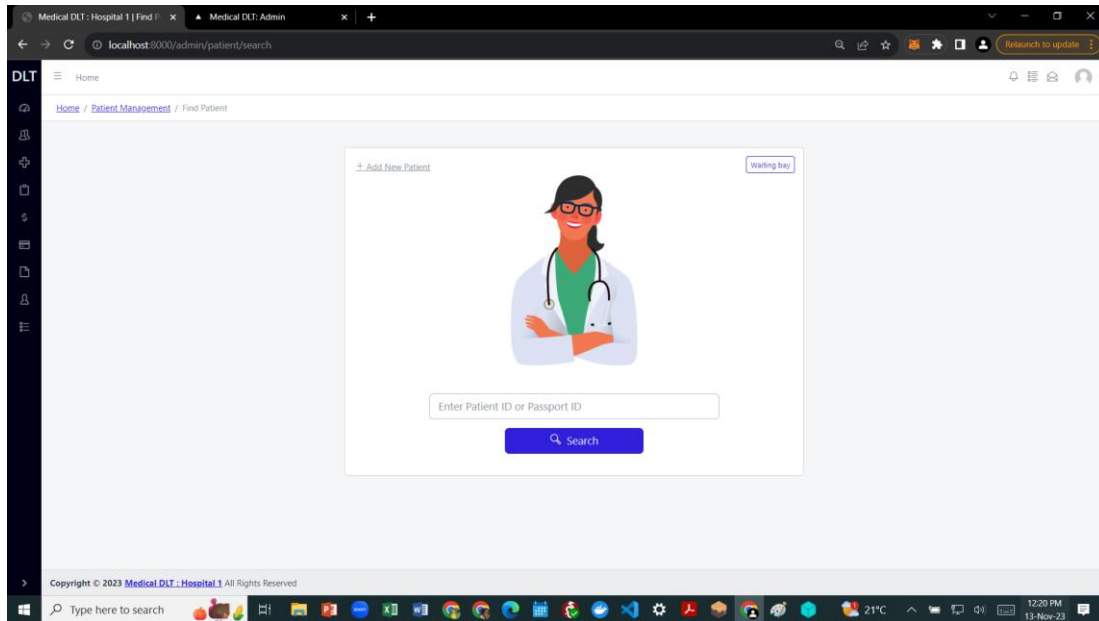


4.4.8.3 Medical DLT System Add Patient or Search Patient Interface

The Medical DLT System Add Patient or Search Patient Interface allows the receptionist to add a new patient into the medical DLT System. The role of adding new patients to the medical DLT system is assigned to the receptionist. This interface is also used by other healthcare professionals to search for a patient from the Medical DLT system. To search a patient from the Medical DLT system, the healthcare practitioner is required to enter the patients' ID for identification. Once the patient ID matches the one that is already in the Medical DLT, then the patient records are retrieved, but the data is encrypted, which implies that the patient is required to authorize access to their patient's medical historical personal health information (PHI). Figure 43 shows the Medical DLT System Add Patient or Search Patient Interface.

Figure 43

Medical DLT System Add Patient Interface

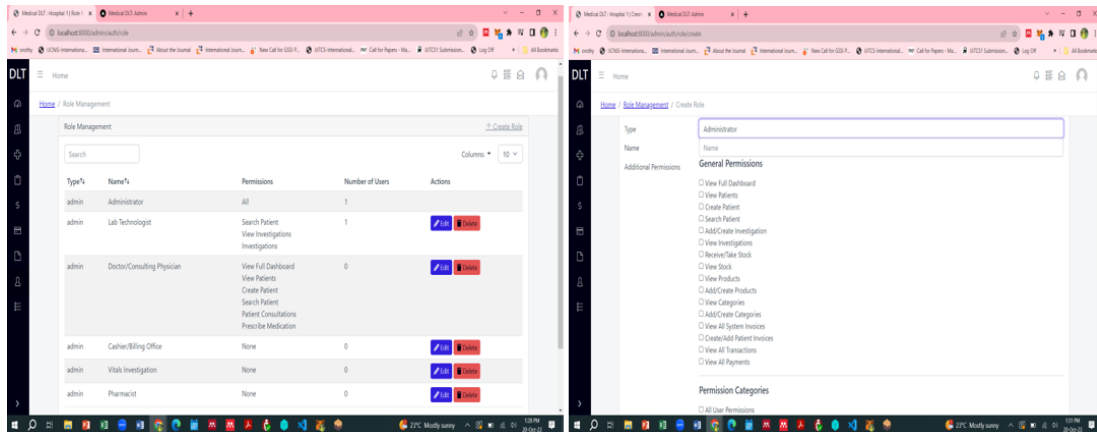


4.4.8.4 Medical DLT System Administrator Interface

The Medical DLT system administrator interface allows the administrator to oversee and manage various aspects of the medical system efficiently and effectively. It provides access privileges such as viewing and searching patients, viewing all investigations, viewing all inventory, viewing all invoices, payments and transactions, viewing all insurance claims and reports, access to user and role management and logs to the Medical DLT system administrator. It plays a central role in the effective management, configuration, and optimization of the Medical DLT system. It empowers the medical system administrators to maintain system integrity, ensure compliance, and enhance the overall efficiency of healthcare services and operations. Figure 44 shows the Medical DLT System Administrator Interface used for creating role and role management.

Figure 44

Medical DLT System Administrator Interface used for Creating Role and Role Management

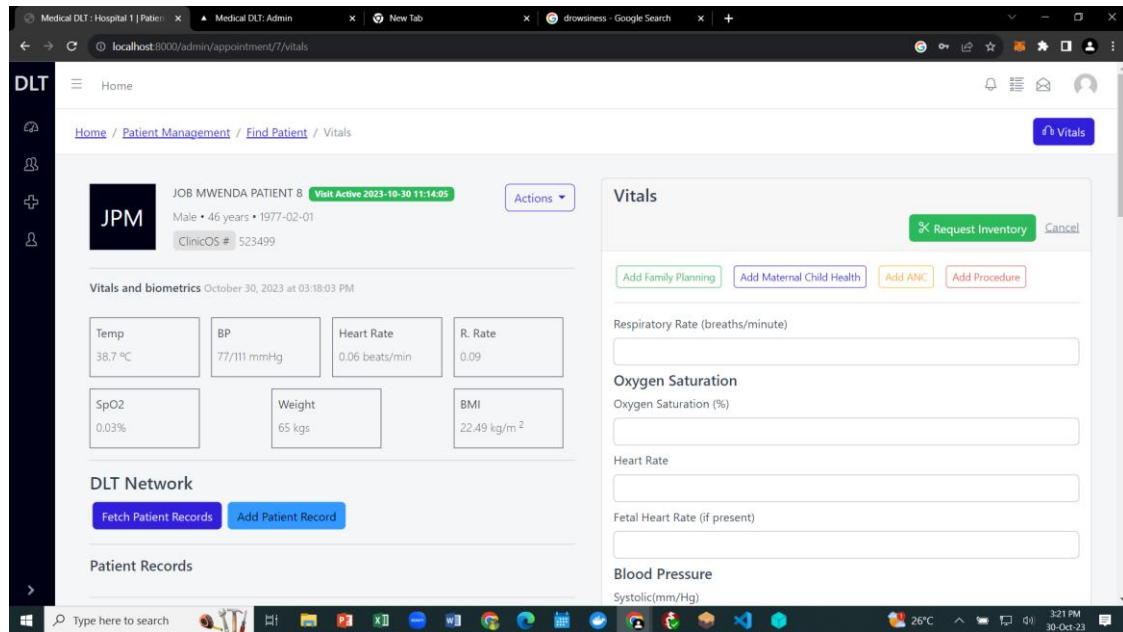


4.4.8.5 Medical DLT System Nurse Interface

The medical DLT System Nurse interface is used by the nurse serving patients at the Triage to add and capture patients' vitals. The patient's vital information captured by the medical DLT system includes the oxygen saturation levels, heart rate, fetal heart rate in cases of expectant mothers, blood pressure (Systolic and Diastolic), temperatures, height, weight, BMI, and nurse's notes. Figure 45 shows the Medical DLT System Nurse interface.

Figure 45

Medical DLT System Nurse Interface

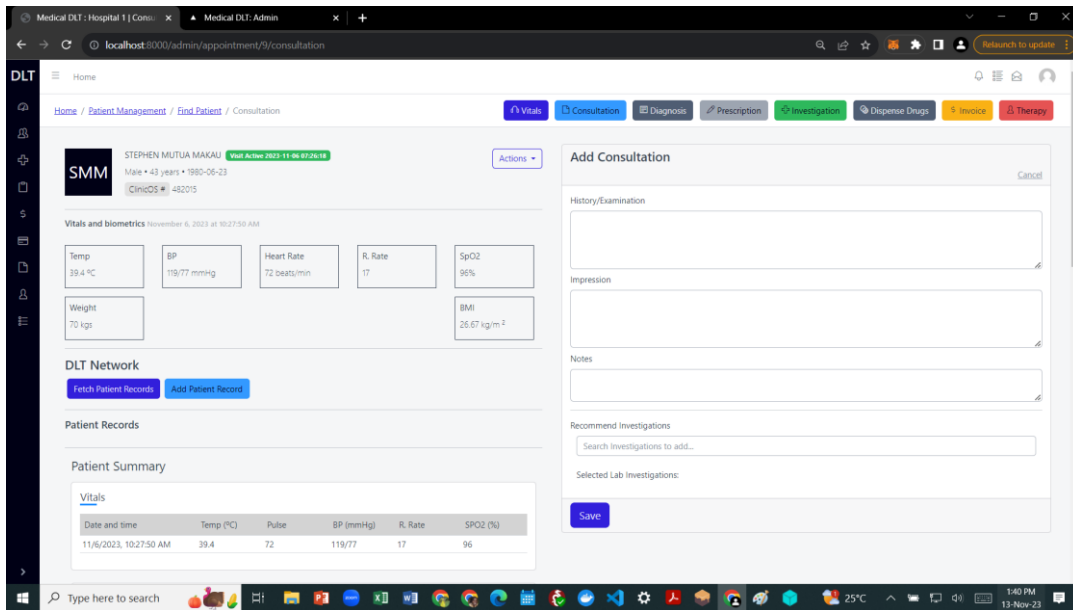


4.4.8.6 Medical DLT System Doctors Interface

The Medical DLT system doctors interface is designed to provide an interface that allows doctors to carry out various clinical and administrative tasks aiming at enhancing efficiency and quality of patient care. These services include consultation, diagnosis and drug prescription. Figure 46 shows the Medical DLT system doctors interface.

Figure 46

Medical DLT System Doctors Interface



4.4.8.7 Add Patient Record / Fetch Patient Records

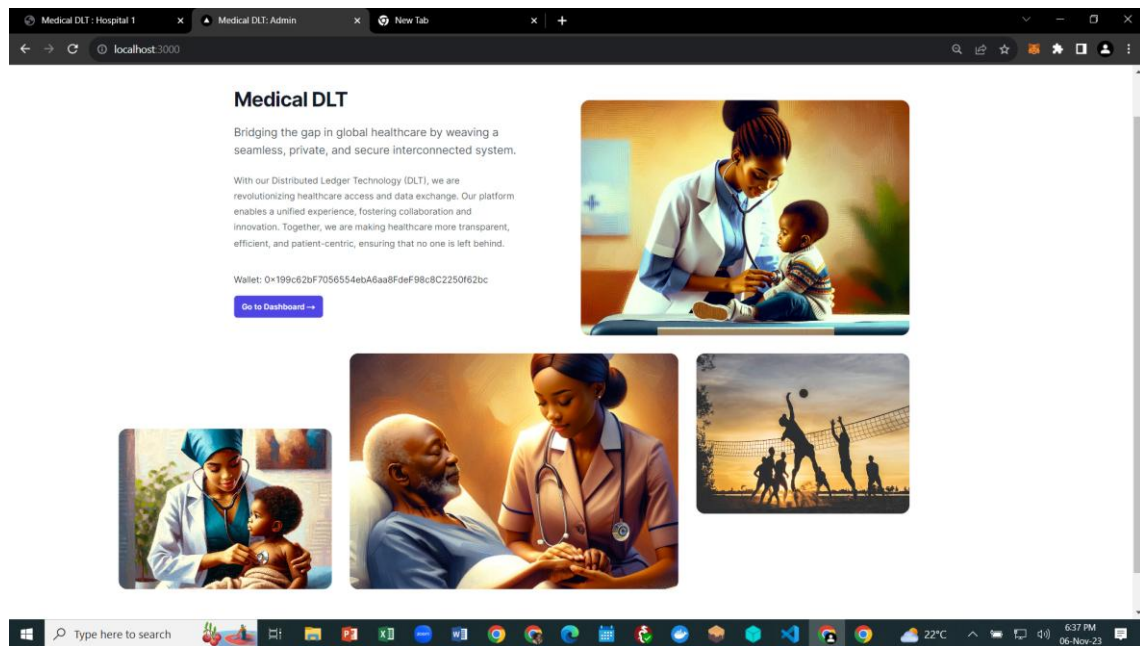
For the doctor to be able to add patient records to the Medical DLT system or fetch patient historical record from the Medical DLT system, the patient needs to authenticate and authorize the event using their symmetric Key. This event necessitates the healthcare practitioner to launch and use the medical DLT portal interface to seek authentication and approval by the patient using their patient wallet and their symmetric key.

4.4.9 Medical DLT Portal Module

This web interface acts as the Medical DLT Portal Front End web interface. The authenticated and authorized healthcare worker like Doctor is required to click on “Go to Dashboard” tab to open the medical DLT portal web interface. Figure 47 shows the medical DLT portal.

Figure 47

Medical DLT Portal



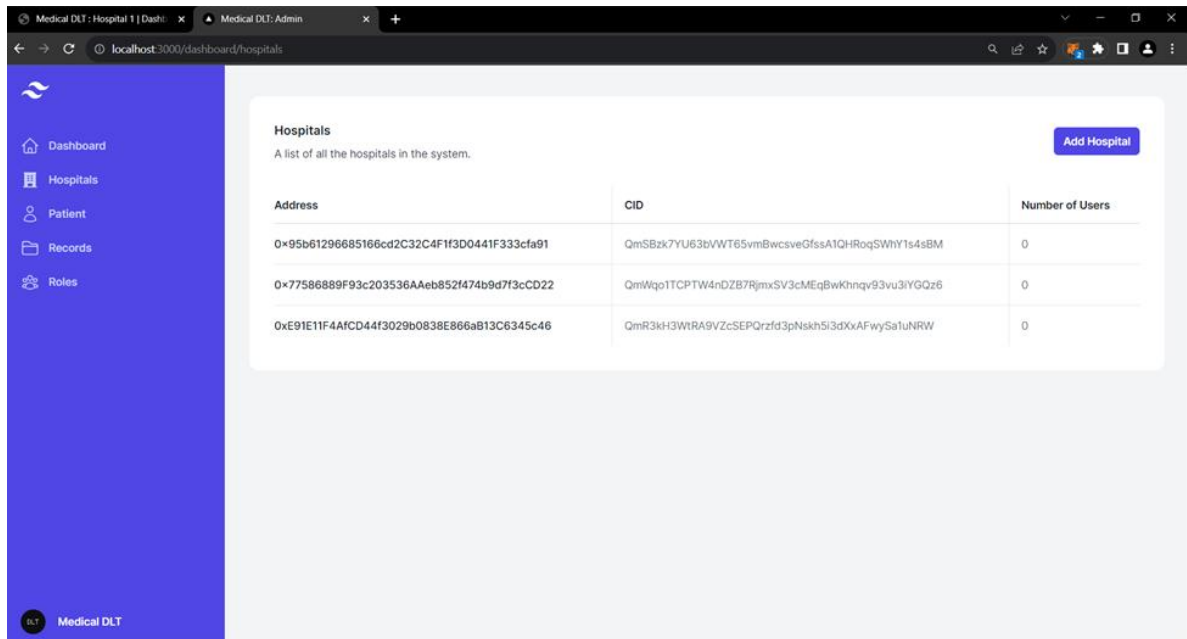
This is the first page of the medical DLT Portal which is the front end, and has a Graphical User Interface (GUI). This is the page that links the Medical DLT to the Medical DLT EMR to aid secure exchange of patients' medical data. This Medical DLT Portal interfaces with the Patient's Wallet to allow the patient authenticate the medical practitioners who should access their historical electronic medical records. Upon clicking the Connect to Wallet tab, the portal links to a page that lists and provides options to access the Dashboard, Hospitals, Patient Records and Roles. The Hospital dashboard lists the addresses and the Content Identifiers (CIDs)of the approved health facilities (hospitals). Each of the options under the doctor's medical DLT portal are as shown in Figure 48.

