2017

# A Scheme for Improving data confidentiality in the cloud computing environment

Fabiano Iriale Tikwang
*Faculty of Information Technology (FIT)*
*Strathmore University*

# A SCHEME FOR IMPROVING DATA CONFIDENTIALITY IN THE CLOUD COMPUTING ENVIRONMENT

**TIKWANG IRIALE FABIANO**

**Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Science in Computer-Based Information Systems at Strathmore University.**

**Faculty of Information Technology,**

**Strathmore University,**

**Nairobi, Kenya**

**June, 2017**

## Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

TIKWANG IRIALE FABIANO

……………...........................................

12th June, 2017

## Approval

The dissertation of Tikwang Iriale Fabiano was reviewed and approved by the following:

**Name of Supervisor: Dr.Vitalis Gavole Ozianyi,**
Senior Lecturer, Faculty of Information Technology,
Strathmore University

**Dr. Joseph Orero,**
Dean, Faculty of Information Technology,
Strathmore University

**Prof. Ruth Kiraka,**
Senior Lecturer, Faculty of Information Technology,
Strathmore University

## Dedication

I bestow special thanks to Nelly Cheposepoi and entire AkÖchÖ’s family. For you, I am.

# Acknowledgement

I acknowledge the tireless effort, advice, patience and guidance offered to me by my supervisor Dr. Vitalis Gavole Ozianyi in ensuring the dissertation was successfully completed. My appreciation also goes to my class mates for their support and encouragement. Above all, I give honour to God who granted me the health, strength, perseverance and the will to keep going on despite challenges.

# Abstract

Cloud computing has ushered in an era whereby small and medium sized companies enjoy computing power which was usually a preserve for big corporations. Despite these benefits, the present cloud data confidentiality techniques are still evolving, and as they evolve so are the threats, hence posing security and privacy challenges, thus becoming an impediment to cloud adoption. Currently, cases have been cited where hackers have stolen stored cloud data, later to appear in social media embarrassing the firms. Among the key vulnerabilities attributed to loss of cloud data include: account hijacking, malicious insider breaches, data breaches attributed to weak identity and access management, phishing, SQL injection, among others.

Several research articles have been reviewed with some proposed solutions but these solutions have fallen short of addressing account hijacking and malicious insider threats. In addition, the online survey conducted highlighted that insider breaches are among the main form of vulnerability to cloud data. These challenges within the cloud storage informed the basis for the design of a scheme for improving data confidentiality in the cloud computing environment.

The data confidentiality is achieved by implementing authentication login which triggers a six digit code to be sent to a client mobile or e-mail for further authentication, thus, enabling situational awareness of data breaches in real-time. This approach will enhance reliability and trust of cloud services enabling users to maximize on potential benefits offered by the cloud environment.

## Table of Contents

## Table of Figures

## Abbreviations/Acronyms

| | | |
|---|---|---|
| **API** | - | Application Programming Interface |
| **CSA** | - | Cloud Security Alliance |
| **CSCC** | - | Cloud Standards Customer Council |
| **CSP** | - | Cloud Service Provider |
| **DES** | - | Data Encryption Standard |
| **IaaS** | - | Infrastructure as a Service |
| **IDG** | - | International Data Group |
| **IEEE** | - | Institute of Electrical and Electronics Engineers |
| **IT** | - | Information technology |
| **PaaS** | - | Platform as a Servicce |
| **RSA** | - | Rivest Shamir Adleman |
| **SaaS** | - | Software as a Service |
| **SAML** | - | Security Assertion Markup Language |
| **SSO** | - | Single Sign-On |

# Chapter 1: Introduction

## 1.1 Background of Study

Cloud Computing is gaining popularity, with no universal agreement on its definition. According to Daylami (2016) there is an endemic confusion of what Cloud computing stands for. Similarly, Kepes (2017) points out that cloud computing is amorphous, since it fails to settle on one thing, it begins with Infrastructure as a Service (IaaS) at the base, through Platform as a Service (PaaS) to Software as a Service (SaaS). Firstly, NIST (2016) defines cloud computing as a model for enabling suitable, on-demand network access to pooled configurable computing resources that can be speedily provisioned with minimal management effort. Secondly, Bartock, et al., (2015) observe that clouding computing are designed to be highly agile and flexible, using whatever resources are available to process workloads for their customers. Similarly, clients access services according to their preferences regardless of the location (Rajkumar, 2013). While Daylami and Kepes highlight the contention of defining cloud computing, NIST agrees with Bartock, et al., on key traits if a resource is to be referred as cloud. Rajkumar, on the other hand, draws attention on the freedom of choice offered to clients. Thus, Cloud availability when needed, is a key factor persuading users towards the cloud. On the other hand, this strength has been exploited by hackers including states to create internet anarchy, thus, being the contributing factor for user's lack of trust and confidence in keeping their data in the Cloud.

Crawford and Johnstone (2012) observe that in 1999 Saleforce.com had the first delivery of applications via the web, followed closely by Amazon Web Services (AWS) in 2002; in 2006 Google docs and Amazon Elastic Compute Cloud (EC2) came into existence, then Eucalyptus in 2008 and subsequently Microsoft Azure in 2009. The trend of adopting Cloud computing is gaining popularity. Cisco (2016) highlight that by 2020, 92% of workload will be processed by cloud data centers, in comparison to 8% for traditional data centers. This means that growth of the data center workload is by a factor of 2.6 from 2015 estimates. Businesses both big and small have been slowly embracing cloud services as a measure to reduce cost from buying Information Technology (IT) products as well as employment of IT staff.

