Mara International Journal of Scientific & Research Publications
Vol. 2, No. 1, July 2018, Pages 1 – 14, ISSN 2523-1456

A Framework for Assessing Security in a SaaS Cloud Paradigm for SMEs

Satwinder S. Rupra*, Nickson Karie and Kefa Rabah
School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: satwinder@sumocomputers.net, nickson.karie@gmail.com, kefa.rabah@gmail.com

* Corresponding author

Received: July 17, 2018
Published: July 31, 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. The extremely scalable nature of cloud computing allows its users to access huge amounts of data and use distributed computational resources via different interfaces. 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. Many clients, especially SMEs, worry about their susceptibility to attack if their businesses' crucial IT resources and information are outside the firewall. Numerous security and privacy concerns like loss of control, lack of trust and multi-tenancy issues appear with the usage of cloud. These challenges, if left unaddressed, could lead to severe data breaches and possible business losses. The lack of knowledge, governance and improper policies can also sometimes create further vulnerabilities in the cloud. This paper is intended on proposing a framework for implementing security in (SaaS) cloud computing paradigm and, therefore, aid SMEs to counter the possible threats and vulnerabilities associated with the cloud. The researcher devised security checks to counter the cloud threats, which included Cloud provider's security and risk management, backups, internal human resources security, access control, software security and encryption, logging and compliance with legislation. The framework is a vital tool for SMEs to test and rate their cloud security and, therefore, make improvements to mitigate the security threats associated with cloud computing.

Keywords: Cloud computing, SaaS, SME, Security challenges

1. INTRODUCTION

Cloud computing is defined as both the applications distributed as services over the Internet and the systems software and hardware in the datacenters that offer those services [1]. Corporate information has increased in volume beyond the convectional computer storage growing into thousands of Gigabytes over time. The reliance on data for performing most business operations means data has to be available anywhere and anytime. Cloud computing is a platform that provides such flexibility of making data available on demand. Being a fairly new platform in computing, cloud computing is becoming a popular method of data storage as well as a service platform due to its numerous benefits. Most importantly, cloud computing provides a storage facility that is hosted and accessible over the internet, making data readily available when and as required [2].

Cloud computing has become increasingly popular service due to the numerous advantages it possesses. These include high computing power, cheaper cost of services, better performance, scalability, accessibility and availability among others [6]. Organizations are now comfortable to allow their employees access organization's information on their mobile phones and tablets and to carry out business-critical tasks. However, in the past this was not always the case. For a long time many managers were against the idea of letting their staff store and access organization sensitive information in this way, because of credible concerns about what would happen to their data should the device be lost, stolen or hacked. However, in the recent past mobile security technologies have come on leaps and bounds, but many organizations have also turned to virtualization which is an aspect of cloud computing to protect their data, and ensure their infrastructure can cope with the growing number of end-points connected to it. It is clear that mobility and virtualization has helped organizations in the publishing and manufacturing industries to meet their business objectives. However, since this kind of computing paradigm is fairly new, it has shortfalls that need to be addressed to make its services more convenient to use.

1.1 Problem Statement

Recent cloud computing models are known to be very promising internet-based computing platforms, however, these models could result in a loss of security over customer data. This usually happens because the enterprise IT assets are hosted on third-party cloud computing platforms. Where cloud computing can help organizations accomplish more by paying less and breaking the physical boundaries between IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing exemplar [3,4].

Therefore, to address the problem of different cloud security threats as well as the lack of enough guidelines and mitigation strategies; this research intends to come up with a framework for implementing security in a SaaS cloud paradigm for SMEs. The framework will be used to aid SMEs to mitigate the cloud threats by assessing their level of security and providing details on how secure their data is in the cloud. The framework can be used to assess the level of security in a cloud environment as well as give details and guidelines on how security can be improved.

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, integration and development services [8].