4.4.9.1 Dashboard/ Hospital

The Medical DLT Portal Dashboard hospital page allows users to view the accredited healthcare facilities (hospitals) by list their addresses and their content identifier (CID) that is used to uniquely identify the accredited healthcare facilities.

Figure 48

The Medical DLT Portal Dashboard



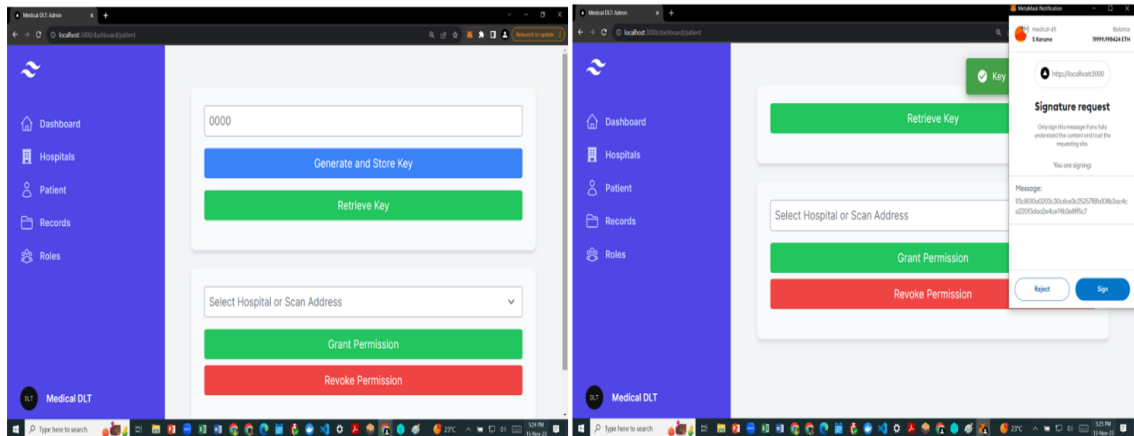
4.4.9.2 Dashboard /Patient (Generate and Store Key/ Retrieve Key/ Grant and Revoke)

Upon the doctor clicking on the patient tab on the Medical DLT Portal, a patient's authentication and authorization interface is launched. This interface allows the Patient to enter their Patient wallet PIN, which is a four digit characters. The patient clicks on generate and Store Key option the medical DLT portal which links to the Patient wallet and references their Public Key and Private Key in order to generate the symmetric Key by launching MetaMask interface. This gives the patient a chance to generate a unique symmetric Key that allows the patient to sign, encrypt, hash and grant or revoke a healthcare facility access to their electronic medical records stored in the medical DLT.

The patient in turn authorizes and authenticates the medical practitioners (Doctor) who needs to access their historical medical records using their symmetric key which is unique. In cases where the patients are not comfortable with the medical services provided at the healthcare facility visited, they still have the power to revoke permission of the healthcare facility, hence making all the healthcare services to be patient-centric. Figure 49 shows the Medical DLT portal displaying all the operations that are available to the patient to authenticate access to their personal electronic medical records.

Figure 49

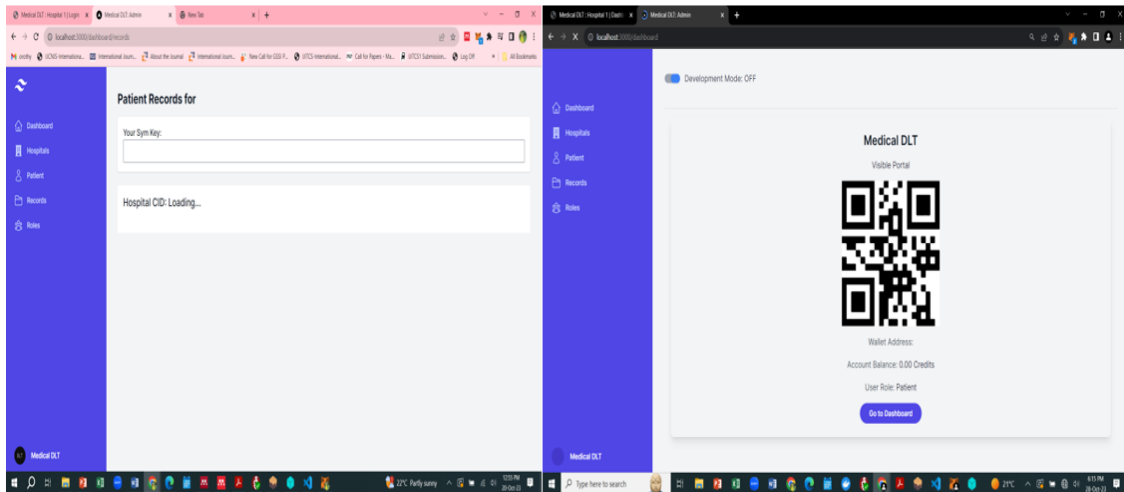
Dashboard /Patient (Generate and Store Key/ Retrieve Key/ Grant and Revoke)



After the patient has signed and confirmed that they are authorizing and authenticating the doctor to add, update or fetch their t electronic medical records, the patient then scans or enters their symmetric key to complete the event as shown in Figure 50.

Figure 50

Medical DLT Portal Patients Record Page



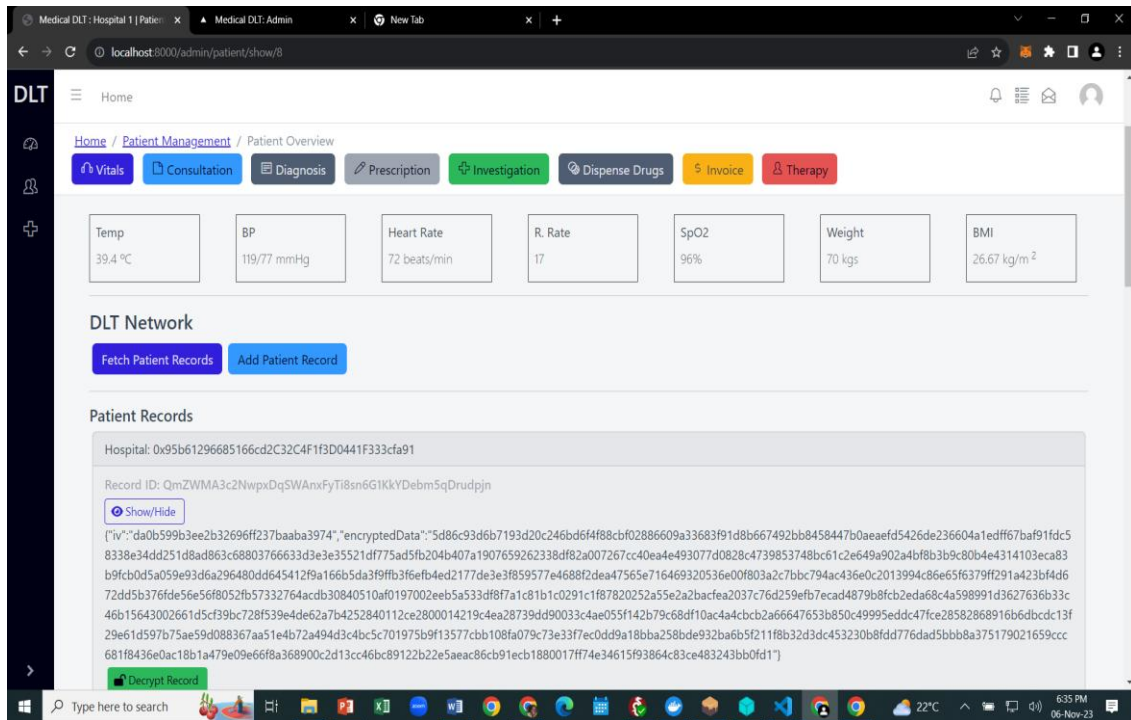
The medical DLT portal checks for correctness of the symmetric key entered. If the patient symmetric key conforms to the symmetric used during the patient record creation instance, then it links the doctor to the medical DLT system and retrieves or fetches the encrypted historical electronic medical records as shown in Figure 50.

4.4.9.3 Medical DLT System Fetch Historical Patient Records Sub-Module

Upon verifying and authenticating the patients' symmetric key, the medical DLT portal links the doctor back to the medical DLT system and fetches the patient records that are encrypted, hence prompting the patient to enter their Public Key (Pu), Private Key (Pr) and Symmetric Key (Sk) to decrypt their historical electronic medical records (EMRs) as shown in Figure 51.

Figure 51

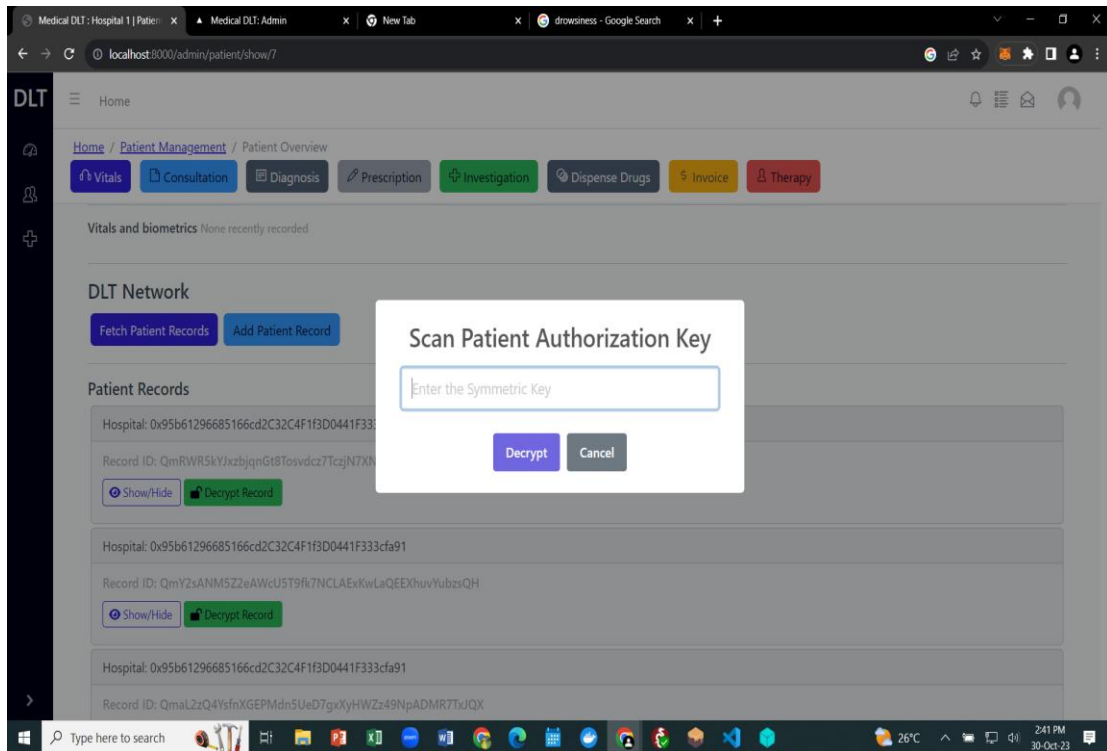
Medical DLT System Fetch Historical Patient Records Sub-Module



The encrypted patient's historical electronic medical records need to be decrypted to make them usable by the Doctor. This is another layer of security provided by the medical DLT system. It provides a multi-factor layer of authentication requiring the patient to enter their symmetric key to decrypt the EMRs once again, as shown in Figure 52.

Figure 52

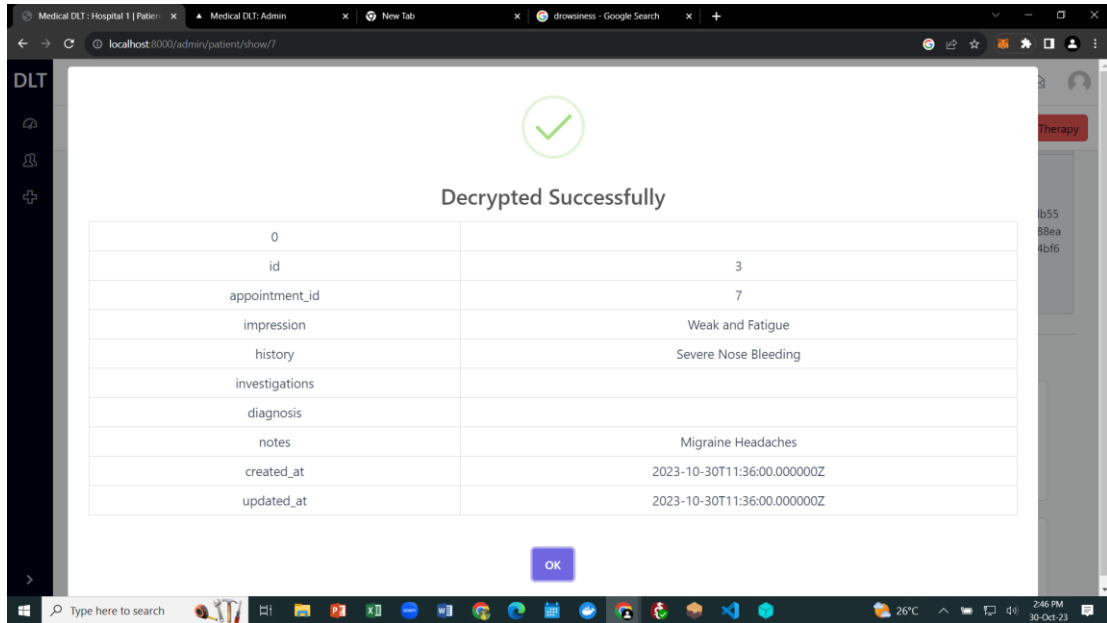
Patient Multi-Factor Layer Authentication



If the Symmetric key entered or scanned by the patient is correct, then the EMRs are decrypted and the Doctor is able to read the historical EMRs from the medical DLT; as seen in Figure 53.

