

Investigate the Security Challenges in SaaS Private Cloud using OwnCloud

Satwinder S. Rupra

School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: satwinder@sumocomputers.net

Received: July 14, 2018

Published: July 28, 2018

Abstract

Cloud storage is becoming a fast emerging resource used for storage of information by corporates and organizations as a substitute to get data available anywhere and anytime. Cloud entities such as cloud service providers, users and business associates share the offered resources at diverse levels of technological operations. The cloud computing model is considered to be a very capable and able internet-based computing platform, which offers numerous benefits like mobility, flexibility, reliability and cost-effectiveness. However, like any other technology, cloud computing is not without a challenge or as problem free as it may seem. This paper intended to investigate the security challenges in private SaaS clouds and this was done with the aid of OwnCloud, which is an open-source cloud storage platform. Users were given access to the experimental cloud to collect details on the threats and vulnerabilities associated with the cloud. The challenges identified were specific to small businesses and SMEs. The research yielded numerous challenges including insider threats, improper data deletion, bandwidth issues, hacking, repudiation issues and government laws. Further to this, strategies and countermeasures to mitigate these challenges were suggested so that small organizations can understand their cloud security better as well as implement security in an effective manner.

Keywords: Cloud computing, SaaS, SME, Security challenges.

© 2016 by the author(s); Mara Research Journals (Nairobi, Kenya)

OPEN ACCESS

1. INTRODUCTION

Cloud storage is a means of data storage whereby the data is stored and accessed over the network, mostly through the internet. The data is stored on multiple servers (and often locations), and the environment is controlled and managed by a hosting company called cloud storage providers. It is a kind of outsourcing of computer programs, where users are able to access software and applications from wherever they are. The providers always keep the data available and accessible wherever and whenever the owner or users require access to it [1]. Put differently, cloud computing is the provisioning of IT resources including hardware, software, or services from third parties over a network, usually the internet. It is the delivery of scalable of IT resources over the Internet, as opposed to hosting and operating those resources locally on the LAN or private network [2]. Researches [3] assert that cloud computing is a web-service that comprises provision of storage capacity and virtualized computing resources. The virtual computing resource (email, software, data storage) are managed through remote servers by cloud providers. The cloud provides manage the cloud platform to offer Software as a service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) and the end users, access these services through normal browsers on computing devices such as; PC, iPad and smart phones, among others. Therefore, end users do not have to manage or scale the IT infrastructure resources and instead focus on their core businesses. This leads to reduced running/capital costs, increased productivity, mobility, collaboration and profitability of businesses [4, 5]. It is a model that enables on-demand access to shared configurable computing resources, which can then be configured for

usage by an organization. These resources include applications and services, or the infrastructure on which the services operate. By deploying IT infrastructure through the cloud, an organization can purchase additional resources on an as-required basis and avoid the initial costs of software and hardware (e.g., networks, servers, storage, application software) [6].

A research study called Cloud in Africa: Reality Check 2013 conducted in Kenya indicated that as of 2013, 25% of the organizations opting for cloud are using private cloud compared to 13% opting for hybrid cloud and only 7% of companies opting for the public cloud. The most popular category for cloud use was storage at 28% of companies, followed by SaaS at 10% of companies [7].

By effectively implementing cloud services, numerous opportunities are available to SMEs that allow them to increase their competitive edge in business [9]. SMEs can offer their clients a number of services including business services, application software services, infrastructure services, and integration and development services [8].

1.1 Problem Statement

Despite the benefits of cloud computing being well known to SMEs in Kenya, a majority are not fully aware of the key IT related risks and the mitigation strategies. For example, a breach in the security of any component in the cloud can be a disaster for any organization (the customer); data can be compromised leading to heavy losses or loss of confidential information, and of course not to mention, reputation.

In a cloud computing infrastructure, the resources and/or the client data is usually stored at a different premise that the customer is unaware of. The customer accesses the resources and data remotely through the internet. Therefore, it is of utmost important for SMEs to understand the risks they are likely to face once they step into the world of SaaS cloud computing. Other concerns that may be of important value include; what happens to the data and its copies once the cloud service is discontinued and what happens in case you want to transfer data from one cloud platform to another. These areas of cloud computing are prone to security breaches, and hence, this makes the research of cloud computing security an important and current subject.