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/upsize 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 Security Threats for IS on the Cloud

In the modern era of technology including cloud computing, information security has become a critical business enabler as opposed to convectional processing and technology. With the new and evolving tools, standards, frameworks and technologies available and evolving, SMEs have pretty decent to average way of aiding them to secure their operations, critical information and hardware and software infrastructure. Despite this, SMEs still have challenges to keep up with regulatory requirements, economic conditions and risk management [15]. Many organizations are yet to clearly understand the role of information security in their operations. Many bosses and senior management especially in small or medium organizations feel that information security is just an additional cost that they occur, however on the contrary, effectively managed

information security organizations can be instrumental in helping an enterprise meet its business goals by improving efficiency and aligning business objectives [16].

Small organizations may time and again interpret information security in isolation: often thinking that security is not the organization's responsibility and on the contrary is someone else's responsibility. Therefore, there senior management and staff make little effort to link the security implementations and aspects to business goals. As a result of this tagged approach, it is quite easy to suffer weaknesses in security management, and could result in to serious exposure. From a financial perspective, it is quite possible for this lack of understanding to result in unnecessary expenditure on security and control as security is tacked after a breach occurs instead of prevention [17]. From an operational perspective, information security efforts might not be able to achieve the intended business benefit, which may also result in information at risk.

Some SMEs might interpret information security as being just a technical aspect. Although information technology offers implements that are vital for protecting information, information technology in itself is not an acceptable solution. To prevent breaches and safeguard information, SMEs need to establish information security policies that are supported by standards, procedures and frameworks [18]. The guidance establishes the direction for the information security program and expectations as to how information is to be used, shared, transmitted and destroyed [19]. In many enterprises, technology strategies, policy, process and standards are developed without an understanding of how organizational culture impacts program effectiveness. Security efforts that fail to consider how humans react to and use technology often do not deliver intended benefits. Information security programs need to take into account how the organization and its people, processes and technologies interact, and how organizational governance, culture, human factors and architectures support or hinder the ability of the enterprise to protect information and to manage risk.

Information security managers have struggled to create programs that are aligned with enterprise goals and priorities, that bring value to the enterprise, and that support the ability of management to innovate while controlling risks. Developing an information security program and integrating it into business goals, objectives, strategies and activities are complicated by the lack of a model that describes what an effective information security program encompasses, how it functions, and how it relates to the enterprise and the enterprise's priorities. What is missing is a descriptive model that business unit managers and their counterparts in information security can use to implement information security in business, rather than technical, terms.

Securing any Information system includes firstly identifying the unique threats and challenges that pertain to the system using risk management plan and, thereafter, implementing the relevant countermeasures to be overcome the threats and reduce the security risks [20]. Eventually, the identified security requirements and selected security measures are introduced to the development and integration process, to incorporate the security controls with the information systems requirements. These include both functional and operational requirements, and may include other related system requirements like reliability, maintainability and supportability [21].

Cloud computing paradigm includes numerous security benefits due to the nature of its technology. These include centralization of security, redundancy and high availability. Although much of the traditional challenges posed by security threats are countered effectively due to the infrastructures of the cloud, several peculiar security challenges are introduced. Cloud computing may require risk assessment in aspects like availability and reliability issues, data integrity, recovery, and privacy and auditing [22].

Security in general for any system, is usually related to confidentiality, integrity and availability; these therefore are vital components when implementing any IT system securely. [2]. The aspects of security

discussed above apply to the three broad categories of assets which need mandatory securing. These are data, software and hardware resources. The importance of confidentiality, integrity and availability in the cloud paradigm is discussed in detail in the below sections.

2.2.1 Confidentiality

Confidentiality is one of the pillars of CIA that simply means protection of information from unauthorized disclosure. This means that only authorized personnel have the ability to access protected data. Since the cloud has numerous points of access due to the devices and applications involved, threats of data breach increases in the cloud platform. In the cloud computing architecture, resources are significantly shared by users at multiple levels including the network, host and application level. Although virtually the users are isolated, the underlying hardware is usually one and the same. This can cause problems with data confidentiality if not implemented well.