Figure 53

Successful Symmetric Key Authentication for Decryption of Patient Records



The medical DLT system checks and decrypts the historical EMRs without judging from which health facility (hospital) they were entered, hence providing interoperability of medical systems.

By leveraging a Medical DLT prototype to validate an enhanced secure distributed ledger interoperability framework for medical system, the medical system software developers can address the security and interoperability challenges in the development process, resulting to a more robust, secure and interoperable medical systems.

4.5 Discussions of the Findings

In this study, an analysis was carried out to establish reasons for lack of secure interoperability of medical systems. The researcher went ahead to design an algorithm that enhances security of Distributed Ledger interoperability for medical systems. A secure distributed ledger interoperability framework prototype for medical systems was designed, developed and validated for secure medical data exchange.

4.5.1 Existing factors that affect Secure Interoperability of Medical Systems

The findings of this study showed the factors affecting secure interoperability of medical systems compared to existing systems as analyzed. This was achieved through a systematic review of literature as seen in Chapter Two, sections 2.6, 2.6.1, to 2.6.7; where the structural, semantic, security and technical factors were found to affect interoperability of medical systems. Section 2.8 highlights the interoperability frameworks for medical systems; and Section 2.11 discusses the research gaps that show the cause for interoperability challenge for medical systems.

The identified causes include structural interoperability relating to data standardization, syntax, protocols and formats; and semantic challenges which relate to medical data coding and standardization of data meanings. Further, the data that was collected from the domain experts, who were the medical systems software developers, concurred with the reviewed literature. Chapter Four, sections 4.2.1 and 4.2.2 shows that the respondents indicated that technical, semantic, security and privacy factors hinder secure interoperability of medical systems. This implies that the medical system software developers need to address the aforementioned challenges to be able to design and develop secure interoperable medical systems.

4.5.2 Algorithms Designed to Enhance Secure Distributed Ledger Interoperability Framework for Medical Systems

The study went ahead to design algorithms that enhance secure interoperability of the framework for interoperability of medical systems. This was achieved through the design of a secure interoperability algorithms in Chapter Four section 4.3.6.1 to 4.3.6.10. The algorithms include handle Proof of Authentication (PoA), record fetching, record creation, creation of patient wallet, generation and storage of symmetric key, retrieval of

symmetric key, signing of patient EMR, hashing patient EMR, encryption and decryption of patient EMR.

4.5.3 An Enhanced Distributed Ledger Interoperability Framework for improving the Security of Medical Data Exchange Between Medical Systems

The study went ahead to develop an enhanced secure Distributed Ledger Interoperability whose layout has been achieved in Chapter Four Section 4.3.3 in a figure. The figure elaborates the different layers, starting from the core technical layer, operational layer, and the interaction/application layer. It clearly outlines how the medical DLT web interface, remote procedure calls pass messages between the interaction and operation layers, and how the content identifier manages sharing of data between the Master Medical DLT and the IPFS. The interaction layer handles both the users and medical DLTVPN; the Operation Layer handles the Medical DLT Portal, API and EMR; while the Core Layer handles the Master Medical DLT comprising of Smart Contracts, Data Security Layer and consensus layer together with the IPFS.

4.5.4 Validated Enhanced Secure Distributed Ledger Interoperability Framework

This study aimed at ensuring that the enhanced secure medical DLT is interoperable; hence, validation of the secure distributed ledger interoperability framework was carried out as outlined in Chapter Four section 4.4, through proof of concept using prototype and following the delphi method various domain experts' viewpoints and opinions were included in the study. Several simulated use cases were run to validate the enhanced distributed ledger interoperability framework for secure medical systems. Sections 4.4.1 to 4.4.9.3 contains simulations of the medical DLT, API and EMR System portals, clearly outlining the measures taken and approaches applied in ensuring that there is

secure interoperability of the medical systems to guarantee security and privacy of patients' medical records in transit from one system to the other.

4.5.4.1 Validation Process

The validation was achieved through the setting up of a VPN, IPFS, Smart contracts, Medical DLT module, Patient Wallet, Medical DLT API, EMR backend, and the System web interface containing administrator, doctor, nurse and patient interfaces, that fetch and authenticate reference to patient historical records. Further the medical DLT system prototype was shared with six (6) domain experts who were purposively sampled based on the years of experience and knowledge on medical systems deployment and healthcare policies, standards and regulations for validation and evaluation which was used as the inclusion criteria.

The deployment of the developed modules in the medical DLT system prototype by the medical systems software developers enabled the validation and testing of the developed framework and algorithms that enhanced security of patient electronic medical records within medical systems by applying the distributed ledger technology. The domain experts were also given a validation guide to fill and give their feedback and opinion on six (6) validation parameters usability, security and privacy, access control, authentication and authorization, interoperability and adherence to healthcare standards of the developed Medical DLT System prototype. A validation guide questionnaire was distributed via google form to the domain experts to give their feedback. The results from the validation and evaluation are summarized in the subsequent sections.

4.5.4.2 Validation and Evaluation Metrics and Parameters

Parameter A: Usability

The sampled domain experts were supposed to indicate their opinion on the simplicity and user friendliness of use of the developed Medical DLT system prototype's user interface design in which, 80% thought the user interface design was simple to use and intuitive, whilst 20% thought otherwise. This suggests that most people found the interface to be user-friendly and had a favorable experience with it. To guarantee a flawless experience for every user, there is still space for improvement.

The participants were also required to state on a scale of 1 to 5, how they would rate the simplicity and ease of use of the developed Medical DLT system prototype for managing medical data and electronic medical records. 50% of participants rated the simplicity and ease of use as 5 (Excellent), another 40% rated it as 4 (Simple and easy to use), and 10% rated it as 3 (Fair). The high percentage of participants rating the system as excellent or simple and easy to use suggests that the medical DLT prototype is generally intuitive and straightforward for managing medical data. However, the 10% who rated it as fair highlights the need for further refinement to improve the overall user experience. Although the user interface design is intuitive, the feedback indicates that more concise and clear labels should be added to the navigation to make it better. This input is consistent with the first question's results, which show that although most users considered the interface intuitive, it could still be improved by giving navigation elements more clarity and proper labeling.

Parameter B: Security and Privacy

The study sort to understand the domain experts' opinion on whether the Medical DLT system prototype sufficiently solves privacy and security issues with handling which entails processing and sharing of patient data and electronic medical records (EMRs). Of

the participants, 90% thought the Medical DLT System prototype sufficiently tackles privacy and security issues, while 10% disagree.

This implies that most users are confident in the privacy and security features included in the prototype. To adequately address security and privacy problems, additional enhancements might be required, according to the 10% of respondents who voiced concerns. Additionally, the participants were required to indicate the extent in which they thought the Medical DLT system prototype's security safeguards are protecting sensitive patient medical data. Of the participants, 40% showed great confidence, 40% showed medium confidence, and 20% of respondents expressed little faith in the security protocols. The findings indicate that participants' levels of confidence were mixed, with an equal number expressing high and medium levels of confidence.

The 20% of users who expressed low confidence emphasizes the necessity of reinforcing security measures even more in order to increase user confidence. On the response by participants providing extra information on privacy or security flaws and vulnerabilities in the Medical DLT system prototype that they validated, 80% did not identify any specific security or privacy vulnerabilities, compared to 20% who did, indicating that additional attention and development are needed in securing third party engagements, partnerships and collaborations. This has calls for development of extra frameworks to address the issue on partnership collaborations as capture in the recommendations section 5.4.1.

Parameter C: Access Control

The participants were also required to indicate whether the Medical DLT system prototype provided adequate mechanisms for controlling user access to patient electronic medical records. All 100% of participants thought the prototype has sufficient access

control methods. This suggests that all of users were contented with the prototype's access control mechanisms integrated into the Medical DLT prototype. On a scale of 1 to 5, the participants were asked to indicate their level of satisfaction on the granularity and flexibility of the access control mechanisms implemented within the Medical DLT system prototype.

Regarding the granularity and flexibility of the access control methods, 40% of participants rated them as extremely satisfied (rating 5), 40% as satisfied (rating 4), and 20% as somewhat satisfied (rating 3). The majority of participants (80%) expressed satisfaction or extreme satisfaction with the access control mechanisms, which suggests that they offer a suitable degree of flexibility and granularity. The 20% of respondents who expressed only moderate satisfaction, however, raise the possibility that the flexibility and granularity of the access control elements could be strengthened. Upon asking the participants if they would recommend any extra modifications or additions to the Medical DLT system prototype's access control features, the results revealed that the granularity of the access control methods might be enhanced by introducing more precise roles and permissions, even though they are already good.

Parameter D: Authentication and Authorization

The study further asked the participants to indicate whether they were satisfied with the authentication and authorization mechanisms used to verify user identities within the Medical DLT system prototype. All, 100% of the participants indicated that they were satisfied with the authentication and authorization process to identifying users within the medical DLT system prototype.

On a scale of 1 to 5, the participants were requested to indicate how they would rate the Medical DLT system prototype authentication and authorization mechanisms in terms of

defining and enforcing access privileges for different user roles. The study revealed that 40% of participants rated the authentication and authorization mechanisms as excellent (rating 5), 40% rated them as good (rating 4), and 20% rated them as fair (rating 3). The bulk of participants (80%) evaluated the mechanisms as good or exceptional, according to the results, demonstrating that they successfully define and uphold access privileges for various user roles. The 20% of respondents who gave them a fair rating, however, indicate that there might be room for improvement in terms of boosting the authentication and authorization systems' efficacy and clarity. Although the authorization and authentication processes are sound, the feedback indicates that the system would benefit from further user education on multi-factor authentication capabilities and benefits.

Parameter E: Interoperability

On interoperability on the medical DLT system prototype the participants tested the interoperability of the Medical DLT system prototype with other existing medical systems. 30% of participants have not tried the prototype's compatibility with other medical systems, compared to eighty percent who have. 60% of participants managed to test the interoperability of the medical DLT system prototype with other medical systems, while 40% did not. This indicates that the majority of participants managed to evaluate the prototype's ability to integrate and exchange data with other medical systems. The 40% who did not tested interoperability may have limited their evaluation to the standalone functionality of the prototype. On a scale of 1 to 5, the participants rated the Medical DLT system prototype ability to seamlessly exchange medical data with different medical systems and platforms. 50% of participants rated the interoperability as excellent (rating 5), 40% rated it as good (rating 4), and 10% rated it as fair (rating 3). The feedback suggests that while the interoperability is good, the

medical DLT system prototype could benefit from additional testing and validation with various forms of medical systems to ensure seamless data exchange.

Parameter F: Adherence to Healthcare Standards

The study further sort to understand the domain experts opinion on whether the Medical DLT system prototype design was complying with established healthcare interoperability standards such as HL7, FHIR, and DICOM. 90% of participants believe that the prototype complies with healthcare interoperability standards, while 10% do not. This implies that most users are comfortable with the prototype's conformance to accepted healthcare regulation norms. The 10% of respondents who disagreed or expressed ambiguity, however, suggest that more precise information about the prototype's adherence to healthcare standards may need to be communicated or documented.

On asking the participants to indicate how important they thought adherence to healthcare standards is for the success and adoption of the Medical DLT system prototype, the results shown that adherence to healthcare standards is deemed highly important by 40% of participants, moderately important by 50%, and low important by 10% of participants. According to the data, 90% of participants think that following standards is at least somewhat crucial to the prototype's success and uptake. This emphasizes how important it is to maintain adherence to accepted healthcare standards in order to promote system integration and broad acceptability. Further the study sort to understand if the participants had encountered any instances where the Medical DLT system prototype deviates from healthcare standards or best practices, the feedback indicates that although the system conforms to healthcare standards, there is room for improvement in the documentation to guarantee unambiguous adherence.

In conclusion, the participants' responses, feedback and input provide insightful information about the Medical DLT system prototype's advantages and shortcomings. The majority of participants are happy with the prototype's usability, security and privacy, authentication and authorization, access control, interoperability, and conformity to healthcare standards, according to the results. The feedback aided in improving the prototype's overall efficacy and as result it will improve service delivery in healthcare industry.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter is made up of four sub sections; namely, introduction, summary, conclusion, recommendations for policy, and recommendations for future work outlined in accordance to the objectives of the study. Section 5.1 introduces the chapter five. Section 5.2 summarizes the study by outlining each objectives accomplishment. Each objective is summarized in sections 5.2.1 to 5.2.4. Section 5.3 concludes the study by outlining the achievements as per each objective. Section 5.4 contains recommendations to policy and future research. The objectives of the study were: to establish the factors affecting secure interoperability of medical systems; to design an algorithm to enhance security of DL interoperability framework for medical systems; to develop a secure DL interoperability framework for improving the security of medical data exchange between medical systems; and to validate the developed secure distributed ledger interoperability framework for secure medical data exchange.

5.2 Summary of the Findings

To create an enhanced distributed ledger interoperability framework, the research set out to solve the urgent demand for safe interoperability across medical systems. Examining variables that affect secure interoperability brought to light the difficulties that centralized medical systems face, and highlighted the need for standardized formats and procedures. This research created and implemented a DLT-based algorithm-driven framework to strengthen medical data interchange security. The framework's capacity to bridge the gap in current interoperability architectures, standards and security of medical data flow across medical systems was validated.

5.2.1 To establish the factors affecting Secure Interoperability of Medical Systems

Objective one aimed to determine factors affecting secure interoperability of medical systems. Important factors influencing safe interoperability across medical systems were established. These factors related to technical, structural, semantic and security issues. The objective underlined the difficulties of centralized medical systems that confront trust, privacy and security of patients' medical records; and the need for standardized protocols, data formats and architectural designs to guarantee secure medical data interchange.

5.2.2 To Design an Algorithm to Enhance Security of DL Interoperability Framework for Medical Systems

Objective two aimed to develop an algorithm to strengthen the distributed ledger interoperability framework's security for medical systems. In order to strengthen the security of the distributed ledger (DL) interoperability architecture, a customized algorithm that demonstrated proof of authentication was created. The objective of this algorithm was to tackle the variables that have been shown to impact the authentication of who accesses the electronic medical records (EMRs), to achieve safe flow of data in medical systems, hence improving medical systems interoperability.

5.2.3 To develop a Secure DL Interoperability Framework for Improving the Security of Medical Data Exchange Between Medical Systems

Objective three aimed to create a secure DL interoperability framework to strengthen the security of medical data exchange. The research produced a robust DL-based interoperability framework intended to improve the security of medical data exchange across different systems. The created proof of authentication consensus algorithm was integrated into this framework to provide a safe environment for data sharing among medical systems.

5.2.4 To validate the Developed Secure Distributed Ledger Interoperability Framework for Secure Medical Data Exchange

Objective four aimed to verify the secure distributed ledger interoperability framework for secure medical data exchange. Comprehensive testing and validation procedures using proof of concept prototype was used to verify the efficacy and dependability of the developed framework. Following the prototype's development, the various security, privacy, and interoperability parameters, such as, user authentication, authorization levels, access control, encryption, hashing, and signing, as well as the capacity to safely transfer patient electronic medical records between various healthcare facilities, were validated using the Delphi method.