Corporate companies and governmental organizations usually have the power and money to afford to hire trained security consultants; however unlike them, SMEs lack the necessary resources and expertise to be able to scrutinize the working environment of cloud computing.

There are six crucial areas in the cloud that require protection to be able to suffice against the threats [10]. These six areas are as follows:

1. *Security of data at rest* – This ensures that data should be secure when it is stored in the cloud server(s). This is usually achieved by providing encryption for all data stored.
2. *Security of data in transit* – Means that data should be secure when being transferred from the cloud to the user computers and vice versa. This can be achieved by providing TLS/SSL security.
3. *Authentication of users* – Users who have access to data should pass some sort of access control to be able to keep off unwanted users. These include strong passwords and biometrics among others, that is, one factor to three actor authentication depending on the mission critical of the data.
4. *Robust isolation between data belonging to different customers* – Although not applicable to private clouds, however, for public clouds each customers data is isolated using different VMs.

5. *Cloud legal/regulatory issues* – All customers should usually have their legal and regulatory experts inspect cloud provider policies and practices, especially for things like data retention, deletion, corruption, and security.
6. *Incident response* – Customers should understand how incidents and disasters will affect their data and should, therefore, implement relevant recovery and business continuity procedures for the same.

2. LITERATURE REVIEW

Cloud computing is believed to have been introduced as early as 1969 by J.C.R. Licklider, who was in charge of the development of Advanced Research Projects Agency Network (ARPANET). His vision was to create a platform for accessing data and programs from anywhere and at any site. This vision is quite similar to the modern cloud computing. Since those days, cloud computing and storage has evolved a long way [6]. However, since in the early years the internet was not able to offer bandwidth capacities like today, cloud computing for the masses has been adopted and widely used much later. [11]

For a paradigm to be classified as a cloud computing, it usually possesses the following characteristics as indicated by [12]:

- *Elasticity*: Cloud users can at their convenience downsize/upscale computing resources, as and when need arises, without human interaction. This means that to add or reduce resources on the cloud, one will not need to buy additional hardware, users can do this by the use of controlled software.
- *Access on multiple devices*: Users of the cloud are not limited to the number or type of devices they use. Mostly, if devices can access internet and have the relevant cloud applications, a user can connect to the cloud from any device.
- *Accessible anywhere*: Cloud customers may be able to access their data and service irrespective of the geographical location. Therefore, the cloud user has no control or whereabouts of the location of the assets. Similarly, the cloud vendor does not have restrictions over the location of its users [13].
- *Reliability*: Clouds data are usually backed up on multiple redundant sites sometimes even offshore, therefore, all data saved on the cloud has disaster recovery catered for.
- *Economies of scale and cost effectiveness*. Cloud implementations, regardless of the deployment model, tend to be, as large as possible, in order to take advantage of economies of scale. Therefore, cloud vendors can be located in areas where electricity and real estate prices are lower eventually lowering their start-up and running costs.

2.1 Benefits of Cloud Computing

The shift from grid computing to cloud computing is getting more evident by the day. Cloud computing offers numerous benefits, which could not be attained in the native computing infrastructure [14]. The advantages of cloud computing paradigm include the following:

1. *Mobility*: The primary benefit of cloud computing by far would be the ability to access data from anywhere at any time. Once cloud users have registered themselves to a cloud vendor, all that is needed is an internet connection to be able to access their information and services. This feature lets users move beyond time zone and geographical boundary issues.
2. *Flexibility*: Users only have to pay for services and capacity which they are really using. So if they need less they pay less and if they need more, they can simply acquire additional storage and services, which of course leads to higher costs, but it is still much more flexible than adding

another server to the company internal IT resources. The addition or removal of processing units or storage space does only take seconds to minutes and not days like it would in a company internal data center using physical servers.

3. *Reliability*: Cloud computing also adds to reliability of data in case the user loses their device. If a laptop or mobile phone is stolen, the user's data cannot be lost since it is stored in the cloud; the user can simply buy another device and connect it to the internet to access their data.
4. *Reduction of cost*: Many cloud services are provided for free and offer enough functionality for most of the users. Therefore, users can save much money by using cloud services.
5. *Cost-effective*: Allow IT people to concentrate on other areas by taking the load of data storage, application control and update from off their work.