Confidentiality can further be breached accidentally due to data remanence [23]. Due to a nominal erase or remove operation, some data residue may be left intact. This may lead to the unwilling disclosure of private data; however, a user may claim a large amount of disk space and then scavenge for sensitive data. Confidentiality in the cloud is associated with user authentication. Electronic authentication is the process of establishing confidence in user identities, electronically presented to an information system. Lack of strong authentication can lead to unauthorized access to users account on a cloud, leading to a breach in privacy [22].

2.2.2 Integrity

The second aspect of information security is integrity. Integrity means that data (and sometimes hardware and software) should only be modified by authorized personnel. Data Integrity refers to securing data from unauthorized changes including deleting or modification [25]. By denying unauthorized access, a customer can achieve better assurance and integrity in data. Furthermore, this can also offer greater accountability on whom or what may have altered data or system information. Authorization is a means by which an authenticated user is given access to secure resources controlled by the system based on their level of authority [22]. Because the cloud allows may access points for its users to connect (usually from anywhere with internet access), authorization is crucial to maintain data integrity and security at large.

A cloud computing provider is entrusted by their clients to provide integrity for their data. However, due to the working nature of the cloud model, several threats including sophisticated insider attacks can take place. Data can be deleted, modified or changed purposefully or accidentally. For example, an unhappy employee may purposefully fabricate a program to fail when a certain command is executed or a certain time is reached. Additionally, the security of cloud services is dependent on the security of the API or interfaces that the cloud providers offer to their customers. If unauthorized users gain control of them, data integrity can be seriously violated [26]. Cloud providers may need to also address hardware and network integrity, as they control the entire hardware and network resources in a cloud model.

2.2.3 Availability

Availability is an attribute of information security that means that a system is always accessible and usable whenever requested by an authorized entity [22]. System availability includes a systems ability to carry on operations even when some authorities misbehave. A secure system must be able to continue operating even if a security breach occurs. A cloud provider needs to assure that all the relevant aspects of the cloud are available to clients upon demand [26].

2.3 Top Security Risks with Cloud Architecture

According to Cloud Risk Assessment report published by ENISA in 2009, the following cloud specific risks have been identified:

- *Loss of Control:* when using the cloud infrastructure, the clients usually gives away control on several issues that could affect security. In such a case, the security services are usually not committed and documented in the SLAs therefore leaving a gap in the security defenses. The cloud vendor also usually does not allow the client to carry out audits and this also means that certain kind of compliances cannot be achieved. E.g. PCI DSS. This has been earlier discussed in more details.
- *Management interface compromise*: most management interfaces in the cloud platform are accessible through the internet browsers. These interfaces are connected to a larger set of resources and therefore pose an increased risk especially through web browser vulnerabilities.
- *Data protection*: cloud computing poses a number of data protection risks. Because the owner of the data has not control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.
- *Insecure or incomplete deletion of data*: whenever the data owner makes a command to delete a cloud resource, there is not certain way of telling that the data has been deleted to its entirety. This could possibly be because either extra copies of data are stored for backup purposes and therefore not available to the client or because the disk shares data from other clients and hence cannot be destroyed.
- *Malicious insider:* a cloud administrator may become a very high risk if turn rouge and try and access data stored on clouds. Although this is usually less likely, the potential damage that may be caused by malicious insiders is often far greater.
- *Availability Chain*: the internet connectivity forms a single point of failure as far as the cloud is concerned. This means that if the internet is down, then there is no cloud access and therefore loss of availability.