Through multiple rounds of consultation, domain experts' feedback was gathered from medical system software engineers using the Delphi technique. This was carried out covertly in order to support impartial responses to the validation and assessment of the Medical DLT system prototype. Usability, security and privacy, access control, authentication and authorization, interoperability, and conformity to healthcare standards were among the characteristics taken into consideration in order to come to a consensus. The Delphi technique, which is structured and iterative, was used to gather and distill the opinions of domain experts. This validation confirmed that the framework can fill in the gaps in current interoperability architectures, standards and safeguard safe exchange of medical data across medical systems.

5.3 Conclusions

This study aimed to establish factors that affect the ability of medical systems to securely interoperate; to design an algorithm that enhances security of distributed ledgers of medical systems to interoperate; develop a secure distributed ledger interoperability framework that aims to improve secure exchange of medical data between medical

systems; and validate the developed secure distributed ledger interoperability framework for secure medical data exchange. All the objectives of the study were achieved.

The results highlight the urgent need for secure, standardized interoperability for medical systems. The variables that were found to be impeding safe data sharing comprised the shortcomings of the existing methods and highlighted the need for a strong remedy. Developing a secure DL interoperability framework after creating algorithms was a crucial step in tackling the problems caused by incompatible systems. The capacity of the developed framework to safely facilitate transmission of medical data was confirmed by validation findings, which highlighted the potential of the framework to completely transform healthcare data-sharing procedures.

Objective one was achieved through a systematic literature review in Chapter Two, sections 2.1, 2.2, 2.3, and 2.4. This review of literature culminated in establishing research gaps highlighted in section 2.10. Structural interoperability for handling data syntax and standardizing data formats and protocols is missing from the current medical interoperability frameworks. Addressing challenges of standardization of syntax, data formats, and protocols used globally to connect all medical systems and for safe data interchange across them can result in structural interoperability. In order to achieve semantic interoperability, medical data was codified using common models and data components with defined definitions and meanings. Sections 4.1.7.2, 4.1.7.3, and 4.1.7.4 illustrate the awareness of interoperability, sharing of information and architectural interoperability with a significant positive correlation of ($r=0.265$, $p<0.05$), and a strong correlation between healthcare organization and sharing of information across medical systems, organizational needs, and adherence to healthcare design policies.

The factors affecting secure interoperability of medical systems are covered in section 4.2.1. These factors include technical factors at 32%; semantic factors at 22%; security and privacy factors at 20%; legal and regulatory factors at 11%; organization financial factors at 10%; and human and cultural factors at 5%. Barriers to secure interoperability of medical systems under technical, semantic and security factors are covered in section 4.2.2; where data confidentiality, integrity led at 83.3%, followed by ease of access, data portability and scalability of system at 62.5%; and file sharing at 50%. Section 4.2.5 shows the level of awareness of security standards and policies; where 75% of respondents indicated their awareness of security principles governing medical system design, and the same percentage (75%) indicating their awareness of interoperability problems associated with medical systems. Section 4.2.6.2 showed the level of awareness of medical systems interoperability, where structural level returned 75% awareness response.

Objective two was to design an algorithm to enhance security of distributed ledger interoperability framework for medical systems. This has been achieved in section 4.3, while section 4.3.1 illustrates the design requirements for the medical DLT interoperability architectural framework, further illustrated in figure 18. Algorithms to enhance the security of DLT interoperability framework for medical systems in this study are highlighted in sections 4.3.6 to 4.3.6.11. The designed algorithms include, proof of authentication, fetch record, create record, create patient wallet, generate and store symmetric key, retrieve symmetric key, sign patient EMR plaintext, hash EMR plaintext, encrypt patient EMR plaintext, and decrypt patient EMR cipher.

Objective three was to develop a secure distributed ledger interoperability framework for improving the security of medical data exchange between medical systems. This objective has been achieved in Section 4.3.3, where secure medical DLT interoperability

framework layout for secure medical exchange, which highlights the interaction, operation and core layers, is shown in figure 19. The Core Layer of the framework contains the Master Medical DLT that comprises of the consensus layer, smart contracts and data security layer, and the InterPlanetary File System (IPFS). The Master Medical DLT houses the administration module allowing regulatory bodies to create and accredit health care facilities referred in the study as nodes. The operational layer contains the Medical DLT Portal, API and EMR. The Medical DL Portal which allows the system administrators to create health facilities and wallets; and patients to create their wallets through the VPN as per the accredited credentials. The Medical DLT API interfaces, the Medical DLT and Medical EMR ensure secure communication and data exchange of patient data.

The Medical DLT EMR enhances the interoperability of medical systems through storage of patient medical data via standardized patient data formats shared across health facilities. This has been achieved through integration of Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR) and Clinical Data Interchange Standards Consortium (CDISC) standards. It also applies International Categorization of Disease (ICD) standard for diagnosing conditions, and applies Logical Observation Identifiers Names and Codes (LOINC) standard in the identification of health measurements.

Objective four was to validate the developed secure distributed ledger interoperability framework for secure medical exchange. This Objective has been achieved in sections 4.4.1 to 4.4.9.3 Validation was achieved through the use of proof of concept using prototyping of a Medical DLT system module, including the web interface, API, Portal, Smart contract, Patient Wallet, IPFS and VPN, and simulated data to test how the interoperability aspect of the system was achieved. The prototype evaluated the designed algorithms used for the implementation of the enhanced secure framework for

interoperability of Medical Systems. The validated results proved that the developed framework and algorithms for secure medical systems interoperability successfully addressed the interoperability challenges identified in the development of existing medical systems; thereby ensuring robustness and security of the developed framework.

This research has brought forth significant contributions to the existing knowledge in the field of secure distributed ledger interoperability for medical systems. The study has suggested an enhanced secure distributed ledger interoperability framework for medical systems that overcomes the drawbacks of the existing methods, offering a more complete and reliable solution for smooth integration and data interchange between disparate medical systems. The unique architecture of the framework improves the general confidentiality, integrity, and non-repudiation of patients' medical data by including cutting-edge security features like multi-layered encryption, multilayered authentication and authorization, decentralized identity management, integrity of EMRs and tamper-evident auditing.

Through the integration of strengthened security mechanisms and distributed ledger technology (DLT), the framework provides a comprehensive solution for the safe exchange and access of medical data across various systems and platforms. The field of distributed ledger technology has extended its understanding of how to apply distributed ledger interoperability protocols, consensus processes, and encryption approaches to enhance data interoperability and integrity in healthcare contexts. Furthermore, the corpus of knowledge regarding the deployment of safe medical information systems has increased as a result of the investigation of security flaws and threat mitigation techniques.

Additionally, this work has advanced knowledge of the particular difficulties and specifications involved in establishing secure interoperability in the medical field, where patient safety, regulatory compliance, and data privacy are crucial. The thorough examination of the current obstacles and the suggested fixes broaden the body of knowledge in this important sector, opening the door for future developments.

This research has important practical ramifications since the healthcare sector may be greatly impacted by the enhanced secure distributed ledger interoperability framework. The framework facilitates the safe sharing and exchange of patient data and electronic medical records (EMRs) between healthcare organizations across organizational boundaries by offering a scalable and flexible solution that can be easily integrated into current medical systems.

Practically speaking, putting this approach into practice can result in better patient outcomes, better healthcare coordination and more effective healthcare delivery. Healthcare providers are better equipped to make judgments, lower the possibility of medical errors and offer individualized care that is catered to the needs of each patient when the safe and rapid sharing of medical data is enabled. The developed framework offers real advantages to patients, healthcare providers, and other stakeholders, with substantial implications for the healthcare sector. The framework enables safe and transparent data transfer between medical systems, which promotes smooth interoperability and improves patient outcomes, care coordination, and the effectiveness of healthcare delivery. The framework can be utilized by healthcare establishments to surmount interoperability obstacles, optimize data sharing procedures, and guarantee data confidentiality and integrity throughout the healthcare network.

Additionally, putting strong security measures in place guarantees adherence to legal obligations like GDPR and HIPAA while protecting private patient medical data from hacking, illegal access, and other security lapses. The framework's compliance with legal and healthcare standards, including HIPAA and with GDPR, guarantees healthcare companies can take advantage of the advantages of secure distributed ledger technology while staying compliant. Consequently, this can facilitate the development of patient trust and promote a more open and responsible healthcare system. In the end, the actual implementation of the suggested framework might change how medical data is shared, handled, and used, which could lead to resulting in enhanced patient experiences and healthcare outcomes.

In conclusion, the study described in this thesis adds significant knowledge and solutions to the continuous efforts to improve security and interoperability in medical systems. The framework provides a promising route towards a more interconnected, safe, and effective healthcare ecosystem by bridging the gap between theory and practice, which will eventually benefit patients and healthcare professionals alike.

5.4 Recommendations

This section summarizes the recommendations to policy and recommendations to further research as explained in details in the subsequent sections.

5.4.1 Policy Recommendations

The following are the specific policy recommendations on the implementation of interoperability rules and policies relating to the standardization of data formats in medical systems.

- i. **Establishing National Standards:** This study promotes the creation of national standards and their application to data formats and recommendations for interoperability in medical systems. The study suggests that relevant parties and stakeholders, including governmental bodies, healthcare institutions, IT professionals, and regulatory bodies, create and implement these medical standards and rules worldwide.
- ii. **Legal Requirements for Adherence:** The study suggests passing legislation mandating that medical healthcare institutions follow standardized data formats and interoperability norms. To ensure compliance and promote adoption, the medical and healthcare regulatory agencies may need to provide incentives or sanctions.
- iii. **Promoting the Acceptance of Secure Interoperability:** The study suggests that the Ministry of Health (MoH) provide tax exemptions, grants, and other financial assistance to medical and healthcare organizations that actively adopt and implement interoperability standards. This would encourage the healthcare sector to embrace standardized medical systems swiftly.
- iv. **Collaborative Frameworks and Partnerships:** The study suggests the promotion of partnerships and collaborations between technology firms, regulatory authorities, the public and commercial medical and healthcare institutions to build comprehensive frameworks for data standardization and interoperability. This collaboration could facilitate the creation of beneficial laws and regulations.
- v. **Education and Training Programs:** The study further suggests that the MoH launch educational and training programs to familiarize medical staff and software developers for medical systems with the importance, benefits, and techniques of implementing interoperability protocols and standardized data

formats. This ensures smooth deployment and execution across all medical and healthcare levels.

- vi. **Frequent Audits and Assessments:** The study proposes that the MoH regularly audits and assesses medical systems to ascertain if compliance with medical systems is practical and adheres to established criteria for continuous improvement and adherence to evolving best practices.
- vii. **Data Security and Privacy Safeguards:** To protect patients' medical data security and privacy, the study suggests incorporating stringent processes within the healthcare policy framework. Standardizing data communication should ensure that private medical information is not accessible to unauthorized parties and that patient confidentiality is not compromised.
- viii. **Adaptation to Technology Advancements:** The study suggests that the MoH should establish rules that allow for adaptable changes in response to fresh technology innovations and advancements in data management. Regular updates and modifications are required to keep up with standards, regulations, and technological improvements.
- ix. **Multinational Collaboration and Alignment:** The study recommends collaborating with international medical and healthcare standardization bodies and harmonizing regulations with international standards, which are necessary to promote interoperability across national boundaries and facilitate the easy exchange of medical data for improved patient care worldwide.
- x. **Public Awareness and Engagement:** The study recommends that the MoH launch public awareness initiatives to inform and engage patients about the need for interoperability and standardized medical data formats in healthcare. Inform patients about the benefits of interoperable medical systems and their rights to

access their medical records. If these policy recommendations are implemented carefully and systematically, standardizing data formats and interoperability standards may significantly increase medical systems' effectiveness, security, and efficiency.

5.5 Recommendations for Further Research

The conclusions of the study allow for the following research suggestions on development of interoperable medical systems and shared medical data in future:

- i. Examine emerging technologies or technology advancements to aid secure interoperability by looking at how implementing standardized data formats like Fast Healthcare Interoperability Resources (FHIR), among other emerging technology advances like use of Internet of Things (IoT), has improved EMR interoperability.
- ii. Effects of secure interoperability on Medical System: Future research can focus on how better interoperability could affect the healthcare industry, specifically how it can lower medical mistakes, simplify care coordination, and make patient health histories more accessible.
- iii. Regulatory environment and organizational responses: Examine how interoperability affects industry participants and stakeholders. This can take into account leadership concerns, business partnerships and agreements, new processes and data requirements, and the necessity for comprehensive organizational responses in readiness for changes in the regulatory environment.
- iv. Technical capabilities and infrastructure: Future research could examine other medical platforms and underlying technical capabilities, such as data input, integration, sharing considerations, controls, and infrastructure, which are required to make interoperability of medical systems a reality.

Besides addressing technical capabilities, legal settings, and technological improvements, these recommendations are meant to direct future research efforts toward the goal of establishing secure interoperable and shareable medical data among medical systems in the healthcare industry.

REFERENCES

- (AIRA), A. I. R. A. (2020). *Evaluation of Data Exchange Technologies for Communicating with IIS. 1*(08162010), 1–15.
- (ONC), T. O. of the N. C. for H. I. T. (2019). Standards and Interoperability Framework. *HealthIT.Gov*. <https://www.healthit.gov/topic/interoperability>
- Abernethy, A., Adams, L., Barrett, M., Bechtel, C., & Brennan, P. (2022). The Promise of Digital Health: Then, Now, and the Future Digital Health in the 21st Century. *NAM Perspectives*.
- Accenture. (2019). *Cyber Threatscape Report 2019*. 71. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf
- Acuña Ulloa, K. E., & Cabanillas Castillo, J. C. (2022). On the Dual Attack of LWE Schemes in the Presence of Hints. *Cryptology EPrint Archive, 1*, 270–276. <https://ehrintelligence.com/features/how-health-data-standards-support-healthcare-interoperability>
- Ajayi, O., Abouali, M., & Saadawi, T. (2020). Secure architecture for inter-healthcare electronic health records exchange. *IEMTRONICS 2020 - International IOT, Electronics and Mechatronics Conference, Proceedings*. <https://doi.org/10.1109/IEMTRONICS51293.2020.9216336>
- Al-mutar, F. H. N., Ucan, O. N., & Ibrahim, A. A. (2022). Providing scalability and privacy for smart contract in the healthcare system. *Optik, 271*, 170077. <https://doi.org/10.1016/J.IJLEO.2022.170077>
- Albarki, I., Rasslan, M., Bahaa-eldin, A. M., & Sobh, M. (2019). ScienceDirect Robust Hybrid-Security Hybrid-Security Protocol Protocol for for HealthCare HealthCare Systems Systems. *Procedia Computer Science, 160*(2018), 843–848. <https://doi.org/10.1016/j.procs.2019.11.001>
- Albouq, S. S., Sen, A. A. A., Almashf, N., Yamin, M., Alshantqiti, A., & Bahbouh, N. M. (2022). A Survey of Interoperability Challenges and Solutions for Dealing With Them in IoT Environment. *IEEE Access, 10*, 36416–36428. <https://doi.org/10.1109/ACCESS.2022.3162219>
- AlQudah, A. A., Al-Emran, M., & Shaalan, K. (2021). Medical data integration using HL7 standards for patient's early identification. *PLoS ONE, 16*(12). <https://doi.org/10.1371/JOURNAL.PONE.0262067>
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*(November 2018), 143–174. <https://doi.org/10.1016/j.rser.2018.10.014>
- Andrew, J., Priya, D., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems : Architecture , security challenges , trends and future directions. *Journal of Network and Computer Applications, 215*(September 2022), 103633. <https://doi.org/10.1016/j.jnca.2023.103633>
- Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed ledger technology review and decentralized applications development guidelines. *Future Internet, 13*(3), 62. <https://doi.org/10.3390/fi13030062>