2.2 Challenges in the Cloud

Cloud computing is not a standalone computing platform, it instead combines several technologies including networks, operating systems (OS), databases, virtual servers and components, resource scheduling, transaction processing, concurrency control techniques, load balancing, memory management and numerous others for its functionality and operation [15]. Therefore a threat in any one of the technologies becomes a threat for the entire cloud platform. Most security problems stem from loss of control, lack of trust or multi-tenancy. These problems are described below in more detail:

2.2.1 Loss of control

Since most cloud platforms are hosted off-site, an organization cannot have full control over the hardware, technology and backend details of the cloud platform. Moreover, when an organization outsources their data and services to a cloud vendor, they are not aware and have no control over the location of their data. This possesses serious concerns from a user perspective; organizations lose control over their vital data and are not aware of any security mechanisms put in place by the provider (Behl, 2011). According to Tech Target, having data in an unknown place and with no control over it, is one of the leading concerns to organizations, when switching to cloud computing.

According to Pearson & Benameur (2010, November), user-centric control does not seem like a possibility with the cloud: as soon as a SaaS cloud infrastructure is used, the cloud vendor becomes responsible for storage of data, while the users' loses visibility and control over it. In the cloud paradigm, users' data is processed in 'the cloud' on hardware, software and platform they do not own or control, and therefore, becomes a threat in terms of theft, misuse (especially for different purposes from those originally notified to and agreed with the consumer) or unauthorized resale. Additionally, it is not clear that it will be possible for a cloud provider to ensure that a data owner can get access to all their data including metadata and system related files. It can also be difficult to get data back from the cloud, and avoid vendor lock-in. Furthermore, there is no sure way of telling that documents or personal data on the cloud has been successfully deleted if the user wants to. Some vendors may also deliberately tie down a customer to proprietary software or hardware so that it becomes difficult to switch providers.

As an example, consider a company X in Nairobi that is using a cloud provider Y who stores their data in India and Australia. X's data is stored on Y's cloud, and therefore, is transmitted between various hardware and software devices located in the three locations. These additional links, require X to entrust its data to different systems and platforms located in different locations, managed by unknown users, and regulated by the laws of other countries (India and Australia). In such a scenario, X does not know whether the security profiles of the remote locations are the same as what they have in-house or whether the regulatory compliances like HIPAA hold in all the locations. X will realize that as soon as the data leaves their

perimeter in Nairobi, it does not have much control over it or what processes it goes through. X does not know who can access its data that is now stored on various disks in multiple locations (India and Australia). This lack of control over the data and processes by X triggers the risk of losing data confidentiality, integrity, and availability [16].

Cloud computing essentially requires a customer to hand over any control of running their applications and storing their data to their providers. They retain only partial control of their data, which is a cause of concern for them.

2.2.2 Lack of Trust

Trust can be defined as an act of faith; confidence and reliance in something that one expects to behave as stated. It is a confidence in the ability and expertise of others, such that one feels they can rely on an entity to care for your valuable assets. Trust in a system is reduced when we have little or insufficient information about its expertise [16].

Trust also has a variation depending on the data ownership. For example, if a company store and execute their data on the cloud, it creates two folds of a trust relationship [17]. Primarily, the company must trust their cloud provider and secondly, the company must make sure that its clients also trust the same provider. A provider and customer often enter into a contractual relationship to establish trust. Typically, a company may be compensated in an event that the service is not delivered as expected and in the case of cloud providers service-level agreements (SLAs) can be used to boost trust. However, in the modern computing world, establishing trust in cloud computing is related to preventing a trust violation rather than to compensate a violation in case it occurs. For any modern organization, a security breach irreparable and money or compensation cannot bring back lost data or the organization's reputation. Therefore, cloud computing trust model should focus more on preventing security breaches as opposed to post-failure compensation [18]. Another vital constituent of cloud trust is reputation, which is arguably a provider's most valuable quality.