2.4 Cloud Frameworks

In the scenario of the SMEs who want to move to the cloud or are using the cloud services, the security tasks which will be carried out by the cloud provider include:

- *Managing of hardware and facilities*, including physical security, power, cooling, etc.
- Managing of server operating systems and the application server, including development, deployment, patching, updating, monitoring, checking logs, etc. For example, it is the responsibility of the provider to patch the server operating systems in time.
- *Managing the application software,* including development, patching, updating, monitoring, and checking logs, and so on. For example, it is the responsibility of the provider to fix software flaws in the office software.
- *Managing updates of software and data.* The customer, the SME in this case, is merely responsible for handing out accounts to its employees, revoking accounts when employees leave, resetting passwords and such operational tasks. In this scenario most security tasks are outsourced to the provider. The customer, once the service has been procured and is up and running, will have few security tasks left to perform. However, because security cannot be outsourced, if something goes wrong causing sensitive data about to leak, then the SME will in the first place be held responsible for the damages. For the SMEs, hence, clarity about security tasks and responsibilities is a crucial consideration in the cloud procurement process.

The ISO/IEC 25010:2011 standard is an international standard that is used for the evaluation of the software quality. It is divided into two sections, product quality and quality in use. The product quality model composes of eight characteristics (which are further subdivided into sub-characteristics) that relate to static properties of software and dynamic properties of the computer system. The model is applicable to both computer systems and software products. The characteristics and sub-characteristics provide consistent terminology for specifying, measuring and evaluating system and software product quality. They also provide a set of quality characteristics against which stated quality requirements can be compared for completeness. When used in conjunction with a deep security assessment, is valuable for putting more structure and coherence around assessing the suitability of new vendors and new technologies, including cloud offerings. The framework can be useful for cloud assessments if it is customized well to fit the requirements.

The table below shows how the product quality characteristics of usability, reliability and security and their sub-characteristics of the ISO/IEC 25010:2011 standard can be mapped to the identified cloud security threats in this research as shown in Table 5.1

Table 1: Sub-characteristics of the ISO/IEC 25010:2011 Standard

Characteristics	Sub-Characteristics	Associated Cloud Risk and Explanation
Usability	Accessibility	Bandwidth and cloud provider uptime can cause serious performance and goal delivery issues.
Reliability	Availability	Data/information stored on the cloud may face a lot of availability issues due to downtime in the internet.
Security	Confidentiality	Deleted data storage can cause numerous security challenges if placed in the wrong hands. Insider threats are a big risk to the usage of data in the cloud.
	Integrity	Insider threats are a big risk to the usage of data in the cloud.
	Non-repudiation	Challenge of non-repudiation leading to a user denying their actions.
	Accountability	Because the owner of the data has not control over the data handling practices of the cloud vendor, there is no sure way of telling that data is being handled in a lawful way.
	Authenticity	Hacking issues an seriously affect the authenticity of information stored on the cloud and otherwise.

The security-related threats and vulnerabilities can also be assessed in an analogous manner by assessing against ISO 27005x controls that are applicable to the exposures within cloud computing as shown in Table 2

Table 2: Assessment against ISO 27005x Controls

Number	Challenge in the Cloud	Likelihood	Impact	Risk
A	Insider Threat	Medium	High	Significant
B	Improper data deletion	Medium	High	Significant
C	Bandwidth and availability issues	Low	Medium	Minor
D	Repudiation and user denial	Low	Low	Minor
E	Multi-Tenancy issues	Medium	Low	Minor
F	Hacking issues	Medium	High	Significant
G	Foreign laws and government regulation	Low	Low	Minor
H	Loss of Control due to moving data in the cloud.	High	Low	Significant

The above challenges can be plotted on to a risk matrix highlighting the key issues and also an indication of their criticality, as shown in Fig. 1.