- Anthony Jnr., B. (2023). A developed distributed ledger technology architectural layer framework for decentralized governance implementation in virtual enterprise. In *Information Systems and e-Business Management* (Issue 1). Springer Berlin Heidelberg. <https://doi.org/10.1007/s10257-023-00634-2>
- Anthony Jnr, B. (2021). Distributed Ledger and Decentralised Technology Adoption for Smart Digital Transition in Collaborative Enterprise. *Enterprise Information Systems*. <https://doi.org/10.1080/17517575.2021.1989494>
- Arlindo, F. da C., Silva, F. S. C. da, Rocha, V., Locoro, A., & Jo. (2018). (PDF) *Eletronic Health Records using Blockchain Technology*. https://www.researchgate.net/publication/324793302_Eletronic_Health_Records_using_Blockchain_Technology
- Arslan, S. S., Jurdak, R., Jelitto, J., & Krishnamachari, B. (2020). Advancements in distributed ledger technology for Internet of Things. *Internet of Things (Netherlands)*, 9. <https://doi.org/10.1016/j.iot.2019.100114>
- Australia, K. (2020). *Voices on 2030 Digitalising government*.
- Azbeq, K., Ouchetto, O., Jai Andaloussi, S., & Fetjah, L. (2021). An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions. *Advances in Intelligent Systems and Computing*, 1188(August 2022), 357–369. https://doi.org/10.1007/978-981-15-6048-4_31
- Bakibinga, P., Kamande, E., Kisia, L., Omuya, M., Matanda, D. J., & Kyobutungi, C. (2020). Challenges and prospects for implementation of community health volunteers' digital health solutions in Kenya: a qualitative study. *BMC Health Services Research*, 20(1), 888. <https://doi.org/10.1186/s12913-020-05711-7>
- Baron, R., & Chaudey, M. (2019). Blockchain and Smart-Contract: A Pioneering Approach of Inter-Firms Relationships? The Case of Franchise Networks. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3378477>
- Baysal, M. V., Özcan-Top, Ö., & Betin-Can, A. (2023). Blockchain technology applications in the health domain: a multivocal literature review. *The Journal of Supercomputing*, 79(3), 3112–3156. <https://doi.org/10.1007/s11227-022-04772-1>
- Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2020). A survey on blockchain interoperability: Past, present, and future trends. *ArXiv*.
- Belfer, R., Kashtalian, A., Nicheporuk, A., Markowsky, G., & Sachenko, A. (2020). Proof-of-activity consensus protocol based on a network's active nodes. *CEUR Workshop Proceedings*, 2623, 239–251.
- Belmonte, E. M., & Ot, S. (2021). *Proposal for a Standard Architecture for the Integration of Clinical*.
- Bhartiya, S., & Mehrotra, D. (2013). Exploring interoperability approaches and challenges in healthcare data exchange. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8040 LNCS, 52–65. https://doi.org/10.1007/978-3-642-39844-5_8

- Blobel, B. (2016). Interoperability is more than just technology. *European Journal for Biomedical Informatics*, 12(01), 12–13. <https://doi.org/10.24105/ejbi.2016.12.1.1>
- Bokolo, A. J. (2022). Exploring interoperability of distributed Ledger and Decentralized Technology adoption in virtual enterprises. *Information Systems and E-Business Management*, 20(4), 685–718. <https://doi.org/10.1007/S10257-022-00561-8/TABLES/6>
- Braunstein, M. L. (2018). Healthcare in the age of interoperability: The promise of fast healthcare interoperability resources. *IEEE Pulse*, 9(6), 24–27. <https://doi.org/10.1109/MPUL.2018.2869317>
- Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating Health Activity Data Using Distributed Ledger Technologies. *Computational and Structural Biotechnology Journal*, 16. <https://doi.org/10.1016/j.csbj.2018.06.004>
- Budman, M.;e. al. (2021). *Deloitte's 2021 Global Blockchain Survey* (p. 28). [https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf%0ADeloite Insights](https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf%0ADeloite%20Insights)
- Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (PoET). *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10616 LNCS(May 2019), 282–297. https://doi.org/10.1007/978-3-319-69084-1_19
- Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access*, 7, 74361–74382. <https://doi.org/10.1109/ACCESS.2019.2919982>
- Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS ONE*, 15(12 December), e0243043. <https://doi.org/10.1371/journal.pone.0243043>
- Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M., & Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. *IEEE Access*, 7, 167930–167943. <https://doi.org/10.1109/ACCESS.2019.2953729>
- Clunie, D. A. (2021). DICOM Format and Protocol Standardization—A Core Requirement for Digital Pathology Success. *Toxicologic Pathology*, 49(4), 738–749. <https://doi.org/10.1177/0192623320965893>
- Cohen, T. (2020a). Middleware System - an overview | ScienceDirect Topics. *Science Direct*, 2(2), 543–549. <https://www.sciencedirect.com/topics/engineering/middleware-system>
- Cohen, T. (2020b). The integration and convergence of medical and information technologies. *Clinical Engineering Handbook, Second Edition*, 543–549. <https://doi.org/10.1016/B978-0-12-813467-2.00082-1>

- Colombo, F., Oderkirk, J., & Slawomirski, L. (2020). Health Information Systems, Electronic Medical Records, and Big Data in Global Healthcare: Progress and Challenges in OECD Countries. In *Handbook of Global Health*. https://doi.org/10.1007/978-3-030-05325-3_71-1
- da Conceição, A. F., da Silva, F. S. C., Rocha, V., Locoro, A., & Barguil, J. M. (2018). *Electronic Health Records using Blockchain Technology*. <http://arxiv.org/abs/1804.10078>
- Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39, 283–297. <https://doi.org/10.1016/j.scs.2018.02.014>
- Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A Survey. *IEEE Internet of Things Journal*, 6(5), 8076–8094. <https://doi.org/10.1109/JIOT.2019.2920987>
- Das, S., & Port, S. (2018). *COMPARISON OF FTP V/S FTPS*. 6(1), 1125–1128.
- Dawood, M., Tu, S., Xiao, C., Alasmay, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*, 15(11), 1–33. <https://doi.org/10.3390/sym15111981>
- de Mello, B. H., Rigo, S. J., da Costa, C. A., da Rosa Righi, R., Donida, B., Bez, M. R., & Schunke, L. C. (2022). Semantic interoperability in health records standards: a systematic literature review. *Health and Technology*, 12(2), 255–272. <https://doi.org/10.1007/S12553-022-00639-W/FIGURES/4>
- Denecke, K. (2021). Biomedical Standards and Open Health Data. *Systems Medicine*, 521–531. <https://doi.org/10.1016/B978-0-12-801238-3.11527-2>
- Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. *Science and Technology*, 13(July), 29–35. <https://doi.org/10.5923/j.scit.20231302.04>
- Durneva, P., Cousins, K., & Chen, M. (2020). The Current State of Research, Challenges, and Future Research Directions of Blockchain Technology in Patient Care: Systematic Review. *Journal of Medical Internet Research*, 22(7), e18619. <https://doi.org/10.2196/18619>
- Edemekong, P. F., & Micelle, J. H. (2020). Health Insurance Portability and Accountability Act (HIPAA). In *Encyclopedia of Information Assurance* (pp. 1299–1309). CRC Press. <https://doi.org/10.1081/e-eia-120046838>
- Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data*. https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf
- Eklund, J. M. (2019). *Blockchain Technology in Healthcare: A Systematic Review*. <https://doi.org/10.3390/healthcare7020056>
- El Ioini, N., & Pahl, C. (2018). A review of distributed ledger technologies. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11230 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-02671-4_16

- Elvas, L. B., Serrão, C., & Ferreira, J. C. (2023). Sharing Health Information Using a Blockchain. *Healthcare (Basel, Switzerland)*, *11*(2). <https://doi.org/10.3390/healthcare11020170>
- Emergen Research. (2022). *Interoperability Solution in Healthcare Market Trend / Healthcare Interoperability Solutions Industry Forecast 2021-2030*. Emergen Research. <https://www.emergenresearch.com/industry-report/interoperability-solutions-in-healthcare-market>
- Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. <https://doi.org/10.1109/MCC.2018.011791712>
- Eunice, O., Dorothy, B., & Omosa, O. (2019). The Impact of Cyber Attacks on E-Businesses. *IJCSN-International Journal of Computer Science and Network*, *8*(4), 354–357. www.IJCSN.org
- European Commission, & Directorate-General for Communications Networks Content and Technology. (2013). eHealth European Interoperability Framework. In *Deloitte Consulting*. <https://doi.org/10.2759/14325>
- Ezéchiél, K. K., Kant, S., & Agarwal, R. (2019). A systematic review on distributed databases systems and their techniques. *Journal of Theoretical and Applied Information Technology*, *97*(1), 236–266.
- Facundo, S., Agostino, D., & Timpanaro, J. P. (2017). *Ripple Protocol performance improvement: Small world theory applied to cross border payments*. 143–154. <http://47jaiio.sadio.org.ar/sites/default/files/ASSE-13.pdf>
- Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*, *177*, 102936. <https://doi.org/10.1016/J.JNCA.2020.102936>
- Fernandez, E. B., Wu, J., & Qian, H. (2000). Combined functional and object-oriented approach to software design. *International Journal of Computers and Applications*, *22*(2), 51–61. <https://doi.org/10.1080/1206212X.2000.11441601>
- Frikha, T., Chaabane, F., Aouinti, N., Cheikhrouhou, O., Ben Amor, N., & Kerrouche, A. (2021). Implementation of Blockchain Consensus Algorithm on Embedded Architecture. *Security and Communication Networks*, *2021*. <https://doi.org/10.1155/2021/9918697>
- Gagnon, M. L., & Stephen, G. (2018). A Pragmatic Solution to a Major Interoperability Problem: Using Blockchain for the Nationwide Patient Index. *Blockchain in Healthcare Today*, *1*, 1–9. <https://doi.org/10.30953/bhty.v1.28>
- García, J. F., Hieronimus, S., Spatharou, A., Beck, J.-P., & Jenkins, J. (2020). Transforming healthcare with AI The impact on the workforce. *McKinsey & Company, March*, 1–131.
- Gomathy, C. K. (2021). *The building of hypertext transfer protocol server*. December.
- Guclu, M., Bakir, C., & Hakkoymaz, V. (2020). A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security. *Scientific Programming*, *2020*. <https://doi.org/10.1155/2020/8875069>

- Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access*, 8, 125244–125262. <https://doi.org/10.1109/ACCESS.2020.3007251>
- Haque, A. K. M. B., Arifuzzaman, B. M., Siddik, S. A. N., Kalam, A., Shahjahan, T. S., Saleena, T. S., Alam, M., Islam, M. R., Ahmmed, F., & Hossain, M. J. (2022). Semantic Web in Healthcare: A Systematic Literature Review of Application, Research Gap, and Future Research Avenues. *International Journal of Clinical Practice*, 2022. <https://doi.org/10.1155/2022/6807484>
- Hassan, M. M., Lin, K., Yue, X., & Wan, J. (2017). A multimedia healthcare data sharing approach through cloud-based body area network. *Future Generation Computer Systems*, 66, 48–58. <https://doi.org/10.1016/j.future.2015.12.016>
- Health Act, K. M. of H. (2017). The Health Act. *Health Act, 2017*, 59(59), 165. http://www.ilo.org/dyn/travail/docs/505/Employment_Act_2007.pdf
- Health Insurance Portability and Accountability Act (HIPAA) - StatPearls - NCBI Bookshelf*. (n.d.). Retrieved March 12, 2020, from <https://www.ncbi.nlm.nih.gov/books/NBK500019/>
- Hegde, P., & Maddikunta, P. K. R. (2023). Amalgamation of Blockchain with resource-constrained IoT devices for healthcare applications – State of art, challenges and future directions. *International Journal of Cognitive Computing in Engineering*, 4, 220–239. <https://doi.org/10.1016/j.ijcce.2023.06.002>
- HelpSystems. (2020). *Managed File Transfer*.
- HIMSS. (2022). *Interoperability in Healthcare | HIMSS*. <https://www.himss.org/resources/interoperability-healthcare>
- Holweger, J., Bloch, L., Ballif, C., & Wyrsh, N. (2021). *Privacy-preserving methods for smart-meter-based network simulations*. <http://arxiv.org/abs/2110.03491>
- Hong Kong Monetary Authority. (2016). Whitepaper On Distributed Ledger Technology. *Astri*, 98. http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf
- Ibañez, J. I., & Rua, F. (2023). The Energy Consumption of Proof-of-Stake Systems: Replication and Expansion. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4324137>
- IBM. (2021). IBM: Cost of a Data Breach Report. *Computer Fraud & Security*, 2021(8), 4–4. [https://doi.org/10.1016/s1361-3723\(21\)00082-8](https://doi.org/10.1016/s1361-3723(21)00082-8)
- Institute, F. R. (2020). *Survey on HL7 FHIR Final Report. March*.
- ISO/IEC. (2020). *ISO 27001 A Complete Guide - 2020 Edition*. <https://www.scribd.com/read/424717726/ISO-27001-A-Complete-Guide-2020-Edition>
- ITU-T FG DLT. (2019). Distributed ledger technology regulatory framework. *Technical Report FG DLT D4.1*. <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d41.pdf>
- Iyengar-Emens, R. (2018). Blockchain in Healthcare: A Data-Centric Perspective. In *Medium*. <https://medium.com/crypto-oracle/blockchain-in-healthcare-a-data-centric-perspective-109e898d73f3>