A consumer's insight mostly is that cloud computing is not as secure as internal paradigms; however, improved transparency can counter this. Data stored in cloud devices is stored and processed across the entire virtual layer. Two issues arise from this in relation to trust: firstly the physical storage and processing sites are unknown to the data owner, and secondly the security implementations in these sites. A company should know where its data is processed and stored, because laws in different countries may not be favorable to the company in case of breaches. A company also needs to know how its data is protected while being moved within the system or across multiple sites owned by the cloud providers [17]. If there is no transparency between the provider and the customer, a company will not know if their security requirements are in line with the cloud provider's security assurances.

Ultimately, usage of the cloud is a question of trade-offs between security, privacy, compliance, costs and benefits [19]. Trust is a vital component to the adoption of cloud computing and therefore trust needs to be included right along the chain of service provision.

2.2.3 Multi-tenancy issues

Multi-tenancy refers to the cloud characteristic of resource sharing. Several resources are shared including memory, programs, networks and data. Cloud computing heavily relies on an operational model where resources are shared. This means that more than one user to use the same resource at different levels including the network, host and application. Although users are isolated at a virtual level, hardware is not separated, thus an attacker can legitimately be in the same physical machine as the target. With a

multitenant architecture, a software application is designed to virtually partition its data and configuration so that each client organization works with a customized virtual application instance. Multi-tenancy, is relative to multitasking in operating systems.

Multi-tenancy in cloud computing is unique such that both the attacker and the victim are sharing the same physical hardware like servers. A setup like this cannot be countered by native security measures and controls. This is because they are not designed to secure inside the servers and they are limited just to the network layer [19].

According to [20] by spending a little money to buy cloud space, an attacker has a 40% chance to allocate his VM next to the victim's VM. After such a multi-tenancy has been achieved, any attack takes advantage of the system characteristics can be launched to hack breach the victim's data. The risk from for such an attack (like side channel attacks) is high because they cannot be detected by the hypervisor or the operating system.

2.2.4 Downtime

This is a major disadvantage of cloud computing especially in evolving countries. Many parts of Kenya still face challenges with stable and affordable internet connections. Because all the data, resources and applications are only accessible through the internet, an internet outage means users have no access to them. Downtime may be reduced by having multiple ISP connections in an organization; however that also means an increase in cost.

2.2.5 Privacy Challenge

Privacy risks always exist on data and information stored online. Like all data stored online, data on the cloud is prone to accidental leakage or compromise.

2.2.6 Other Security Challenges

Since cloud is a collection of different technologies and fields, security issues for each of these technologies becomes a threat to the cloud too. For example, networks and databases have their security threats like man in the middle attack or SQL injection attacks, which become threats to data in the cloud too. Threats and flaws in other technologies like operating systems, virtual platforms, transaction processing systems, concurrency control procedures and the likes also form part of the cloud security issues. It is therefore also of utmost importance that each of these cloud technologies be secure enough to provide for overall security of the system. For example, the network between the end users and the cloud infrastructure needs to be secure. Data at rest also needs to be secure by encrypting the data and enforcing relevant policies for data sharing. Additionally, resource distribution and memory management systems need to be secured. Lastly, techniques for malware detection also need to be implemented in the clouds – an approach which is usually adopted in intrusion detection systems (IDSs) [21].

3. FINDINGS AND RESULTS

This paper sought to investigate how data stored on the cloud reacts during different file operations as well as determine the threats posed in cloud from the provider's end. This was experimented by use of OwnCloud version 10.0.4

OwnCloud was installed on a domain that the researcher registered and hosted online. Accounts were then created on the software that were given to different users to save their dummy data in using both the OwnCloud client software version 2.4.0 as well as the web browser.

3.1 The Challenge of Insider Threat

This is the worst-case scenario for when a malicious system administrator works for the cloud provider. Because of their business role in the cloud provider, the insider can use her authorized user rights to access sensitive data. Depending on the insider's motives, the result of such an attack in a cloud infrastructure will vary from data leakage to severe corruption of the affected systems and data. It is noted using OwnCloud that as much as the administrator does not have access to user passwords, they have the ability to change the password for any user at any given time.