Cloud computing models vary, an organization choice, will determine whether all or parts of it’s hardware, software and data will reside in the cloud or not (Crowe, et al., 2012). Now it is a question of own versus rent, the concerns worsen as Cloud Computing providers store client data outside their countries. El-Hoby, Salah and Suhaini (2014) argue that cloud services have several perspectives but they share the same core elements, namely: People, Procedures and Technology. Thus, while Crowe, et al., highlight cloud choices, El-Hoby, Salah and Suhaini, on the other hand, give system core elements which unless properly coordinated would raise substantial security and trust issues.

In a traditional computing environment, separation of networks and data was one way of enforcing security, since the organization had intranet and Internet facing networks within the company’s premises. The shift from traditional forms of computing to cloud computing has created benefits to companies who have relied on computing power for their operations (Woley, 2012). According to Cisco (2016) survey of cloud uptake, the yearly global cloud Internet Protocol (IP) traffic will reach 14.1 ZB (1.2 ZB per month) by the end of 2020, up from 3.9 ZB per year (321 EB per month) in 2015. This, therefore, means that in the next five years global cloud IP traffic will quadruple. However, despite such growth, security challenges within the cloud still persist, hence being an impediment to migration to the cloud.

Marsh, Basu and Dwyer (2013) argue that while protected systems are the backbone of an effective interconnected system, they are not client-oriented because they have exposed user’s information that was meant to be private to be shared by a chosen few, to the many. CSA (2016) highlights that information security threats need to be analyzed using Microsoft STRIDE, it include: spoofing identity (S), tampering with data (T), repudiation (R), information disclosure (I), denial of service (D), elevation of privilege (E). Although adequate security is more complex to achieve in a cloud than traditional computing infrastructure, organization policy should inform cloud security architecture design. It is therefore, important to addresses policy issues, because, the inherent security/privacy challenges facing the cloud not only emanates from outside but also from within the organization.

## 1.2 Problem Statement

Cases of hacking into individual e-mail accounts and organization servers have being rising with the growth of online lifestyle. According to IBM (2015) the threat landscape is evolving with unauthorized access incidents becoming more dominant, with sixty percent of all attackers being insiders. Similarly, Feldman (2012) observe that cloud computing is rife with history of leaks, both accidental and deliberate that has led to the recognition of the privacy risks of cloud deployment. Therefore, whether it is insiders or outsiders breaching data confidentiality in the cloud, such attacks occurs using stolen account credentials of a client. Thus, this challenge of stolen account credentials and lack of situational awareness on the client or system administrator side, when client account is accessed, informs this research.

This dissertation therefore, is aimed at designing a scheme whereby when an account is hacked, the first successful authentication triggers a six digit code to be sent to client mobile or email account for the second round authentication before accessing cloud data. Since the hacker does not have client mobile or e-mail credentials, access will be denied, thus, enhancing confidentiality. The proposed system will ensure better situational awareness as well as hardening it, hence, making it costly to obtain client data. In addition, it would detect insider breaches in real-time, therefore, becoming a better deterrence against the growing vector threats.

## 1.3 Research Objectives

The main objective of this research is to develop a scheme for enhancing cloud data confidentiality using authentication and encryption.

The specific objectives of this research are:

i. To analyze different types of security threats that affect data in cloud storage.
ii. To review merits and shortcomings of security models, architectures and algorithms used for cloud storage implementation.
iii. To develop a scheme for enhancing cloud data confidentiality using authentication and encryption.
iv. To test the proposed scheme.

## 1.4 Research Questions

i. What are the different types of security threats affecting data in cloud storage?
ii. How do the current security models, architectures and algorithms used in cloud storage implementation work?
iii. How can cloud data confidentiality scheme be realized using authentication and encryption?
iv. How can the effectiveness of the scheme be evaluated?

## 1.5 Justification

Cloud promises to deliver low cost computing power to majority of users, especially small and medium enterprises, who are yet to benefit from this model. The high costs of acquisition of hardware and software products in traditional computing, coupled with costly installation that follows such acquisitions, because of required skills, has been hindrance to companies. These costs have kept away majority of small and medium sized companies despite their eagerness to use computing power to leverage on their businesses.

Despite, the low cost factor, cloud computing is ripe with security challenges. According to Cloud Security Alliance (2016) in mid-2015, BitDefender had client usernames and passwords stolen, which was attributed to a security weakness in it's public cloud application hosted on AWS. Similarly, British telecom provider TalkTalk had multiple security incidents in 2014 and 2015, resulting in the theft of four million clients' personal information. These security challenges, therefore, is what the dissertation aims to address.

The proposed research analyzed different types of security threats that affect data in cloud storage. As such, identified challenges offered insights that informed development of a scheme for effective deployment of data within Cloud storage. This solution addressed lack of trust within cloud ecosystem, therefore, enhancing confidence and faith in the usage of applications available in the Cloud. This research has contributed to the existing literature on the Cloud computing storage by highlighting gaps that require further inquiry.

### 1.6 Scope

Confidentiality, integrity and availability are the three main ways of addressing data security threats within the cloud environment. Cloud data confidentiality is a challenging task to promise clients. Despite the challenge, this dissertation has proposed a scheme that provides an enhanced cloud data confidentiality by triggering an alert by sending six digit code through mobile or e-mail notification, which the client will use for the a second round of authentication before being granted access. Similarly, php mcrypt encryption will provide another layered security perimeter for efficient and secured data storage. The layered security strategy offered by the proposed system will address security and privacy challenges within the cloud environment. Thus, the system is aimed at curtailing breaches by internal as well as external unauthorized users, who may have stolen user account credentials, by means of having real time monitoring of access to the client accounts.

The challenges within Infrastructure as a Service and Platform as a Service will not be addressed in the proposed research, although this dissertation will discuss the general security breaches that cut across the three main cloud computing service models. In addition, the research will not address the legal aspects that could compel cloud service providers to ensure confidentiality of user’s information hosted in their servers.

### 1.7 Limitations

Limitations may be experienced in testing the scheme because it will be running in hybrid cloud, thus, it’s working in different deployment models for instance community cloud and public cloud may not be tested. Despite the above limitation, the researcher will design the system in a way that will cover the scope of the research while maintaining it’s relevance in meeting the intended research objectives.