- Juárez, I. A., Nicanor, L. D., De La Vega, J. A., & Hernández, J. E. M. (2022). API Design based on HL7 standard to interoperability of medical information systems. *Applications in Software Engineering - Proceedings of the 11th International Conference on Software Process Improvement, CIMPS 2022*, 60–68. <https://doi.org/10.1109/CIMPS57786.2022.10035566>
- June Okal. (2018). *General Data Protection Regulation: What Kenyans Need to Know*. <https://techweez.com/2018/04/27/gdpr-need-care/>
- Kangas, E. (n.d.). *HIPAA-compliant Email Basics: Safeguarding Your Healthcare Practice and Protecting Patient Privacy*. Retrieved October 14, 2023, from https://luxsci.com/hipaa-ebook/adwords/head-terms/hipaa?adwords/SL&utm_term=hipaa_rule&utm_campaign=&utm_source=adwords&utm_medium=ppc&hsa_acc=5253494179&hsa_cam=1757586410&hsa_grp=151101221278&hsa_ad=662318052675&hsa_src=g&hsa_tgt=kwd-320885643071&hsa_kw
- Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2020). Trade-offs between Distributed Ledger Technology Characteristics. *ACM Computing Surveys*, 53(2). <https://doi.org/10.1145/3379463>
- Katehakis, D. G., & Kouroubali, A. (2019). A Framework for eHealth Interoperability Management. *Journal of Strategic Innovation and Sustainability*, 14(5), 51–61. <https://doi.org/10.33423/jsis.v14i5.2521>
- Kim, J., Macieira, T. G. R., Meyer, S. L., Ansell (Maggie), M., Bjarnadottir (Raga), R. I., Smith, M. B., Citty, S. W., Schentrup, D. M., Nealis, R. M., & Keenan, G. M. (2020). Towards implementing SNOMED CT in nursing practice: A scoping review. *International Journal of Medical Informatics*, 134. <https://doi.org/10.1016/j.ijmedinf.2019.104035>
- Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors (Switzerland)*, 20(10). <https://doi.org/10.3390/s20102913>
- Kotey, S. D., Tchao, E. T., Ahmed, A. R., Agbemenu, A. S., Nunoo-Mensah, H., Sikora, A., Welte, D., & Keelson, E. (2023). Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication. *IET Communications*, 17(8), 891–914. <https://doi.org/10.1049/cmu2.12594>
- Kothari, C. R. (2004). Research Methodology. In *Second Revised Edition* (Second, Vol. 59). NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS.
- Kouroubali, A., & Katehakis, D. G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of Biomedical Informatics*, 94(April), 103166. <https://doi.org/10.1016/j.jbi.2019.103166>
- Krishnamohan, T. (2022). Proof of identity - a blockchain consensus algorithm to create a dynamically permissioned blockchain. *International Journal of Blockchains and Cryptocurrencies*, 3(4), 289. <https://doi.org/10.1504/IJBC.2022.128888>
- Krishnamurthi, R., & Shree, T. (2021). A Brief Analysis of Blockchain Algorithms and Its Challenges. <https://Services.Igi-Global.Com/Resolvedoi/Resol ve.aspx?Doi=10.4018/978-1-7998-5351-0.Ch002>, 23–39. <https://doi.org/10.4018/978-1-7998-5351-0.CH002>

- Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *MDPI*, 1–17. <https://doi.org/10.3390/computers9010018>
- Kruse, C. S., Stein, A., Thomas, H., & Kaur, H. (2018). The use of Electronic Health Records to Support Population Health: A Systematic Review of the Literature. In *Journal of Medical Systems* (Vol. 42, Issue 11, pp. 1–16). Springer New York LLC. <https://doi.org/10.1007/s10916-018-1075-6>
- Kuo, J. W. Y., & Kuo, A. M. H. (2017). Integration of health information systems using HL7: A case study. *Studies in Health Technology and Informatics*, 234, 188–194. <https://doi.org/10.3233/978-1-61499-742-9-188>
- Kuo, N. (2015). Action Research for Improving the Effectiveness of Technology Integration in Preservice Teacher Education Action Research for Improving the Effectiveness of Technology Integration in Preservice Teacher Education. *I.E.: Inquiry in Education*, 6(1), 1–19. <https://doi.org/10.1130/G33059.1>
- Laroiya, C., Saxena, D., & Komalavalli, C. (2020). Applications of Blockchain Technology. In *Handbook of Research on Blockchain Technology*. INC. <https://doi.org/10.1016/b978-0-12-819816-2.00009-5>
- Le Nguyen, T. (2018). Blockchain in healthcare: A new technology benefit for both patients and doctors. *PICMET 2018 - Portland International Conference on Management of Engineering and Technology: Managing Technological Entrepreneurship: The Engine for Economic Growth, Proceedings*. <https://doi.org/10.23919/PICMET.2018.8481969>
- Lehne, M., Sass, J., Essenwanger, A., Schepers, J., & Thun, S. (2019). Why digital medicine depends on interoperability. *Npj Digital Medicine*, 2(1), 1–5. <https://doi.org/10.1038/s41746-019-0158-1>
- Leonulous, R. (2020). *Various types of Distributed Ledger Technology / DataDrivenInvestor*. <https://www.datadriveninvestor.com/2020/12/04/various-types-of-distributed-ledger-technology/>
- Li, E., Clarke, J., Ashrafian, H., Darzi, A., & Neves, A. L. (2022). The Impact of Electronic Health Record Interoperability on Safety and Quality of Care in High-Income Countries: Systematic Review. *Journal of Medical Internet Research*, 24(9), 1–15. <https://doi.org/10.2196/38144>
- Li, E., Clarke, J., Neves, A. L., Ashrafian, H., & Darzi, A. (2021). Electronic Health Records, Interoperability and Patient Safety in Health Systems of High-income Countries: A Systematic Review Protocol. *BMJ Open*, 11(7), 1–5. <https://doi.org/10.1136/bmjopen-2020-044941>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egy.2021.08.126>
- Liang, H. W., Chu, Y. C., & Han, T. H. (2023). Fortifying Health Care Intellectual Property Transactions With Blockchain. *Journal of Medical Internet Research*, 25. <https://doi.org/10.2196/44578>

- Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2018). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, 2017-October*, 1–5. <https://doi.org/10.1109/PIMRC.2017.8292361>
- Lorenzen, B., & Schwartz, A. (2021). Changes in Emergency Department Patient Volume and Acuity Associated with Early Stages of the COVID-19 Pandemic in a Unique Environment. *The Permanente Journal*, 25(2). <https://doi.org/10.7812/TPP/20.212>
- Lv, T., Yan, P., & He, W. (2019). On Massive JSON Data Model and Schema. *Journal of Physics: Conference Series*, 1302(2). <https://doi.org/10.1088/1742-6596/1302/2/022031>
- Makridakis, S., & Christodoulou, K. (2019). Blockchain: Current challenges and future prospects/applications. *Future Internet*, 11(12), 1–16. <https://doi.org/10.3390/FI11120258>
- Manolache, M. A., Manolache, S., & Tapus, N. (2021). Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Computer Science*, 199, 580–588. <https://doi.org/10.1016/j.procs.2022.01.071>
- McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135(September 2018), 62–75. <https://doi.org/10.1016/j.jnca.2019.02.027>
- Mehta, S., Grant, K., & Ackery, A. (2020). Future of blockchain in healthcare: Potential to improve the accessibility, security and interoperability of electronic health records. *BMJ Health and Care Informatics*, 27(3). <https://doi.org/10.1136/bmjhci-2020-100217>
- Mishra, A. R., Rani, P., Alrasheedi, A. F., & Dwivedi, R. (2023). Evaluating the blockchain-based healthcare supply chain using interval-valued Pythagorean fuzzy entropy-based decision support system. *Engineering Applications of Artificial Intelligence*, 126. <https://doi.org/10.1016/j.engappai.2023.107112>
- Mitchell, M., & Kan, L. (2019). Digital Technology and the Future of Health Systems. *Health Systems and Reform*, 5(2), 113–120. <https://doi.org/10.1080/23288604.2019.1583040>
- MoH Kenya. (2020). Kenya Health Information Systems Interoperability Framework Table of Contents. *Global Partnership for Sustainable Development Data*. [https://www.data4sdgs.org/sites/default/files/services_files/Kenya Health Information Systems Interoperability Framework.pdf](https://www.data4sdgs.org/sites/default/files/services_files/Kenya_Health_Information_Systems_Interoperability_Framework.pdf)
- MoH, M. of H. (2021). *2021 Kenya Medical Devices eHealth*.
- Moon, J., Do, J., Lee, D., & Choi, G. W. (2020). A conceptual framework for teaching computational thinking in personalized OERs. *Smart Learning Environments*, 7(1). <https://doi.org/10.1186/s40561-019-0108-z>
- Moubarak, J., Chamoun, M., & Filiol, E. (2020). On distributed ledgers security and illegal uses. *Future Generation Computer Systems*, 113, 183–195. <https://doi.org/10.1016/j.future.2020.06.044>

- Muinga, N., Magare, S., Monda, J., English, M., Fraser, H., Powell, J., & Paton, C. (2020). Digital health Systems in Kenyan Public Hospitals: A mixed-methods survey. *BMC Medical Informatics and Decision Making*, 20(1), 1–14. <https://doi.org/10.1186/s12911-019-1005-7>
- Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., & Balusamy, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing and Applications*, 32(3), 639–647. <https://doi.org/10.1007/s00521-018-3915-1>
- NAHIT. (2005). *What is National Alliance for Health Information Technology (NAHIT)? -Definition from WhatIs.com*. <https://www.techtarget.com/search/healthit/definition/National-Alliance-for-Health-Information-Technology-NAHIT>
- Natarajan, H., Krause, S. K., & Gradstein, H. L. (2017). Distributed Ledger Technology (DLT) and Blockchain. *FinTech Note*, 1, 1–60. <http://hdl.handle.net/10986/29053%0Ahttp://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>
- Olsson, M. (2020). *A study and review of distributed ledger technologies*. C. <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1447100>
- Onik, M. M. H., Aich, S., Yang, J., Kim, C.-S., & Kim, H.-C. (2019). Blockchain in Healthcare: Challenges and Solutions. In *Big Data Analytics for Intelligent Healthcare Management*. Elsevier Inc. <https://doi.org/10.1016/b978-0-12-818146-1.00008-8>
- Panda, S. K., Mishra, V., Dash, S. P., & Pani, A. K. (Eds.). (2023). *Recent Advances in Blockchain Technology*. 237. <https://doi.org/10.1007/978-3-031-22835-3>
- Patange, G. S., Sonara, Z., & Bhatt, H. (2021). Semantic Interoperability for Development of Future Health Care: A Systematic Review of Different Technologies. *Lecture Notes in Networks and Systems*, 176 LNNS, 571–580. https://doi.org/10.1007/978-981-33-4355-9_42
- Pawczuk, L., Massey, R., & Holdowsky, J. (2019). Deloitte’s 2019 Global Blockchain Survey - Blockchain gets down to business. *Deloitte Insights*, 2–48. https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf
- Persons, K. R., Nagels, J., Carr, C., Mendelson, D. S., Primo, H., “Rik,” Fischer, B., & Doyle, M. (2020). Interoperability and Considerations for Standards-Based Exchange of Medical Images: HIMSS-SIIM Collaborative White Paper. *Journal of Digital Imaging*, 33(1), 6–16. <https://doi.org/10.1007/s10278-019-00294-0>
- Pillai, B., Biswas, K., & Muthukkumarasamy, V. (2020). Cross-chain interoperability among blockchain-based systems using transactions. *Knowledge Engineering Review*, 35, 1–17. <https://doi.org/10.1017/S0269888920000314>
- Prasanna, K., Ramana, K., Dhiman, G., Kautish, S., & Chakravarthy, V. D. (2021). PoC Design: A Methodology for Proof-of-Concept (PoC) Development on Internet of Things Connected Dynamic Environments. *Security and Communication Networks*, 2021. <https://doi.org/10.1155/2021/7185827>

- Prince, O. (2021). Overview of Distributed Database System. *International Journal of Computer Techniques*, 8(1), 83–100. <http://www.ijctjournal.org>
- Qureshi, H. A. (2018). Theoretical Sampling in Qualitative Research: A Multi-Layered Nested Sampling Scheme. *International Journal of Contemporary Research and Review*, 9(08), 20218–20222. <https://doi.org/10.15520/IJCRR/2018/9/08/576>
- Radanović, I., & Likić, R. (2018). Opportunities for Use of Blockchain Technology in Medicine. *Applied Health Economics and Health Policy*, 16(5), 583–590. <https://doi.org/10.1007/s40258-018-0412-8>
- Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 78, 641–658. <https://doi.org/10.1016/j.future.2017.02.014>
- Renukappa, S., Mudiya, P., Suresh, S., Abdalla, W., & Subbarao, C. (2022). Evaluation of challenges for adoption of smart healthcare strategies. *Smart Health*, 26(April), 100330. <https://doi.org/10.1016/j.smhl.2022.100330>
- Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., Bukhari, W. A., & Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. In *PLoS ONE* (Vol. 17, Issue 4 April). <https://doi.org/10.1371/journal.pone.0266462>
- Saripalle, R. K. (2019). Fast health interoperability resources (FHIR): Current status in the healthcare system. *International Journal of E-Health and Medical Communications*, 10(1), 76–93. <https://doi.org/10.4018/IJEHMC.2019010105>
- Sater, S. (2018). Blockchain Transforming Healthcare Data Flows. *Ssrn*. <https://doi.org/10.2139/ssrn.3171005>
- Savage, M., & Savage, L. C. (2020). Doctors Routinely Share Health Data Electronically Under HIPAA, and Sharing With Patients and Patients' Third-Party Health Apps is Consistent: Interoperability and Privacy Analysis. *Journal of Medical Internet Research*, 22(9). <https://doi.org/10.2196/19818>
- Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, 181. <https://doi.org/10.1016/j.jnca.2021.103050>
- Schulz, S., Stegwee, R., & Chronaki, C. (2018). Standards in healthcare data. *Fundamentals of Clinical Data Science*, 19–36. https://doi.org/10.1007/978-3-319-99713-1_3
- Seaberg, R. W., Seaberg, T. R., & Seaberg, D. C. (2021). Use of Blockchain Technology for Electronic Prescriptions. *Blockchain in Healthcare Today*, 4. <https://doi.org/10.30953/bhty.v4.183>
- Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare (Switzerland)*, 8(2). <https://doi.org/10.3390/healthcare8020133>

- Shaik, S., & Subhani, S. (2018). A Review on Major Issues of Database Systems for Improving Throughput and Leading to Research Problems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* © 2018 IJSRCSEIT, 3(3), 712–716. <https://www.researchgate.net/publication/344228219>
- Siham, H., & Alyaseen, I. F. T. (2019). *Consensus Algorithms Blockchain: A comparative study*. *International Journal on Perceptive and cognitive Computing (IJPC)*.
- Singh, A., & Chatterjee, K. (2020). *Security and privacy issues of electronic healthcare system : A survey*. 2667. <https://doi.org/10.1080/02522667.2019.1703265>
- Singh, Y., Jabbar, M. A., Kumar Shandilya, S., Vovk, O., & Hnatiuk, Y. (2023). Exploring applications of blockchain in healthcare: road map and future directions. *Frontiers in Public Health*, 11, 1229386. <https://doi.org/10.3389/fpubh.2023.1229386>
- Soltani, R., Zaman, M., Joshi, R., & Sampalli, S. (2022). Distributed Ledger Technologies and Their Applications: A Review. *Applied Sciences* 2022, Vol. 12, Page 7898, 12(15), 7898. <https://doi.org/10.3390/AP12157898>
- Soule, D. (2020). *Healthcare Interoperability: Barriers and Solutions*. <https://www.healthcatalyst.com/insights/healthcare-interoperability-barriers-solutions>
- Sriman, B., Ganesh Kumar, S., & Shamili, P. (2021). Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake. *Advances in Intelligent Systems and Computing*, 1172(September), 395–406. https://doi.org/10.1007/978-981-15-5566-4_34
- STU, F. R. 3. (2018). *Overview - FHIR v3.0.1*. <https://www.hl7.org/fhir/overview.html>
- Suciu, G., Nadrag, C., Istrate, C., Vulpe, A., Ditu, M. C., & Subea, O. (2018). Comparative Analysis of Distributed Ledger Technologies. *6th Global Wireless Summit, GWS 2018*, 370–373. <https://doi.org/10.1109/GWS.2018.8686563>
- Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and Privacy in the Medical Internet of Things: A Review. In *Security and Communication Networks* (Vol. 2018). <https://doi.org/10.1155/2018/5978636>
- Syed Arif Isalm, & Dr.M.Mohan Kumar. (2022). *A Literature Review on Database Cyber Security: Attacks, Countermeasures and Techniques*. February. <https://www.researchgate.net/publication/358816366>
- Szarfman, A., Levine, J. G., Topping, J. M., Weichold, F., Bloom, J. C., Soreth, J. M., Geanacopoulos, M., Callahan, L., Spotnitz, M., Ryan, Q., Pease-Fye, M., Brownstein, J. S., Ed Hammond, W., Reich, C., & Altman, R. B. (2022). Recommendations for achieving interoperable and shareable medical data in the USA. *Communications Medicine*, 2(1), 1–7. <https://doi.org/10.1038/s43856-022-00148-x>
- Tabassum, A., & Lebda, W. (2019). *Security Framework for IoT Devices against Cyber-attacks*. 249–266. <https://doi.org/10.5121/csit.2019.91321>