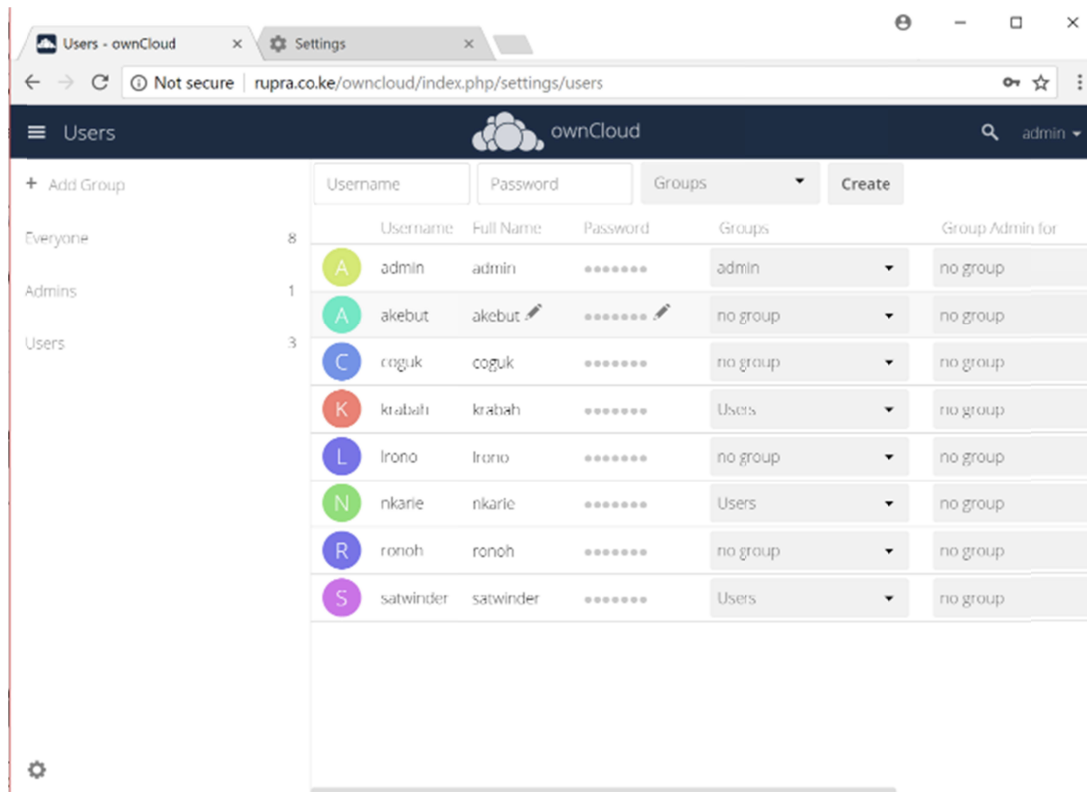


Fig. 1: Users List and Password change

3.2 Challenge of Deleted Data

Dummy files were saved on the cloud using the desktop utility shown below. These files were deleted from the desktop utility moments later. They certainly cease to exist on the local computer after deletion. However, these files still remained in the cloud for an additional 180 days. Once the password for any user is changed, the insider can easily log in to the account of the user and therefore gain access to their data and causing confidentiality, integrity and availability compromise.