# Chapter 2: Literature Review

## 2.1 Introduction

Security is an evolving concept whose requirements keep shifting as old vulnerabilities are addressed. Cloud security being one component of security is in a constant state of evolution due to an ever changing internet environment, hence need for a continuous awareness in order to mitigate new threats as they emerge. Cloud security models, architectures and algorithms were reviewed in order to highlight the shortcomings of the current cloud security implementations.

## 2.2 Security threats

According to Britt (n.d) cloud security refers to the protection of running applications, stored data and processing of transactions within the cloud, adding that the growth of attacks are in exponential factors. Thus, this calls for continuous awareness on how and when to secure systems against threats. NIST (2014) defines continuous monitoring as an ongoing awareness of information security, vulnerabilities and threats to enable risk based decision making. Similarly, Britt (n.d) observes that there have been more malware attacks in the last 18 to 24 months than in the last 18 years. While cloud services promises so many things, for instance agility, scalability and efficiency, its security elements in the Cloud is not being fully met. From the authors above, there is a growing need to secure the ever increasing numbers of endpoint devices used by users because of an ever rising online lifestyle. Thus, these security risks and concerns need to be addressed if users are to benefit from the cloud promise of low-cost computing.

Dahshan (2013) argues that security challenges need to be understood in relation to business chance and appetite for risk, at a times risk is compensated by opportunity. While security challenges in itself cannot hurt businesses, it’s exploitation is what is threat, Dahshan (2013) observes that threats come from: insecure programming interfaces, malicious insiders, shared technology vulnerabilities, data loss/leakage, account and service traffic hijacking, and unknown risk profile. The author, thus, notes that the exploitations of these weaknesses are what threaten the growth of businesses in the cloud environment. Therefore, the question is, are there better ways of addressing various concerns that threaten security in the cloud?

Gupta, Laxmi and Sharma (2014) affirm that specific service model is linked with some security issues, adding that the security challenges in the cloud could be thought first through the eye view of the Cloud Service Provider who in his/her belief claims to be providing secure services, while on the other hand through the eyes of the customer that is using this secure service. Balancing, therefore, data security concerns of customers visa vie cloud service provider guarantee is a challenge, because the cloud has increased the attack vector space. Of importance to this dissertation, therefore, is how these challenges can be addressed to enhance confidence in cloud services. Thus, in this section, various attack vectors will be looked into, including weaknesses brought about by how the services are offered and finally, challenges which have been moved forward to the cloud from the traditional computing model will also be examined.

### 2.2.1 Multi-tenancy

Multi-tenancy simply means sharing of resources by individuals or organizations, as Gupta, Laxmi and Sharma (2014) observe that a cloud model is developed for purposes of sharing of resources, memory, storage and computing. According to Ngo and Tran (2015) multi-tenancy is an indispensable to efficient and sustainable cloud-based systems. Similarly, Sura et al., (2015) attribute many cloud security complexities to multi-tenancy and open system architecture framework. Thus, while first and the second group of the authors agree on centrality of multi-tenancy in cloud computing, Sura et al., on the other hand, argue that it’s complexities and open system architecture creates vulnerabilities that can be exploited by hackers.

In the meantime, Seema and Shaikh (2014) observe that earlier organizations used their own data centres to store their data and it was physically separated from the data of another organization. The authors go further to state that this mechanism provides security to the data. Therefore, while Gupta, Laxmi and Sharma calls for pulling of resources to achieve a big objective in terms of computing and storage power, Seema and Shaikh, on the other hand, argues that separation of data resources was the true guarantor of security. Thus, from the above authors, individuals and organizations are in a dilemma between moving their data to the cloud which lacks physical separation of data or to retain them in their premises hence losing on the benefits of low cost cloud computing environment. In addition, multi-tenancy amplifies threats especially when an organization is sharing cloud resources with people with ill intent as well as from malicious workers employed by the cloud service providers.

Similarly, Crowe et al., (2012) go on to state that in a multi-tenant cloud environment where applications are shared by many companies, the challenges of data leakage is high, when compared to dedicated servers and programs serving an organization. In attempting to address the loopholes brought by multi-tenancy, Sura et al., (2015) proposed a secure multi-tenancy architecture which uses authorization model based on AAAS protocol, arguing that this will secure end-to-end multi-tenant sessions. Since the system was not implemented, it's benefits is yet to be tested.

Likewise, Ngo and Tran (2015) in their research proposed an innovative object-oriented architecture pattern which is used to develop multi-tenant web programs were maximum reuse and modularity is attained and applications are separated. The authors go further to state that their pattern would reduce time and cost to develop multi-tenancy system. Because it is a pattern and not a system to address challenges within cloud computing environment, the security issues still persist, hence, need for further remedies. Therefore, the question remains, is there a way of bringing physical separation of resources to applications in the cloud without necessarily going physical in the true sense, in order to mitigate challenges brought about by shared virtual applications or operating system environments in the cloud?

### 2.2.2 Insider Attacks

According to Gupta, Laxmi and Sharma (2014) cloud comptuing is a multitenant based model that is under the provider's single management domain. Similarly, Seema and Shaikh (2014) observes that cloud computing is a concept transformation in which computing power is relocated from organization premises to a cloud of computers. Thus, while Gupta, Laxmi and Sharma talks of having single management of a domain, Seema and Shaikh on the other hand, highlight the shift of resources from ownership to renting, therefore raising concern especially for organizations that have weak security policies and procedures. It even goes further for countries with weak or no legal framework to regulate the use of data within the cloud environment. Although some collaboration among subscribers and cloud service providers in management of data within the cloud infrastructure can guarantee some elements of security. The question still stands how can a malicious insider be detected?