- Thakur, A. (2022). A Comprehensive Study of the Trends and Analysis of Distributed Ledger Technology and Blockchain Technology in the Healthcare Industry. *Frontiers in Blockchain*, 5(March), 1–8. <https://doi.org/10.3389/fbloc.2022.844834>
- Thwaites, R. (2020). Research design and methodology. *Changing Names and Gendering Identity*, 32–42. <https://doi.org/10.4324/9781315571256-9>
- TMA. (2020). *ESA - Telemedicine Alliance*. https://www.esa.int/SPECIALS/Telemedicine_Alliance/index.html
- Tomić, N. Z. (2021). A Review of Consensus Protocols in Permissioned Blockchains. *Journal of Computer Science Research*, 3(2), 19–26. <https://doi.org/10.30564/jcsr.v3i2.2921>
- Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: a systematic literature review. *BMC Medical Informatics and Decision Making*, 23(1). <https://doi.org/10.1186/S12911-023-02115-5>
- Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*, 15, 1746–1761. <https://doi.org/10.1109/TIFS.2019.2948287>
- U.S. Department of Health & Human Services. (2023). *The Office of the National Coordinator for Health Information Technology*. 1–22. http://healthit.hhs.gov/portal/server.t/community/healthit_hhs_gov__home/1204
- Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. *IEEE Access*, 6, 32700–32726. <https://doi.org/10.1109/ACCESS.2018.2846779>
- Union, E., For, A., Deshpande, A., Stewart, K., Lepetit, L., Gunashekar, S., Galiano, S. S., Charalampidis, P., Fragkiadakis, A., Vujičić, S., Hasanspahić, N., Car, M., Čampara, L., Kannengießer, N., Pfister, M., Greulich, M., Lins, S., Sunyaev, A., Zander, M., ... Prins, T. J. (2020). Understanding the landscape of Distributed Ledger Technologies/Blockchain: Challenges, opportunities, and the prospects for standards. *Understanding the Landscape of Distributed Ledger Technologies/Blockchain: Challenges, Opportunities, and the Prospects for Standards*, 8(August), 1–17. <https://doi.org/10.7249/rr2223>
- Urkude, S. V., Sharma, H., Kumar, S. U., & Urkude, V. R. (2021). Anatomy of blockchain implementation in healthcare. In *Intelligent Systems Reference Library* (Vol. 203). https://doi.org/10.1007/978-3-030-69395-4_4
- Vujičić, D., Jagodić, D., & Randić, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. *2018 17th International Symposium on INFOTEH-JAHORINA, INFOTEH 2018 - Proceedings, 2018-Janua*(March), 1–6. <https://doi.org/10.1109/INFOTEH.2018.8345547>
- Wang, S., Li, H., Chen, J., Wang, J., & Deng, Y. (2022). DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. *Journal of Information Security and Applications*, 66. <https://doi.org/10.1016/j.jisa.2022.103134>

- World Health Organization [WHO]. (2020). *Digital Implementation Investment Guide (DIIG) Integrating Digital Interventions into Health Programmes*. Bulletin of the World Health Organization.
- World Health Organization [WHO]. (2021). *Advancing interoperability and data sharing in the health system country vignette 2 Background*. 1–3. <https://en.fhir-il-community.org/>
- Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. *IEEE Access*, 5. <https://doi.org/10.1109/ACCESS.2017.2730843>
- Xiong, Z., Zhang, Y., Luong, N. C., Niyato, D., Wang, P., & Guizani, N. (2020). The Best of Both Worlds: A General Architecture for Data Management in Blockchain-enabled Internet-of-Things. *IEEE Network*, 34(1), 166–173. <https://doi.org/10.1109/MNET.001.1900095>
- Yadav, R., Murria, S., & Sharma, A. (2020). A research review on semantic interoperability issues in electronic health record systems in medical healthcare. *IoT-Based Data Analytics for the Healthcare Industry: Techniques and Applications*, 123–138. <https://doi.org/10.1016/B978-0-12-821472-5.00009-0>
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. *National Institute of Standards and Technology*, October, 1–68. <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>
- Yang, Z., Jiang, K., Lou, M., Gong, Y., Zhang, L., Liu, J., Bao, X., Liu, D., & Yang, P. (2022). Defining health data elements under the HL7 development framework for metadata management. *Journal of Biomedical Semantics*, 13(1). <https://doi.org/10.1186/S13326-022-00265-5>
- Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, 19(Spring). <https://pmc/articles/PMC9123525/>
- Zhang, K., & Jacobsen, H.-A. (2018). Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, 1337–1346. <https://doi.org/10.1109/ICDCS.2018.00134>
- Zhang, P., & Boulos, K. M. N. (2022). Privacy-by-Design Environments for Large-Scale Health Research and Federated Learning from Data. *International Journal of Environmental Research and Public Health*, 19(19), 1–2. <https://doi.org/10.3390/ijerph191911876>
- Zhang, P., White, Z., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal*, 16, 267–278. <https://doi.org/10.1016/j.csbj.2018.07.004>
- Zheng, X., & Feng, W. (2021). Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain. *IOP Conference Series: Earth and Environmental Science*, 1802(3). <https://doi.org/10.1088/1742-6596/1802/3/032022>

- Zheng, X., Mukkamala, R. R., Vatrappu, R., & Ordieres-Mere, J. (2018, November 9). Blockchain-based personal health data sharing system using cloud storage. *2018 IEEE 20th International Conference on E-Health Networking, Applications and Services, Healthcom 2018*. <https://doi.org/10.1109/HealthCom.2018.8531125>
- Zhou, Z., Sun, C., Lu, J., & Lv, F. (2018). Research and implementation of mobile application security detection combining static and dynamic. *Proceedings - 10th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2018, 2018-Janua*, 243–247. <https://doi.org/10.1109/ICMTMA.2018.00065>

APPENDICES

Appendix I: Questionnaire

“I am a student undertaking Doctor of Philosophy in Information Technology Security and Audit of Kabarak University conducting research on **An Enhanced Secure Distributed Ledger Interoperability Framework for Medical Systems**. This is to request you to spare some few minutes and answer the following questions truthfully as you can to aid in the development of the stated framework. Please note that the information that you will provide will be used for academic purposes only.

Section A: General Questions

- *Please tick (✓) the most appropriate answer in the following questions*

1. Indicate the name of your company
2. Does your company design and develop medical systems only?
Yes [] No []
3. How many years have you been involved in the development of medical systems?
a. 1 to 5 years [] d. 6 to 10 years []
b. 11 to 15 years [] e. 16 to 20 years []
c. 21 to 25 years [] f. 26 years and Above []
4. On a scale of 1-5 (5 being the highest) rate your experience in designing and developing Medical Systems : Choose one:
a. 5 [] b. 4 [] c. 3 [] d. 2 [] e. 1 []
5. Which of the following roles describes best your position in the company?
a. System Analyst [] e. System Designers []
b. Programmer [] f. System Administrator []
c. System Support Staff [] g. Database Administrator []
d. Network Administrator [] h. Web Administrator []
6. Select the type of medical system developed by your company
a. Web-based Medical Systems [] d. Mobile Applications []
b. Enterprise Resource Systems (ERPs) [] e. Websites []
c. Standalone Medical System [] f. Distributed Ledger based Systems []

Section B: Medical Systems Security Questions

7. Is security of the medical system a requirement during the design and development phase?
Yes [] No []
8. Does your company adhere to healthcare design and development security standards and policies?
Yes [] No []
9. What type of security is incorporated in the medical system being designed by your company?
- a. Cryptography/ Encryption []
 - b. Authorization []
 - c. Authentication []
 - d. Automatic Backup []
10. Which levels of security(s) are incorporated in your medical systems; select all that apply
- a. Application Level Security []
 - b. Database Level Security []
 - c. Access Control Levels []
 - d. Data Exchange/ Sharing Security []
11. Are you aware of any medical system security design and development standard?
Yes [] No []
12. If Yes in question (11) above; Indicate any type of these Security Standard that you apply in your company
- a. General Standard like XML, TCP/IP, Web services, Security, Wireless, HL7 and IEEE []
 - b. Data Components like UMLs, WHO, HL7, ISO []
 - c. Data Interchange like HL7, ISO, DICOM, 1073, ASTM []
 - d. Knowledge representation (Guidelines and protocols, decision support algorithms) like HL7, ASTM []
 - e. Electronic Medical Record (EMR) like HL7, ASTM , OpenEHR, CEN []
 - f. Application Level Support like HIPAA, ISO, HL7, CEN, ASTM []
13. In your opinion are the medical systems security standards and policies applicable and necessary during the design and development phases
Yes [] No []
- If Yes in question (13) above; Why _____
- If No in question (13) above; Why Not _____

Section C: Interoperability Questions

14. Are you aware of what is interoperability of Medical Systems?
Yes [] No []
15. If Yes in number (14) above; select the interoperability level (s) achieved by the medical system being designed and developed by your company:
a. Foundational level [] c. Structural Level []
b. Semantic Level [] d. Organizational Level []
16. Do the medical systems developed by your company allow information sharing between two (2) or more healthcare information systems located in other healthcare organizations in a different geographical area?
a. Yes
b. No. If No, Why? _____
17. Does your company work with the interoperability service providers since interoperability is not part of the design and development requirement?
Yes [] No []
18. Indicate if the medical systems being designed have the architectural interoperability inbuilt capabilities
Yes [] No []
19. Does the medical system and the electronic health record product's level of interoperability align with the specific healthcare organizational needs?
Yes [] No []
20. From the factors listed below, which ones best informs you on the need of an interoperable medical system? Select from the factor identified below:
a. Ease of access []
b. Data portability []
c. Data confidentiality, integrity and security []
d. Capture of different data formats []
e. File sharing []
f. Cost reduction []
g. Scalability of systems []
21. On a scale of 1 – 5 (where 5 is the highest and 1 the least), how would you rate the level of standardization of the medical systems structural data formats, syntax and organization of data exchange?

- a. 5 – High structured []
 - b. 4 – Medium structured []
 - c. 3 – Average []
 - d. 2 – Low structured []
 - e. 1 – Very Low structured []
22. On a scale of 1 – 5 (where 5 is the highest and 1 the least), how would you rate the level of standardization of the medical systems semantic standards, codifications and protocols?
- a. 5 – High standardization []
 - b. 4 – Medium Standardization []
 - c. 3 – Average []
 - d. 2 – Low standardization []
 - e. 1 – Very Low standardization []
23. What are the architectures used in developing your medical systems? Select from the options below:
- a. Master-slave architecture []
 - b. Two-tier client–server architecture []
 - c. Multitier client–server architecture []
 - d. Distributed component architecture []
 - e. Peer-to-peer architecture []
24. What information would you allow to be shared across by your developed medical systems?
- a. Patient’s details []
 - b. Patient’s Diagnostic information []
 - c. Patient’s Prescription information []
 - d. Patients referral information []
 - e. Patient’s Financial information []
 - f. Other. Please state _____
25. Indicate what factor(s) hinder successful implementation of interoperability of medical systems _____
- _____
- _____

Appendix II: Interview Guide Questions

1. What type of medical systems do your company develop?
2. Why do you think the medical systems you are developing need to communicate with other medical systems from other software vendors?
3. What contents does your medical systems need to communicate with others?
4. What is the problem experienced when your medical system tries to communicate with others medical system and what solution have been made to solve the problem?
5. Are you satisfied with those solutions provided to solve the communication problem? If not, then what do you propose?
6. Do you prefer a solution in such a way that it doesn't affect your system but it only plays as a middle man between your request and the receiver system, and if yes, would you like to implement it?
7. Why do you think different hospitals don't use the same type of medical system?
8. How is your medical system designed to keep the patients' treatment record for further care prescription or treatment? State the tools used?
9. When a patient is discharged from one hospital and referred to another healthcare institution for care continuity, how does your system handle the prescription record to be exchanged? E.g. (use some portable medium to carry information to be exchanged or it takes place online).
10. According to the National Strategy of Health, to make systems interoperable, specific health standards need to be implemented, so do you know of any such standard that is implemented in your software development company?
11. How is the patients' medical data protected in your systems?
12. According to the National Strategy of Health, the focus is on National database for patient's Electronic Medical Records (EMRs). Would you prefer the centralized data sharing or Peer-to-Peer or distributed data sharing?
13. What architectural design factors are affecting interoperability of medical systems being designed by your company?
14. According to your own opinion would medical systems interoperability problem or challenges be solved by the medical software developers during the development process?
15. In your opinion should compliance with standards for data exchange, messaging, and security, form a part of medical system development requirements?

16. Are you aware of the existence of formal structures (working groups, steering committees, or units), processes, and procedures are in place to guide or enforce compliance with medical data exchange, messaging, and data security standards?
17. Are there interoperability guidance documents that are consistently used and referenced in efforts to guide implementation of medical interoperability to the medical software development vendors?
18. What would you suggest to be included in the medical systems to aid patients allow and trust their medical data/information sharing across different medical systems?
19. Indicate what factor(s) hinder successful implementation of interoperability of medical systems?
20. Would you embrace a medical system interoperability framework to guide the medical system development process?"

Appendix III: Validation Guide Questionnaire

“I am a student undertaking Doctor of Philosophy in Information Technology Security and Audit of Kabarak University conducting research on **An Enhanced Secure Distributed Ledger Interoperability Framework for Medical Systems**. This is to request you to spare some few minutes and answer the following questions truthfully as you can to aid in the evaluation and validation of the development Medical DLT system prototype. Please note that the information that you will provide will be used for academic purposes only.

- *Please tick (✓) the most appropriate answer in the following questions*

Medical DLT System Prototype Validation Metrics (Parameters)

A. Usability:

1. Do you find the user interface design of the Medical DLT system prototype intuitive and easy to navigate?
Yes [] No []
2. On a scale of 1 to 5, how would you rate the simplicity and ease of use of the developed Medical DLT system prototype for managing medical data? (1 being Poor and 5 being Excellent)
 - a. 5 – Excellent []
 - b. 4 – Simple and easy to use []
 - c. 3 – Fair []
 - d. 2 – Not simple and not easy to use []
 - e. 1 – Poor []
3. Please provide any suggestions or feedback on how the usability of the Medical DLT System Prototype can be improved

B. Security and Privacy:

4. Do you believe that the Medical DLT system prototype adequately addresses security and privacy concerns related to the handling of patient electronic medical records (EMRs) and information? Yes [] No []

5. How confident are you in the security measures implemented within the Medical DLT system prototype to protect sensitive patients medical data?
- a. 3 – High []
 - b. 2 – Medium []
 - c. 1 – Low []

6. Are there any specific security or privacy vulnerabilities that you have identified within the Medical DLT system prototype?