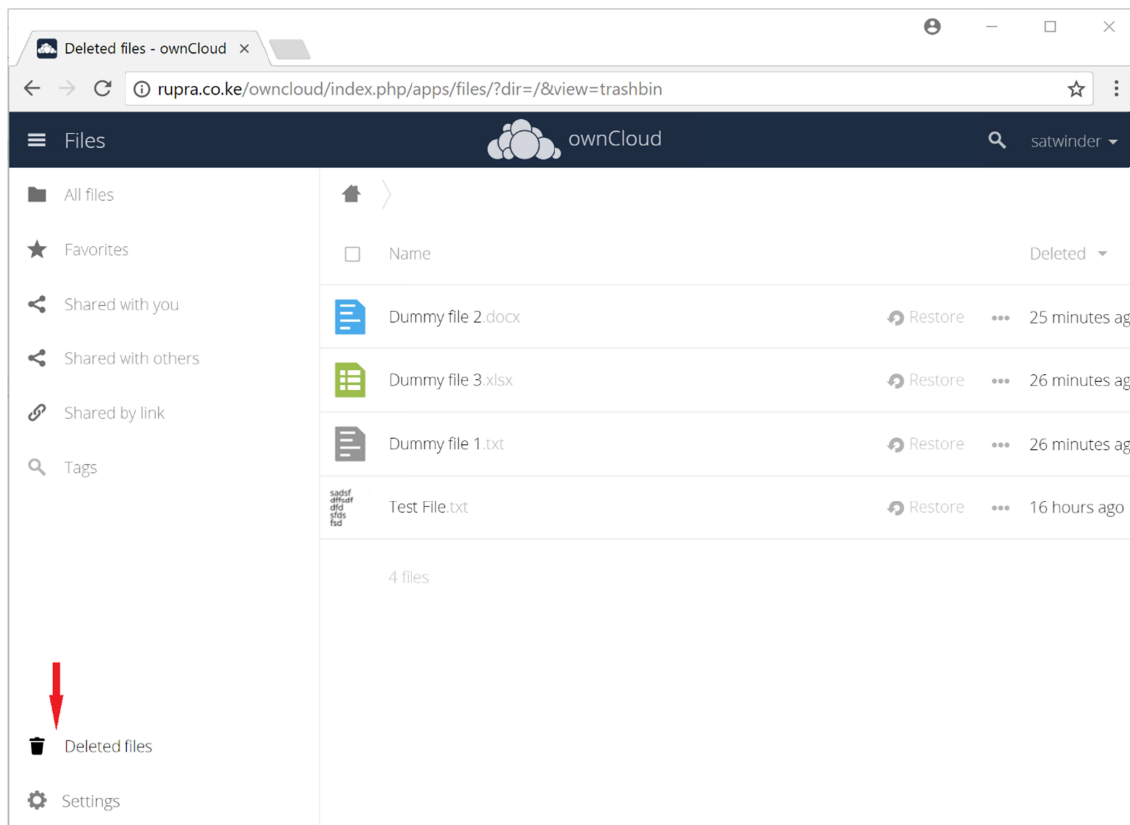


Fig. 2: Deleted Documents in the Cloud

These files are not permanently deleted until you manually delete them, or when your cloud storage is full and the files are automatically deleted to make room for new ones. The deleted files do not show in the desktop of the client anymore nor do they show in the web directories, however, they do stay in the deleted files. Similarly, Dropbox, One Drive and Google will keep versions of deleted files for up to 30 days as stated in their documentation.

3.3 Challenge of Bandwidth and Availability

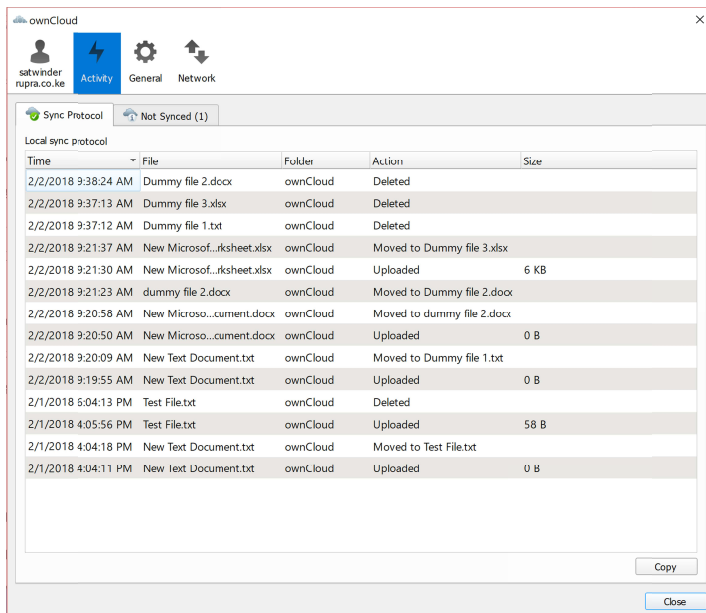
Uploading data on the cloud requires a stable type of internet connection. One GB of data is uploaded through the client utility took approximately 7 hours with a 2Mbps shared Safaricom connection. Other normal operations were also taking place using the same internet. This may not be a problem for uploading a few files, however, if a firm is planning to shift their entire or partial infrastructure on the cloud, then a reliable and stable internet connection is mandatory.