### 2.2.3 Elasticity

Elasticity is the extent to which a system is able to adjust to workload changes by provisioning resources in an automatic way, such that what is provided match the current demand within the specified time (Gupta, Laxmi & Sharma, 2014). This therefore, implies that customers can increase and reduce their demand for cloud services without it affecting the provision of the same to other clients. This scaling up and down of resources raises concern, as Gupta, Laxmi and Sharma notes. The scaling means allocation of resources previously used by other tenants can be provided to a new client, which, however, raises privacy and confidentiality concerns, especially on how to protect previous users' identity signature in a program instance. It is thus, good to note that, despite the blessing brought about by elasticity of resources, the sharing aspect raises security concerns, which this research aims to overcome.

### 2.2.4 Outsider Attacks

According to Seema and Shaikh (2014) a cloud is a virtualized server pool which can provision the different computing power to their users. On the other hand, Crowe, et al., (2012) observe, the concentration of multiple organizations operating on a Cloud Service Provider's (CSP) infrastructure offer a more appealing target than a single organization. Therefore, while the authors talk of virtualized resources being provided by Cloud service Providers, this virtualization and usage by many organizations creates best target for attacks due to publicity such compromise would create.

Thus, the above arguments put into question the cloud delivery model. Gupta, Laxmi and Sharma (2014) observe that cloud encompass additional programming interfaces than private networks, hence, hackers and attackers have the advantage of exploiting the API flaw. This, therefore, raises the risk level of customer data in the cloud, hence requiring a remedy.

### 2.2.5 Governance

Governance is not an attack vector, but it is a contributing factor to the weakness being exploited by hackers within the cloud environment. Attacks against resources in the cloud could be mitigated if proper measures are put in place, both from the customers' perspective as well as cloud service provider's view. Thus, this therefore, calls for a structured governance system where each of the two knows clearly his/her responsibilities in management of the data in the cloud. In addition, it calls for subscribers to have a thorough understanding on where their data is resident, since it is only by their active participation in managing of the cloud resources can the challenges experienced within the cloud be minimized.

### 2.2.6 Data Breaches

Cloud Security Alliance (2016) defines data breach as an occurrence in which vital and private information is released, observed, stolen or used by unauthorized person. According to Samson (2013) data breaches are some of serious challenges to data in cloud. While CSA and Samson both agree on the importance of containing data breaches, a virtual machine side-channel, SQL injection attacks among other methods, have been used by hackers to extract encryption or decryption keys in use by other virtual machines on the same server. This attack which was traditionally used to attack machines within a connected environment has been brought forward to the cloud platform. This, therefore, informs us that some challenges from the traditional computing environment will eventually find their way to cloud computing, thus, making an already fluid cloud security riper with threats.

Samsom (2013) further argues that the countermeasures you put in place to address one can exacerbate the other; an illustration is data encryption, whereby losing your keys, also means losing your data. Thus, this therefore, calls on users to make tradeoffs between security and the information sensitivity to be stored in the cloud environment.

### 2.2.7 SQL and XML Injections

There are mainly two types of databases SQL (Structured Query Language) and XML. SQL and XML databases are highly useful for storing data from websites. SQL is command and control language for querying relational databases while XML is used to query XML databases. According to Weiss (2016) SQL injection attack sends mischievous commands to the database by sneaking through illegal means, adding that attacks against Sony Pictures, PBS, Microsoft, Yahoo, LikendIn and the CIA happened through this means. The author goes on to state that by far the most prevalent such channel is unsanitized input data. This, therefore, in essence signifies that SQL injection is a lethal weapon that can be employed by states as well as criminals to achieve intended objectives.

The injection attack is becoming a popular choice for hackers because it is a category of attacks that rely on injecting data into a web application in order to facilitate the execution or interpretation of malicious data in unpredicted manner. There are various forms of Injection attacks which comprise: cross-site scripting (XSS), SQL injection, head injection, log injection and full path disclosure. Injections are the most common and successful attacks on the internet due to their numerous types, large attack surface and the complexity sometimes needed to protect against them. Similarly, their success can be attributed to the concept that all applications require one form of input of data or another for them to function. Thus, the question is how can information leakage, disclosure and manipulation of stored data, bypassing authorization controls and client-side SQL injection be prevented?

## 2.3 Models, Architectures and Algorithms

In this section a review of the various models, architectures and algorithms for security in cloud computing data storage is presented. First, section 2.3.1 will concentrate on models; secondly, section 2.3.2 will delve on architectures and finally, section 2.3.3 will dwell on algorithms.

### 2.3.1 Cloud Data Security Models

Zoltan and Milan (2016) defines data security to mean self-assurance and reliability preservation of data processed by a company. The authors go on to state that by accessing cloud services and information through the internet, the importance of safety measures increase because data is at greater security risk. From the above statements, the authors allege that organization data is at risk because of it being accessed through the internet. NIST (2016) observes that cloud computing is offered in three services and four deployment models. The three main service models include: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), although others have come up with Security as a Service, Storage as a Service, Business Process as a Service (BPaaS) among others. On the other hand, the four deployment models have so far been identified: private, public, community and hybrid.

According to Rashmi, Sahoo, and Mehfuz (2013) the models form the nucleus of the cloud and they demonstrate certain key traits like on demand self-service, broad network access, resource pooling, calculated service and speedy flexibility. This section will concentrate on reviewing the security implications on service and deployment cloud models with respect to cloud data security models proposed by different authors.

### A. Service Models

#### i. SaaS Model

The SaaS model encompasses the provision of programs to a client or users as a service, on demand. Hashizume, et al., (2013) observes that these applications are normally delivered via the Internet through a Web browser. Flaws in web applications may create vulnerabilities for the SaaS applications, hence affecting data security. Similarly, the authors go further to state that attackers have been using the web to breach user's computers and carry out malicious activities such as steal sensitive information. Therefore, despite the easy of accessing applications via the various devices like mobile phones, public and private computers especially during this era of Internet of Things (IoT), security challenges found within any web application technology have made their way to SaaS cloud, hence, need for new approaches to address these threats. This is because SaaS cloud has inherited challenges emanating from traditional computing security risks as well as attacks that have come due to the internet.