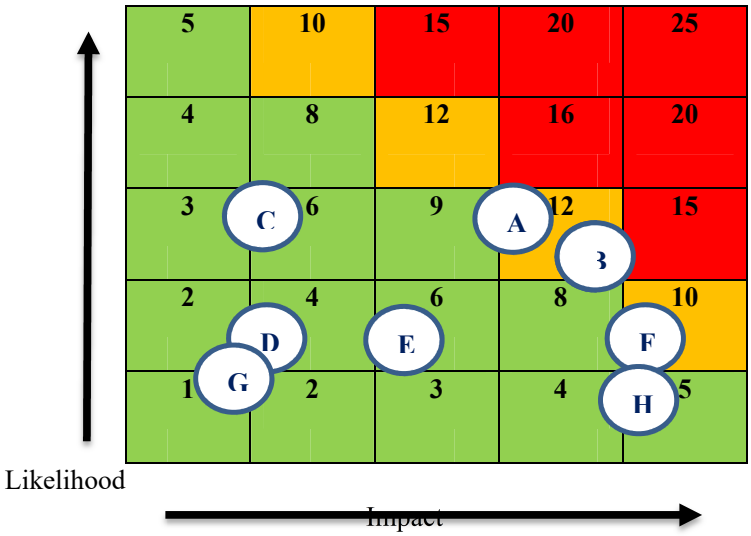

Fig. 1: Impact vs Likelihood Analysis

The green area depicts minor risks, yellow depicts significant risks and red depicts major risks that could significantly affect the SME cloud security. Based on the above information, a list of security checks can be devised that SMEs can use to get the most relevant information about the security of their cloud service, and to understand it better to mitigate the identified challenges in the study. The security checks are aligned to the ENISA risks and opportunities security questions to understand infrastructure security, however selective categories that are relevant to the study have been used and have been tailored to the area of study.

Table 3: Security Checks

Security Check	Challenge That It Addresses
Cloud providers security and risk management	Multi-Tenancy issues, Insider Threat, Improper data deletion.
Contingencies and backups from the provider and SME	Bandwidth and availability issues.
Internal Human resources security	User Errors and all other challenges arising from the SME side like social engineering.
Access Control	Hacking issues, Challenge of insider threat.
Software security and encryption	Hacking issues, Challenge of insider threat.
Data in Transit	Hacking issues
Monitoring and logging	Repudiation and user denial
Compliance with national/international legislation	Foreign laws and government regulation

3. FINDINGS AND RESULTS

The SME or cloud customer should carry out an assessment on the security of the potential cloud vendor themselves. This can be done through clauses in a contract or SLAs, audit reports from third parties, self-assessments by the provider, a track record of past performance and statements from past customers or even getting the information directly from the vendor The researcher therefore suggests the below security checks that concerge into a framework for assessing and implementing cloud security. The security checks are described below as well as details on what to expect in the responses towards the cloud providers side:

3.1 Cloud providers' security and risk management

All SMEs procuring cloud services should have an idea about the quality and effectiveness of the organizational structure and how they manage the security for the data of their customers. The SMEs need to identify the contact person for security incidents and get their general approach in managing security incidents. The SME should asses the security approaches of the cloud provider and see how well equipped they are in terms of their security. The management should obtain briefings from internal and/or external business and technical experts to understand the technology and its alignment to the business objectives. A cloud provider that holds an international standard like ISO 27001 or similar will show that they take their security seriously.

Security questions that a customer should ask their providers include how they manage deleted data and how long do they keep the data for. Does the customer have a choice to control how long deleted data is kept in the cloud server and how they assure the customer that data is not recoverable after deletion. The aim of this security check is to develop model contract terms that would regulate issues such as data preservation after termination of the contract, data location and transfer, ownership of the data. Identifying these best practices will accelerate the take-up of cloud computing and strengthen security by increasing the trust of prospective consumers.

2.2 Contingencies and backups from the provider and SME

For customers it is important to understand how the cloud service is resilient in the face of disasters and how data is backed up. As much as loss of internet is not as much of an issue as it used to be, the researcher

still feels this is an integral challenge that needs to be addressed. An SME should have a secondary link to as a backup in case the primary link fails, even if the secondary link is of a smaller bandwidth and enough to log in to the cloud and carry out basic operations. A good internet of 10mbps speed would be optimum for the connection to work well and an SLA agreement of a 99.5% or above by the ISP is required for continued operations which translate to about 1.8 days in a year.