A 10mbps speed would be optimum as well as a failover link in case the primary one is down. Otherwise an SLA agreement of a 99.5% or above by the ISP is required, which translates to about 1.8 days in a year of down-time. Likewise a similar SLA with the cloud provider is mandatory although during the experiment, there was no downtime noted over a period of three months showing stability on the cloud provider's side. Also attacks on identity services or network connectivity, such as DDoS attacks can jeopardize the availability or degrade the performance of the service.

3.4 Challenge of Repudiation

It is always challenging to ensure true non-repudiation and shifting the data to cloud may make this even more difficult due to login from multiple systems (smartphone, desktop/laptop) or access from devices

which do not have a static IP. OwnCloud shows a number of activities that are carried out on the cloud as shown in Fig. 3.



Time	File	Folder	Action	Size
2/2/2018 9:38:24 AM	Dummy file 2.docx	ownCloud	Deleted	
2/2/2018 9:37:13 AM	Dummy file 3.xlsx	ownCloud	Deleted	
2/2/2018 9:37:12 AM	Dummy file 1.txt	ownCloud	Deleted	
2/2/2018 9:21:37 AM	New Microsoft...ksheet.xlsx	ownCloud	Moved to Dummy file 3.xlsx	
2/2/2018 9:21:30 AM	New Microsof...ksheet.xlsx	ownCloud	Uploaded	6 KB
2/2/2018 9:21:23 AM	dummy file 2.docx	ownCloud	Moved to Dummy file 2.docx	
2/2/2018 9:20:58 AM	New Microso...ument.docx	ownCloud	Moved to dummy file 2.docx	
2/2/2018 9:20:50 AM	New Microso...ument.docx	ownCloud	Uploaded	0 B
2/2/2018 9:20:09 AM	New Text Document.txt	ownCloud	Moved to Dummy file 1.txt	
2/2/2018 9:19:55 AM	New Text Document.txt	ownCloud	Uploaded	0 B
2/1/2018 5:04:13 PM	Test File.txt	ownCloud	Deleted	
2/1/2018 4:05:56 PM	Test File.txt	ownCloud	Uploaded	58 B
2/1/2018 4:04:18 PM	New Text Document.txt	ownCloud	Moved to Test File.txt	
2/1/2018 4:04:11 PM	New text Document.txt	ownCloud	Uploaded	0 B

Fig. 3: Cloud Activities Log

This may still pose a challenge of non-repudiation because when a dynamic IP is used to connect to the cloud (which is mostly the case with mobile data), not much information will be logged to hold a user accountable for some operations. This could eventually lead to a user denying their actions unless some other form of authentication is able to prove that a user logging in and carried out some functions.

3.5 Hacking Issues due to Network, API or Social Weaknesses.

Cloud computing services are consumed and managed via internet connections. Therefore, like any other online service, SMEs need to be aware of the risk of network attacks like spoofing websites, sniffing/eavesdropping on network traffic, Denial-of-Service attacks, man-in-the-middle attacks, pharming, wiretapping, etc., on the normal end-user interfaces, as well management/administrator interfaces, application programming interfaces (APIs), web-services.

3.6 Foreign Law Issues and Government Regulations

In traditional IT data and processes remain on-premises, so foreign jurisdictions are usually not an issue. Cloud services sometimes involves the use of cloud providers or datacenters abroad, which means that to a certain extent foreign jurisdictions may have an impact on the security and privacy of the cloud service. For example, violations of the law by the other customers (co-tenants) may lead to services being ordered shut (for example as part of a criminal prosecution), without taking proper care of the other customers. It has been argued by legal experts that even if the physical location of supporting equipment or datacenters are not in a foreign country there could still be an impact.

Additionally, according to the Kenyan law, a person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment term for a term not exceeding three years, or to both. In the event that a user is unknowingly

duped into disclosing a password to a malicious user, he or she may still be held liable for a crime and prosecuted. Therefore, it is of utmost important to understand the cyber laws carefully and SMEs should understand which foreign jurisdictions may play a role for data stored in different countries and if there are incompatibilities with Kenyan laws.