Hashizume, et al. (2013) state that with the growth of mobile computing this has raised the threat level because data can be stolen through malware targeting mobile phones or tables, insecure Wi-Fi networks, device operating system flaws and insecure applications programming interfaces. It therefore, calls on cloud providers to find more secure ways of offering their services than transferring security challenges which were traditional common in organizations to cloud computing environment since it does not offer any better guarantee.

Zoltan and Milan (2016) have built upon standard cloud storage of three-level data security model in cloud computing which can be extended by proposing a forth level responsible for the data integrity check, which is done by use of Petri nets. The authors observe that Petri nets offer simplicity in discreetly simulating and understanding how the security model operates. The authors go further to state that Petri nets are mathematical formulations suitable to model system which encompasses of parallel components in mutual interactions, hence, provide better understanding of the changes of each step when securing data in cloud environment. Thus, the authors despite their claim on Petri nets model on assured data integrity, fell short of full system development, hence their claims could not be confirmed since it was only a simulation. The Figure 2:1 below shows Petri nets model.

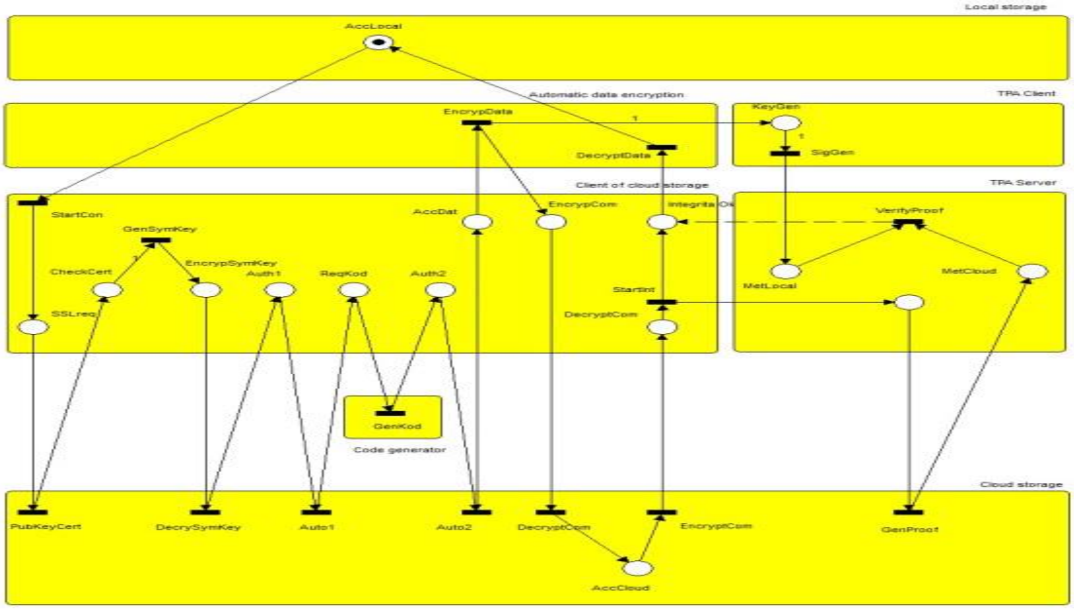


**Figure 2: 1: Cloud data security using Petri nets model (Zoltan & Milan, 2016).**

According to Harris (n.d) since one instance of the application runs on the cloud and many end clients are serviced, this brings advantages as well as raising security concerns for clients' data. From the client perspective, therefore, the need to invest upfront for this service is needless. SaaS service examples include: Netflix (video streaming), Google docs, acrobat.com, saleforce.com, Intuit QucikBooks online among others. The hosting of a single instance of an application lowers cost, thus, in this hosted application, apart from the Service provider, who else is responsible for security?

### ii. PaaS Model

This layer comprises of programs development tools which is encapsulated and offered as a service, upon which other higher levels of the service can be built. As Crowe, et al., (2012) observes a CSP provides its clients with development environment that aid in the creation of software that operates on the cloud provider's hosted infrastructure. Similarly, Harris (n.d) argues that the client has the choice to build his/her own programs, which run on the provider's infrastructure. Both Crowe, et al., and Harris point that the customer becomes key reference in terms of provisions of cloud services enabling him/her the flexibility of scaling the resources according to his/her requirements.

Since PaaS usually describes an additional level of services layered on top of IaaS, it sometimes confuses some clients, hence need to properly coordinate the two services in order to enhance security. According to NIST (2016) PaaS is whereby a customer can deploy, manage and run applications using a programming language and execution environment while IaaS is whereby a customer can provision and use processing, storage or networking resources. Therefore, PaaS is in general a higher level of abstraction than infrastructure. Some well known PaaS are: Google's App Engine, Force.com and LAMP platform (Linux, Apache, MySQL and PHP), Ruby among others.

Unlike SaaS and IaaS, PaaS rely upon a protected and dependable network as well as safe web browser. The PaaS application safety measures, constitutes of Security of the PaaS platform itself (that is runtime engine) and Security of client applications hosted on it (Hashizume, et al., 2013). Therefore, the question is this layering of resources within the cloud from SaaS, PaaS and IaaS creates confusion on who is responsible for the correct integration of these assets so that it does not act as a weak link? Thus, like SaaS, PaaS also brings data security issues due to it's nature of sharing of resources, which raises privacy and confidentiality concerns.