Similarly, it is important to determine what sort of failover mechanisms the cloud provider has in place to counter against attack as well as natural disasters. The cloud provider needs to have their data centers spread out across different geographic regions, nationally or globally. Geographic spread can provide resiliency against regional issues and local disasters such as storms, earthquakes, or cable cuts. It can also be used to mitigate certain Denial of Service (DoS) attacks, allowing customers to get access at other locations. This could improve the overall availability and performance of the service. Therefore an SLA from the service provider that offers 99.9% uptime is appropriate.

2.3 Internal Human Resource Security

Although this aspect of the challenge in cloud security is not demonstrated in the study, however it is still a very important aspect determined by IT bodies including ISACA and ENISA. If users are not trained well and do not understand the system properly, this becomes a huge security challenge. In cloud computing, some administrative processes, like issuing user credentials, do not happen face-to-face between colleagues, but online via emails and websites. This increases the risk of social engineering attacks, in which an attacker fakes communication or information so it appears to come from a trusted source, like the cloud provider. Attackers may target normal users, or users with high-privilege roles, such as software developers, system administrators, managers, both on the cloud provider's and the customer's side.

SMEs should take into account the risk of social engineering, such as phishing/spear-phishing, spoofing, etc. and assess the potential impact on the data and processes. All users of the cloud should have knowledge of the cloud and its risk based on their duties, understand their responsibilities and be accountable for their use of the cloud. The managers and IT administrators should work together to ensure that the involved business and technology staff have the appropriate skills to embark on the cloud initiative or that the needed expertise is obtained externally.

2.4 Access Control

This is the one of the most important factors to consider when assessing cloud security. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security.

Cloud providers that use two factor authentication to authenticate their clients are a lot more secure than simply keying in a password. With two factor authentication enabled for a cloud service, any attempt to sign in on an unrecognized device requires that you enter a secret code, received as a text message or generated by an authenticator app on your previously registered smartphone. You can choose from multiple authenticator apps, which all follow an open standard for generating time-based one-time passwords. Alternatively, security can achieved in different levels such as providing static username-password as the entry level authentication, followed by OTP based on token generator technique that act as credentials for each user.

Two factor authentication also ensures that the insider threat is tackled well. Even if an insider or administrator is able to change a cloud users' password as demonstrated in chapter four, they will still need

a second authentication in terms of a password or similar information to be able to log in. This therefore means that they will need access to the users' device as well to be able to log in therefore increasing security significantly. Another access control technique that will increase security is Risk-Based Authentication (RBA) which is a dynamic response to the changing conditions of the risk rating attached to a particular client at a particular time. Risk ratings are assigned to both the operation and the client. The higher the risk rating of the operation, the higher the authentication level required of the client, in order to complete the operation. RBA determines the customer's risk level by examining behavioural contexts, such as a history of similar requests, location of the customer and operation, and timing of the request. Any behavioural variances can trigger a reaction ranging from a request for further authentication to a denial of the transaction.

2.5 Software security and encryption

Software vulnerabilities could have a big impact on the customer's data or processes. Customers should ask which measures are in place to make sure software underpinning the cloud service is kept secure and which software is not under control of the provider, and should be kept secure by the customer. If the cloud service does not automatically encrypt data before it is uploaded, SMEs should try and encrypt these files beforehand. Third-party encryption tools that will apply passwords and encryption to files could do a great deal of security for data at rest while it is stored in the cloud. A cloud access security broker (CASB) is another way that an SME can encrypt data and control their keys. A CASB offers a single point of visibility and access control into any cloud app in an SME. The control comes through contextual access control, encryption for data at rest and leakage protection of data. A CASB mediates the connections between cloud apps and the general public through several API connectors and proxies.

2.6 Data in Transit:

Another important consideration for SMEs is security of data in transit. SMEs should ask their providers and potential SaaS partners what protocols they use for transmitting data. The Secure Socket Layer (SSL) approach is susceptible to a man-in-the-middle attack and therefore is not the best option. Implementing TLS rather than SSL eliminates the vulnerability, but some legacy systems running older operating systems, such as Windows XP, are unable to implement TLS. Therefore, it is also vital that an SME uses the latest operating systems like Windows 10 that are regularly updated.