4. CONCLUSION

On fundamental challenges, the findings established that cloud computing face substantial challenges in the implementation of SaaS delivery model. Some of the challenges found include: Data/information stored on the cloud issues on downtime in the internet; cloud administrators are exposed to high risk, if they turn rouge and try to access data stored on clouds; lack of certainty in trailing actions of the users, there is no definite way of telling that the data has been deleted to its entirety; there is no control over the hardware, technology and backed up details of the cloud platform; multi-tenancy issues- there is risk that hackers can manipulate weakness in data security model to get an illegitimate access to data or application; and lack of liability in case of security incidences as a result of cloud computing and subsequent misuse of privileges to gain access or support third parties in accessing data/information they are not meant to access, which further interferes with confidentiality and integrity of information within the cloud service.

The researcher recommends the following for the SMEs:

- The SME in its entirety needs to recognize and understand the value of the cloud-based technology and data. There must be constant vigilance and continuous monitoring of risk to these information assets, including ensuring compliance with appropriate laws, regulations, policies and frameworks.
- All users of the cloud should have knowledge of cloud computing and its risks, understand their responsibilities and be accountable for their use of the cloud. From the study findings, the following recommendations were made;
- Both local and national governments should step up in their bid to provide reliable electricity supply to reduce issues of downtime occasioned with power shortage.
- The managers of SMEs should employ qualified IT staff with high integrity to reduce chance of internal and external hacking.
- SMEs should understand and adopt the governmental and legislative rules and acts pertaining to cybersecurity.

5. REFERENCES

1. Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: concepts, technology & architecture*. Pearson Education.
2. Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 693-702). IEEE.
3. Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, 2(1), 60-63.
4. Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *Information and communication technologies (WICT), 2011 world congress on* (pp. 217-222). IEEE.
5. Jansen, W. A. (2011, January). Cloud hooks: Security and privacy issues in cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-10). IEEE.
6. Buyya, R., Broberg, J., & Goscinski, A. M. (Eds.). (2010). *Cloud computing: Principles and paradigms* (Vol. 87). John Wiley & Sons.

7. Cisco, The Cloud in Africa: Reality Check, 2013. Retrieved December 15th, 2017 from: <http://www.cisco.com/web/ZA/press/2013/112813.html>.
8. Hamburg, I., & Bucksch, S. (2016) Cloud Computing in SMEs.
9. Ouf, S., & Nasr, M. (2011, May). Business intelligence in the cloud. In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on (pp. 650-655). IEEE.
10. Computing, C. (2010). Security—A Natural Match. Trusted Computing Group (TCG) <http://www.trustedcomputinggroup.org>.
11. Mohamed, A. (2009, March 01). A history of cloud computing. Retrieved March 12, 2016, from <http://www.computerweekly.com/feature/A-history-of-cloud-computing>
12. Dash, S. B., Saini, H., Panda, T. C., & Mishra, A. (2014). Service level agreement assurance in cloud computing: a trust issue. *International Journal of Computer Science and Information Technologies*, 5(3), 2899-2906.
13. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
14. Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.
15. Shroff, G. (2010). Enterprise cloud computing: technology, architecture, applications. Cambridge university press.
16. Velte, A. T., Velte, T. J., Elsenpeter, R. C., & Elsenpeter, R. C. (2010). Cloud computing: a practical approach (pp. 1-55). New York: McGraw-Hill.
17. Xu, Y., Yang, Y., Li, T., Ju, J., & Wang, Q. (2017, November). Review on cyber vulnerabilities of communication protocols in industrial control systems. In Energy Internet and Energy System Integration (EI2), 2017 IEEE Conference on (pp. 1-6). IEEE.
18. Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer London.
19. Jahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L., & Xu, J. (2014, April). Multi-tenancy in cloud computing. In Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on (pp. 344-351). IEEE.
20. Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. Paper presented at 2010 IEEE 3rd International Conference on Cloud Computing, Miami, Florida.
21. Sen, J. (2013). Security and privacy issues in cloud computing. *Architectures and Protocols for Secure Information Technology Infrastructures*, 1-45.

Cite this article:

Rupra, S. S. (2018). Investigate the Security Challenges in SaaS Private Cloud using OwnCloud. *Mara Res. J. Comput. Sci. Inf. Secur.* Vol. 3, No. 1, Pages 12 - 22, ISSN 2518-8453