Yes [] No []

If yes, please elaborate:

.....

.....

C. Access Control:

7. Does the Medical DLT system prototype provide adequate mechanisms for controlling user access to patient electronic medical records?

Yes [] No []

8. On a scale of 1 to 5, how satisfied are you with the granularity and flexibility of the access control mechanisms implemented within the Medical DLT system prototype?

(1 being very dissatisfied and 5 being very satisfied)

- a. 5 – Very satisfied []
- b. 4 – Satisfied []
- c. 3 – Moderate []
- d. 2 – Dissatisfied []
- e. 1 – Very dissatisfied []

9. Are there any improvements or enhancements you would suggest for the access control features of the Medical DLT system prototype?

.....

.....

D. Authentication and Authorization:

10. Are you satisfied with the authentication and authorization mechanisms used to verify user identities within the Medical DLT system prototype?

Yes [] No []

11. On a scale of 1 to 5, how would you rate the Medical DLT system prototype authentication and authorization mechanisms in terms of defining and enforcing access privileges for different user roles? (1 being very poor and 5 being excellent)
- a. 5 – Excellent []
 - b. 4 – Good []
 - c. 3 – Fair []
 - d. 2 – Poor []
 - e. 1 – Very Poor []
12. Are there any other authentication or authorization-related mechanisms that you would recommend to be included in the Medical DLT system prototype? If Yes, Provide your feedback.

E. Interoperability:

13. Have you tested the interoperability of the Medical DLT system prototype with other existing medical systems?
 Yes [] No []
14. On a scale of 1 to 5, how would you rate the Medical DLT system prototype ability to seamlessly exchange medical data with different medical systems and platforms? (1 being very poor and 5 being excellent)
- a. 5 – Excellent []
 - b. 4 – Good []
 - c. 3 – Fair []
 - d. 2 – Poor []
 - e. 1 – Very Poor []
15. Are there any interoperability challenges or compatibility issues that you have encountered while using the Medical DLT system prototype? If yes, provide your feedback.....

F. Adherence to Healthcare Standards:

16. Does the Medical DLT system prototype comply with established healthcare interoperability standards such as HL7, FHIR, and DICOM?
 Yes [] No []

17. How important do you think adherence to healthcare standards is for the success and adoption of the Medical DLT system prototype?

- a. 3 – High []
- b. 2 – Medium []
- c. 1 – Low []

18. Have you encountered any instances where the Medical DLT system prototype deviates from healthcare standards or best practices? If yes, please provide details:

.....
.....
.....

19. Is there any other feedback or suggestions you would like to provide regarding the usability, security and privacy, access control, authentication and authorization, interoperability and adherence to healthcare standards, aspects of the Medical DLT system prototype?

.....
.....

Appendix IV: KUREC Clearance Letter



KABARAK UNIVERSITY RESEARCH ETHICS COMMITTEE

Private Bag - 20157
KABARAK, KENYA
Email: kurec@kabarak.ac.ke

Tel: 254-51-343234/5
Fax: 254-051-343529
www.kabarak.ac.ke

OUR REF: KABU01/KUREC/001/07/06/23

Date: 13th June, 2023

Dorothy Gatwiri Bundi,
Reg. No: GDS/M/0270/01/19
Kabarak University,

Dear Dorothy,

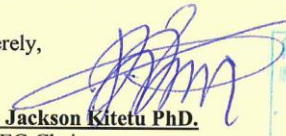
RE: AN ENHANCED SECURE DISTRIBUTED LEDGER INTEROPERABILITY FRAMEWORK FOR MEDICAL SYSTEMS

This is to inform you that **KUREC** has reviewed and approved your above research proposal. Your application approval number is **KUREC-070623**. The approval period is **13/06/2023 – 13/06/2024**.

This approval is subject to compliance with the following requirements:

- i. All researchers shall obtain an introduction letter to NACOSTI from the relevant head of institutions (Institute of postgraduate, School dean or Directorate of research)
- ii. The researcher shall further obtain a RESEARCH PERMIT from NACOSTI before commencement of data collection & submit a copy of the permit to **KUREC**.
- iii. Only approved documents including (informed consents, study instruments, MTA Material Transfer Agreement) will be used
- iv. All changes including (amendments, deviations, and violations) are submitted for review and approval by **KUREC**;
- v. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to **KUREC** within 72 hours of notification;
- vi. Any changes, anticipated or otherwise that may increase the risk(s) or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to **KUREC** within 72 hours;
- vii. Clearance for export of biological specimens must be obtained from relevant institutions and submit a copy of the permit to KUREC;
- viii. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal and;
- ix. Submission of an executive summary report within 90 days upon completion of the study to **KUREC**

Sincerely,


Prof. Jackson Kitetu PhD.
KUREC-Chairman








Cc Vice Chancellor
DVC-Academic & Research
Registrar-Academic & Research
Director-Research Innovation & Outreach
Institute of Post Graduate Studies

As members of Kabarak University family, we purpose at all times and in all places, to set apart in one's heart, Jesus as Lord.
(1 Peter 3:15)

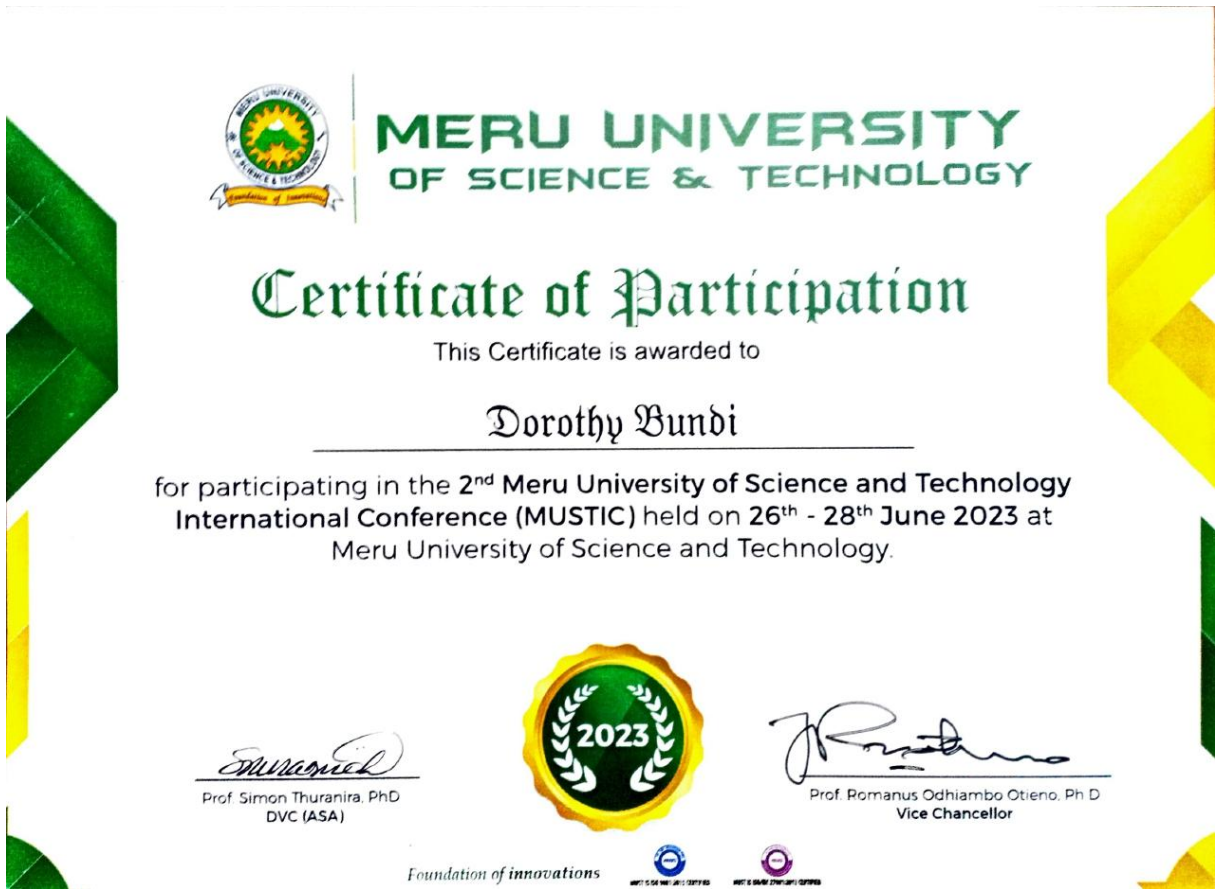


Kabarak University is ISO 9001:2015 Certified

Appendix V: NACOSTI Research Permit

 REPUBLIC OF KENYA	 NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION
Ref No: 207057	Date of Issue: 22/June/2023
RESEARCH LICENSE	
	
<p>This is to Certify that Ms. DOROTHY Gatwiri Bundi of Kabarak University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Meru, Nairobi, Nakuru on the topic: AN ENHANCED SECURE DISTRIBUTED LEDGER INTEROPERABILITY FRAMEWORK FOR MEDICAL SYSTEMS for the period ending : 22/June/2024.</p>	
License No: NACOSTI/P/23/27321	
207057	
Applicant Identification Number	Director General NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION
	Verification QR Code
	
<p>NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.</p>	
See overleaf for conditions	

Appendix VI: Evidence of Conference Participation



Appendix VII: List of Publications



A review of distributed ledger technologies application in medical systems interoperability

Dorothy G. Bundi^{1,2*}, Stephen M. Mutua¹ and Simon M. Karume²

¹Meru University of Science and Technology, Meru, Kenya. ²Kabarak University, Kenya.

ARTICLE INFO

ABSTRACT

KEYWORDS

Distributed ledger technologies

Data interchange, standards

DLT integration

Medical systems interoperability

Semantic interoperability

Structural interoperability

This study of the literature delves into the complex area of medical systems interoperability, focusing on mitigating variables that impact security and data transfer at the structural and semantic levels. In the era of digital healthcare, the secure sharing of medical data is crucial, and this study looks at how Distributed Ledger Technologies (DLTs) can play a major role in addressing these challenges. Complex interoperability issues that come from differences in communication protocols, data formats, established data structures, data models, and data meaning and codification methodologies face the healthcare industry. These problems typically impede the seamless transmission of electronic medical records between healthcare systems. Because of their decentralized structure and cryptographic foundation, DLTs offer a workable solution to these issues. By

critically evaluating previous research and case studies, DLTs may be able to lessen these interoperability issues, as this literature review illustrates. Since DLTs provide an immutable and secure platform for the transmission of medical data, guaranteeing data integrity and confidentiality, they are a natural fit for the sensitive nature of healthcare data. Their importance in creating safe communication protocols, enhancing the meaning of data, and defining models and formats for data is emphasized in this review. A comprehensive architecture for DLT interoperability in healthcare is also recommended by the research. This framework encourages the development of DLT integration, shared data models, standardized data formats, and governance and policy. By implementing this strategy and strengthening secure medical data sharing, healthcare organizations and governments may increase the efficiency, precision, and speed of healthcare delivery. The crucial role that DLTs play in removing the structural and semantic barriers to safe medical systems interoperability is highlighted in the conclusion of this literature review. By adopting DLTs, the healthcare sector may usher in a new era of standardized, safe, and efficient medical data transmission, which will ultimately benefit both patients and healthcare providers. This study shows how distributed ledger technologies (DLTs) have the potential to revolutionize the healthcare industry by enabling the secure and meaningful exchange of medical data between different systems, thereby improving patient care and healthcare outcomes.

Introduction

In the very private and significant healthcare sector, data security, privacy, and interoperability are essential (Kotey et al., 2023). Since secure

medical systems are crucial to maintaining the security and integrity of patient data, their significance cannot be overstated. They are also required to enable efficient data transmission be-

Corresponding author: Dorothy G. Bundi Email: dbundi@must.ac.ke

<https://10.58506/ajstss.v2i2.203>

AFRICAN JOURNAL OF SCIENCE, TECHNOLOGY AND SOCIAL SCIENCES ISSN :2958-0560

<https://journals.must.ac.ke> © 2023 The Authors. Published by Meru University of Science and Technology

This is article is published on an open access license as under the CC BY SA 4.0 license

Underlying Consensus Algorithms, Architectures and Data Structures in Distributed Ledger Technologies Applications

DOROTHY G. BUNDI¹, STEPHEN M. MUTUA², SIMON M. KARUME³

¹ School of Science Engineering and Technology, Kabarak University, Kenya

² School of Computing and Informatics, Meru University of Science and Technology, Kenya

³ School of Science Engineering and Technology, Kabarak University, Kenya

Abstract— *Distribute Ledger Technologies (DLTs) provide a distributed and decentralized environment with no central trusted control authority. DLTs removes a single point of authorization hence increasing the levels of trust of distributed records however there are still challenges in the underlying consensus algorithms, architectures and data structures in DLTs applications that need to be addressed. This paper employs exploratory research design with an objective to review various literature on different consensus algorithms, architectures and data structures applied in DLTs applications. The study revealed proof-of-work and proof-of-stake as some of the common consensus algorithms used in DLTs. The review shows that DLTs use either linear or linked, complex and hybrid data structures. Blockchain, Directed Acyclic Graph, Hashgraph, Holochain and Tempo (Radix) as the common types of DLTs. The findings also indicated that DLTs architectural design is constructed of three layers Protocol, Network, and Data. This study contributes to body of knowledge in DLTs.*

Indexed Terms: *Distributed Ledger Technologies (DLT), Consensus Algorithm, Architectural Layers, Data Structures*

I. INTRODUCTION

Distributed ledger technology (DLT) in the recent times has emerged as a disruptive technology with a wide range of applicability in different sectors [1]. DLT is a network platform with a distributed database in which data and transactions are recorded, stored in a shared ledger that is distributed across various computer nodes termed as the network nodes,

institutions, countries and accessible simultaneously by multiple people spread out in the globe [2]. DLT offers an alternative to centralized storage techniques to databases, which rely on a single server or small network. DLTs have unique features that make them suitable for application in different sectors. The unique DLTs features are decentralization, immutability, distributed, shared ledgers, fault tolerance, transparency, efficiency and use smart contracts [3]. Additionally, DLTs also offer transactions that are secure, encrypted, time-stamped, anonymous, and verifiable records for every transaction without a central repository and usually without a central authority [4], [5].

The development of distributed ledger technology (DLT) has brought about significant changes in record-keeping by moving from a single, authoritative location to a decentralized system. However, there are still challenges in the underlying data structures, architectures, topologies, and consensus mechanisms in DLTs that need to be addressed. This paper aims to explore the algorithms, architectures, and data structures used in DLTs and identify the research issues that need to be addressed to improve the efficiency, scalability, and security of DLTs.

DLTs are made up of three common components the peer to peer network which is created when two or more computers in the network establishes a connection to aid in communication and sharing of information without going through a central server [3],[6]. This component helps in improving the security of the client-server network which store data only on the server side. The Nodes which are the independent computers that record, share and