2.7 Monitoring and Logging

SMEs should be able to monitor the performance and security of the service, via alerts, periodic reports, and dashboards. SMEs should also be able to monitor issues by analyzing transaction logs, either via automatic interface or upon request, for example in the case of an incident. It is critical for an SME to acquire the key log data that offers a clear view into the operational and security events over a period of time. Maintaining logs is not only IT best practices, but it can prevent operation and security risks from being diminished. A third party logging software or internal cloud provider log management is sufficient to monitor the cloud computing activities.

The ability for an enterprise to track what applications users are accessing is vital with respect to both security and regulatory perspective. Multiple failed authentication events or authenticated users attempting unauthorized application access will highlight potential security and fraud related activities. In addition, regulated industries require audit trails to prove that only authorized users have accessed or attempted to access certain confidential systems.

2.8 Compliance with national/international legislation

In cloud computing customers sometimes work with providers and/or datacenters that may be located outside Kenya, this therefore means that foreign legislation might be relevant to take into account. SMEs should ask which jurisdiction is relevant to take into account and which legislation applies to their cloud service. It is also important for users and administrators to understand the Kenya law and how it affects their data and its flow to and from the cloud. The above security checks are summarized in the framework as shown in Fig. 2:

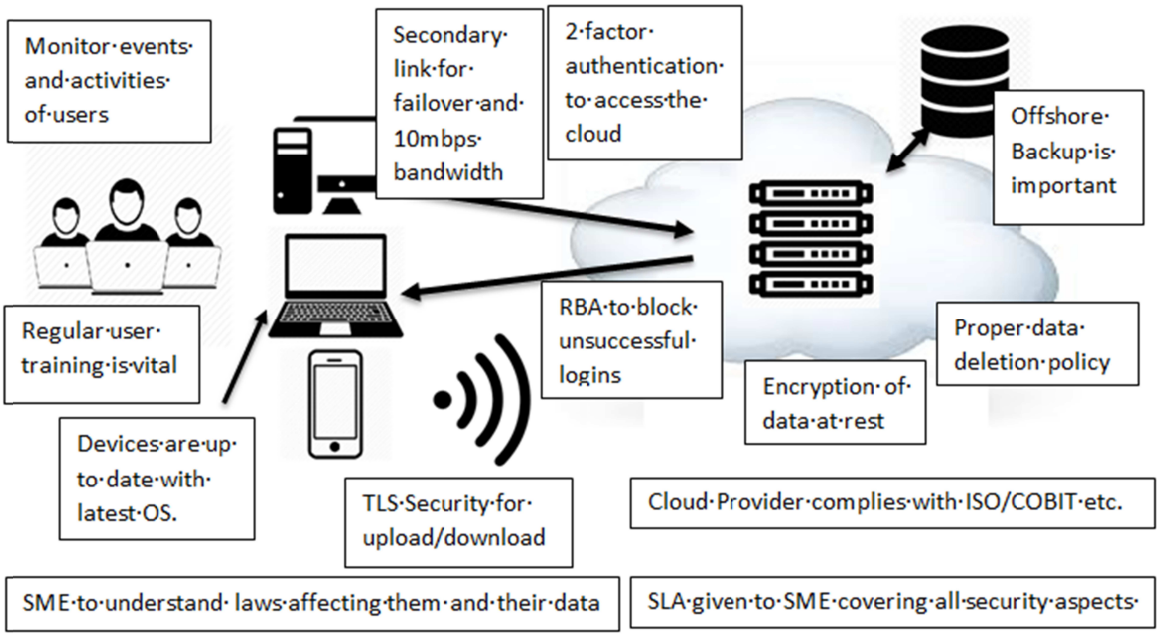

Fig. 2: Proposed Cloud Security Framework

4. CONCLUSION

The research was focused in aiding SMEs adopt cloud security in an effective manner and steer clear of the threats that cloud computing poses if not implemented well. This research was intended to show how security in SaaS cloud paradigm could be improved by adopting a security framework for the same. Specifically, the study developed a framework to address SaaS security vulnerabilities for SMEs in Kenya.