### iii. IaaS Model

In this model, service provider avail to customers the use of processing power, storage and networking capabilities over a network. According to Crowe et al., (2012) the cloud providers offer virtual data center of resources, for instance networking, computing resources, and storage resources. Similarly, the provider configures and manages their own operating systems and software and, to a great extent, scaling their programs and providing all the services required to run it. As Harris (n.d) notes that servers, storage systems, networking equipment, data centre space among others are pooled and readily accessible to handle workloads. Examples of this are: Amazon EC2, GoGrid, IBM cloud and 3 Tera among others. Thus, both Crowe et al. and Harris argues that CSP provides virtual data centres and being responsible for configuring and maintaining operating system, in these pooling of resources, the question remains, who provides/guarantees security?

## B. Deployment Models

### i. Private cloud

This cloud model is run exclusively in support of a particular firm. This can be situated in an enterprise data center or else hosted at a collocation facility that is perhaps owned by a third party, like a cloud provider. This model is intended to take advantage of elasticity and ease of managing cloud model, when it is setup, users can run their individual clouds.

### ii. Community cloud

The cloud infrastructure is shared by quite a lot of organizations and supports a precise community that has common interests, for example mission, industry partnership, or agreement requirements. This cloud may be administered by the community organizations or a third party and may perhaps exist on or off the premises.

### iii. Public cloud

The cloud infrastructure is offered to the general public or a large industry group. It may be owned by a private or public organizations or a combination of them. Thus, through the use of multi-tenancy solutions, shared storage infrastructure can service multiple users hence can create a weak security link in the provision of cloud services.

### iv. Hybrid cloud

NIST (2016) observes that a hybrid cloud encompasses of two or more cloud models (on-site private, on-site community, off-site private, off-site community or public) that stay as different entities but are bound mutually by consistent or proprietary technology that enables data and application portability. Similarly, Cloud Standards Customer Council (CSCC) (2016) argues that hybrid cloud offers the enabling capabilities to link environments, layers and resources such that it is seamlessly automated. CSCC goes on to state that since most enterprises are not ‘born on the cloud’, therefore most cloud resources typically need to be connected to significant on-premise IT systems. Thus, both NIST and CSCC observe that hybrid cloud provide unique virtual resources by combining on-premise IT systems and Cloud services, hence creating loopholes for attacks, because the merge may transfer some traditional computing vulnerabilities to the cloud computing.

In a nutshell, therefore, the security risk increases as you move from private cloud to public cloud, in addition, risk increases as you move from IaaS to SaaS. This is because as you become less in direct control of your data, so is increase in inherent risk. The Figure 2:2 below illustrates.

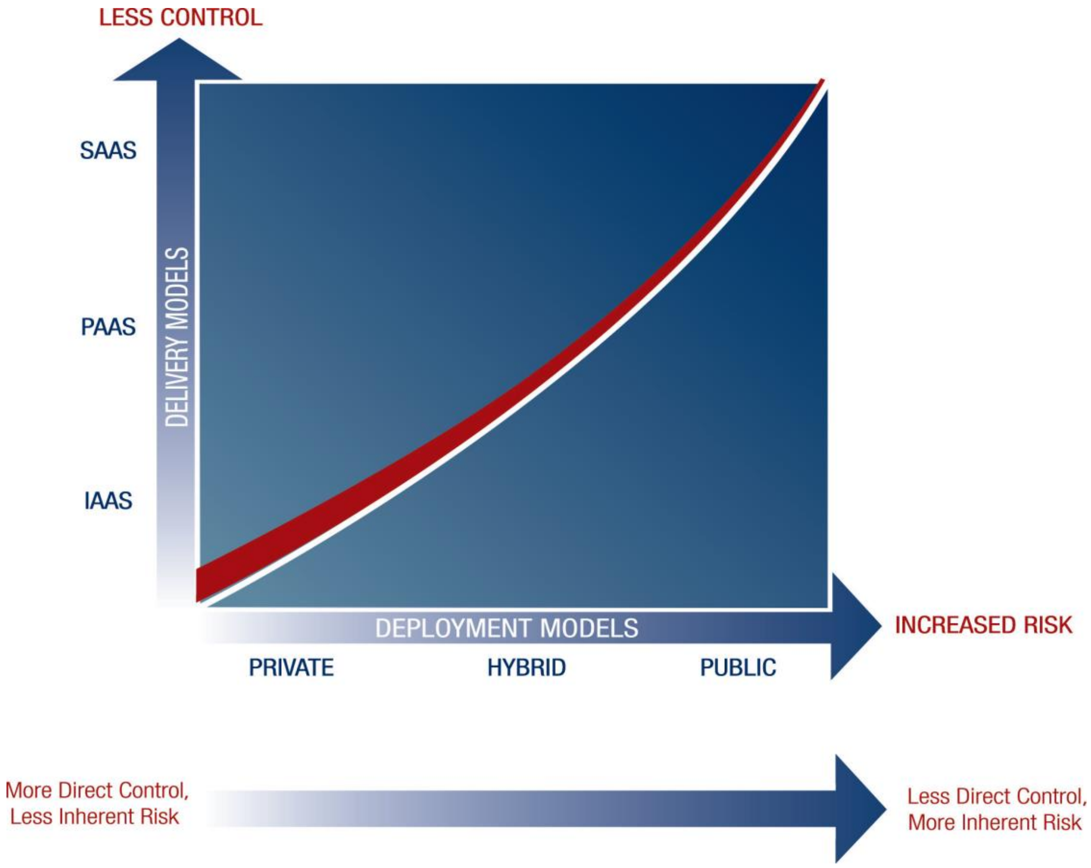


**Figure 2: 2: Cloud Service Delivery and Deployment Models Risk Nexus (Crowe, et al., 2012).**

### 2.3.2 Cloud Security Architectures

Naresh and Sai (n.d.) defines cloud architecture as a system of applications involved in the delivery of cloud computing, normally involving numerous cloud components communicating with each other over a loose coupling means such as a messaging queue. In the meantime, Roy and Rishabh (2015) define cloud computing architecture as consisting two parts: the front and the back end, which link to each other through a network. The front end is client/users side while the back end is the cloud segment of the infrastructure. Similarly, according Dogra and Kaur (2013) cloud computing architecture can be separated into four parts which include: the hardware/data centre layer, the infrastructure layer, the platform layer and the application layer.

From the above authors all agree that cloud architecture entail various sections which are integrated in order to make available seamless services to clients. Therefore, this, calls for proper integration to avoid it being the weakest link in cloud security chain. The Figure 2:3 show an illustration of architecture.

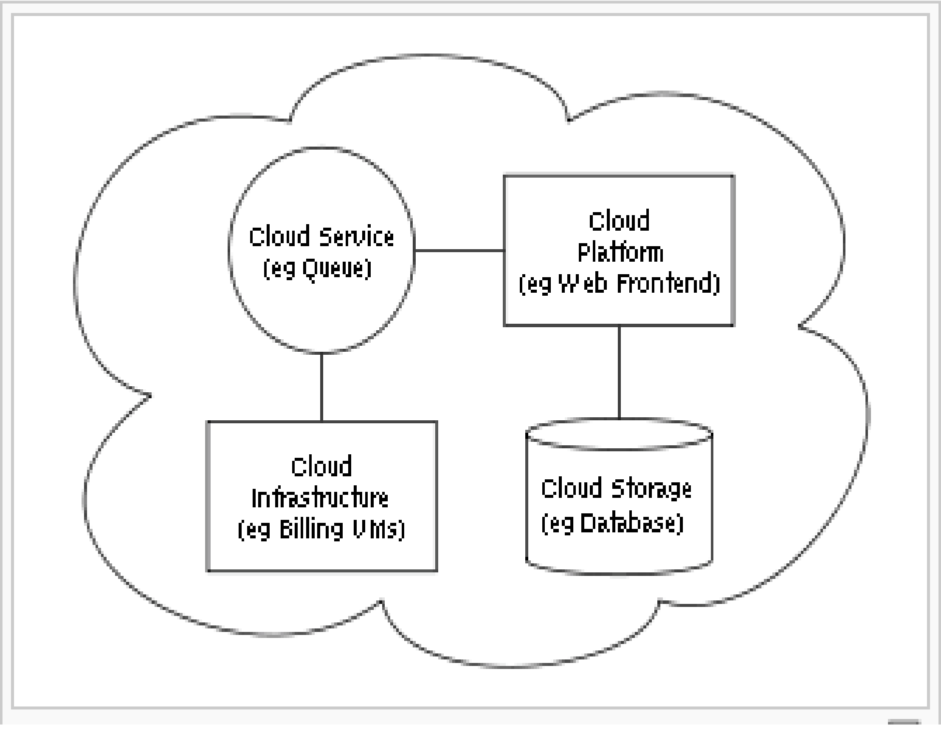


**Figure 2: 3: Basic Cloud Architecture (Naresh & Sai, n.d).**

In an attempt to address cloud computing challenges, Theodoros, Angelos and Dimitrios (2016) offered multi-layered architecture based on defense zones to classify data and provide protection using Intrusion Detection System (IDS), honeypots and firewalls in cloud. In their proposed system, the authors did not specify whether they were addressing confidentiality, integrity and availability, thus creating a gap. Similarly, Amir, et al., (2012) suggested the use of Multi Agent system (MAS) architecture which they claimed is critical to ensure confidentiality, correctness assurance, availability and integrity of collaborative cloud storage data environment. Likewise, the authors argue that by using of a number of agents interacting with each other and exchanging messages across a network security is ensured. Thus, the authors above call for collaborative entities in trying to address cloud security, which brings about complexity, therefore, becoming a detrimental to the systems adoption. The Proposed collaborative functional layers are shown on Figure 2:4.

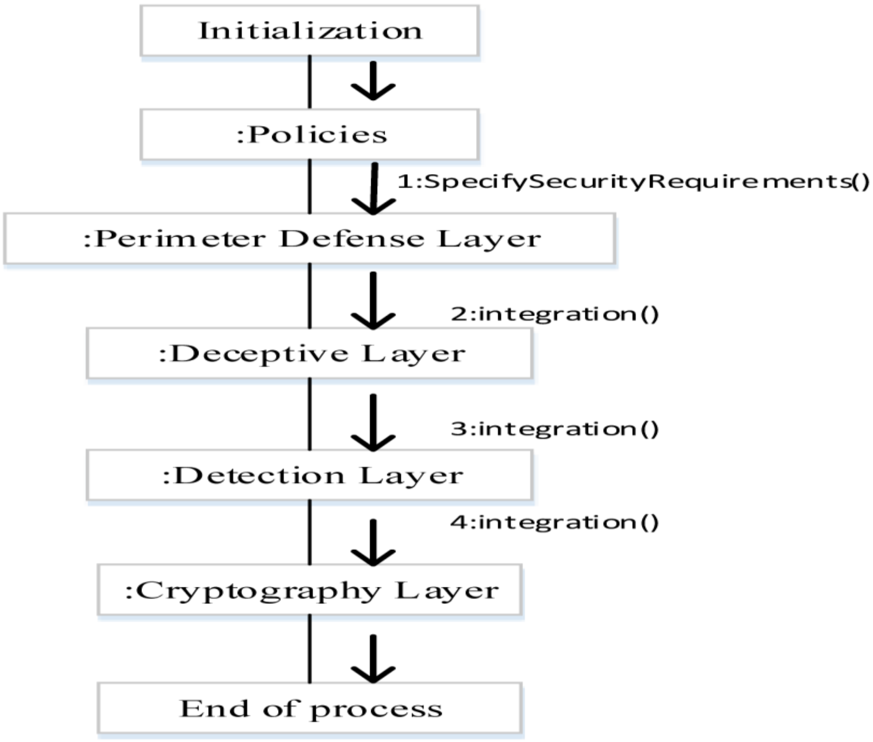


**Figure 2: 4: Collaborative Functional Layers (Theodoros, Angelos & Dimitrios, 2016).**

Elsewhere, Nilesh and Rajesh (2016) have proposed secured architecture for cloud service provider for mapping different security issues related to authentication and data stored on cloud. In addition, the authors’ stated that One Time Password (OTP) for authentication of user, hashing for checking data integrity while encryption will be used to maintain data confidentiality. They went further to argue that the proposed cloud architecture is more efficient because it uses efficient hashing algorithm which maps preimage attack and collision attack, and called for future work to concentrate on the design of hashing algorithm for media files. This limitation on their system can act as the weakest link in cloud architecture security provision.