Based on the above security checks, the researcher has devised a security rating for cloud computing for SMEs which will easily guide the SMEs to make a decision in how secure their cloud provider is and what sort of measures they need to implement to be able increase their security to an acceptable level. If the checks implemented are below 50% then the setup is considered as not secure, if the checks are between 50% and 75% implemented, then they are considered as somewhat secure and if the checks add up to a percentage above 75% then the cloud provider solution will be considered secure. This is the target that SMEs need to achieve out of their cloud security, see Table 4.

Table 4: Security checklist for cloud services implementation

No.	Item checklist	YES	NO
1	Does the cloud provider have an SLA given to you covering the security aspects of the cloud infrastructure?		
2	Is the cloud computing vender complying with an international standard like ISO		

	27001, COBIT (or similar) or having assessed their security with standards like ENISA, ISACA or similar?		
3	Does the cloud provider conform to data deletion after account deactivation in a well communicated and agreed manner?		
4	Does the cloud provider give information on the number of copies of the client data that they retain as well as the storage locations of the data?		
5	Does the SME have a secondary link to act as a backup in case the primary one goes down?		
6	Does the SME have a bandwidth of above 10Mbps to be able to sustain their load?		
7	Does the cloud provider have data backups at geographically different locations to be able to continue working in case of a disaster or an attack?		
8	Are the users of the SME trained well and from time to time to understand the usage, risks, challenges and security of the cloud effectively?		
9	Does the cloud provider offer two factor authentication, one time passwords or similar means of authenticating users?		
10	Does the cloud provider provide Risk-Based Authentication to block unsuccessful attempts to log-in and attempt to determine the identity of the users?		
11	Does the SME have any sort of data encryption in place either through the cloud provider or third party?		
12	Does the cloud provider have Transport Layer Security or similar in place to ensure data is secure against man in the middle or similar attacks?		
13	Does the SME have their computers and devices installed with the latest operating systems and regularly patch and update their operating systems?		
14	Does the SME have any sort of logging software in place either through the cloud provider or third party?		
14	Have the senior management, administrators and users of the SME understood through trainings and briefings how the Kenyan laws and international laws affect their data in the cloud?		

When all the checks are completed and their relevant procedures implemented well, then the SME has implemented cloud security in the recommended manner and therefore have achieved an acceptable security level. To sum up the above discussion, the researcher concludes that for an SME to be able to secure their cloud installations, they need to have the security checks in place as indicated and implement a secure cloud implementation and operation as depicted

5. REFERENCES

1. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), 7-18.
2. Rimal, B. P., Choi, E., & Lumb, I. (2009, August). A taxonomy and survey of cloud computing systems. In INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on (pp. 44-51). Ieee.
3. Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.
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. Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. International journal of information management, 31(3), 272-278.
16. Sallé, M. (2004). IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing. Hewlett-Packard Company, 8-17.
17. Wheeler, E. (2011). Security risk management: Building an information security risk management program from the Ground Up. Elsevier.
18. Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. Information Systems Management, 24(4), 361-372.
19. Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. Cengage Learning.
20. Longley, D., Shain, M., & Caelli, W. (1992). Information security: dictionary of concepts, standards and terms. Springer.
21. Zardari, S., & Bahsoon, R. (2011, May). Cloud adoption: a goal-oriented requirements engineering approach. In Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing (pp. 29-35). ACM.
22. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.
23. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.".
24. Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing, 63(2), 561-592.
25. Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks.
26. Stallings, W., & Brown, L. (2008). Computer security. Principles and Practice.
27. Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.

Cite this article:

Rupra, S.S., Karie, N. and Rabah, K. (2018). A Framework for Assessing Security in a SaaS Cloud Paradigm for SMEs. *Mara int. j. sci. res. publ.* Vol. 2, No. 1, pp. 1 - 14, ISSN 2523-1456.