Despite the proposals by various authors above, cloud computing security being an evolving concept cannot be permanently addressed, as Theodoros, Angelos and Dimitrios (2016) agrees that although they proposed security architecture to mitigate threats, the vulnerabilities and vectors of attacks continue to exist. This, therefore, means the failure to implement proper cloud security architectures within any Cloud storage setting would create a backdoor for hackers and malicious insiders to exploit leading to exposure or loss of data. Since cloud computing focuses on automation, resource sharing among businesses, it therefore, implies that moving to the cloud should be married to the business strategy in order to offer maximum benefits to the organization as it balances between security challenges and opportunities offered.

### 2.3.3 Cloud Security Algorithms

According to Tirthani and Ganesan (n.d) Cloud Computing is a technology where the clients can use high end services in form of applications that reside on different servers in addition to data that can be accessed globally. Accessing of services over open architectures of the internet has it's drawbacks, if proper security is not implemented to enable secure access. Therefore, the need for cryptography comes in handy. As Tirthani and Ganesan (n.d) observes that encryption/decryption is the science of securely transmitting and retrieving data using an insecure channel. The authors went on to propose non breakability of Elliptic curve cryptography for data encryption and Diffie Hellman key exchange mechanism for connection establishment. The authors' proposed an architecture that uses a combination of digital signature algorithm of Diffie Hellman and Advanced Encryption Standard (AES) encryption that would guarantee confidentiality. Despite the authors proposing Diffie Hellman and AES encryption, it's implementation and comparison with different algorithms were not carried out hence their proposal fell short. This section, therefore, will look at various algorithms and how their implementations in the cloud will enhance security and also their drawbacks.

#### A. Shamir Secret Algorithm

Shamir Secret sharing is a concept whereby a secret key is divided into parts, giving every member its own single piece, where a number of the pieces or all of them are required in order to rebuild the secret (Palande et al., 2015). The authors further observe that relying on all members to mutually combine the secret may not be practical, hence, the need therefore, to sometimes use any of the k pieces of the algorithm to recreate the original secret.

The authors, therefore, propose Self-Destructing Data System (SeDas) whereby data images become destroyed after a client-specified time, devoid of his/her involvement, in accessory, the decryption key is destroyed after the client-specified moment, hence, damaging all data images simultaneously and turning them indecipherable in case of hacking. This feature is valuable especially for organizations that handle sensitive data that are sometimes prone to cyber attacks. Thus, the authors see the concept as viable both in terms of usage as well as meeting all the privacy-preserving goals.

In Mathematical terms, the aim is the division of data D into n parts, such that D1,..........., Dn in such a means that the familiarity of any *k* or more D*i* parts makes D easily computable. Similarly, an awareness of any *k*-1 or fewer D*i* parts leaves D totally undetermined. This proposal is called (*k*, *n*) threshold design. If *k* = *n* then all members are needed to recreate the secret. The central thought of Shamir's threshold method is: two points can sufficiently define a line, three points can be used to form a parabola, while four points can recreate a cubic curve and so on. That is, *k* points can define a polynomial of degree *k* – 1. The Figure 2:5 shows.

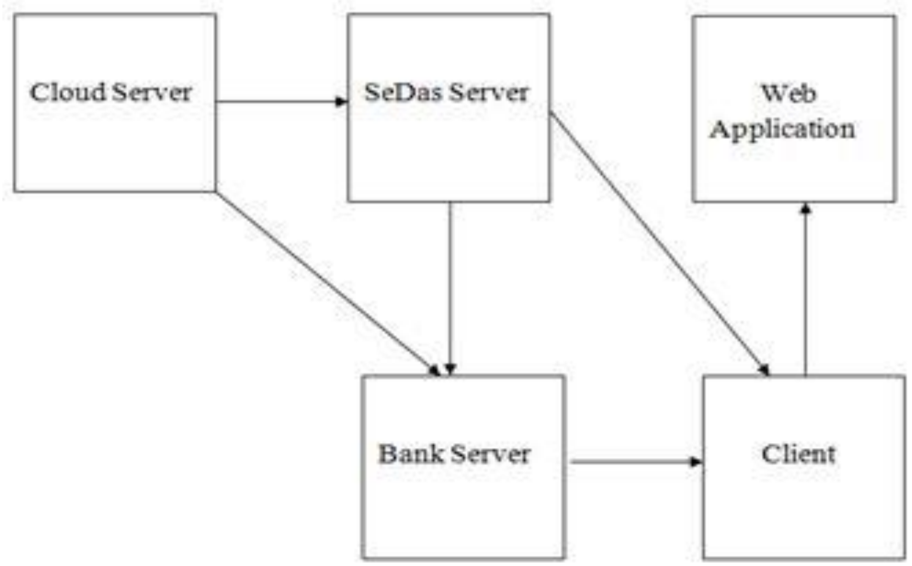


**Figure 2: 5: System Architecture of SeDas (Palande et al., 2015).**

According to Paritosh et al. (2015) Shamir's secret sharing algorithm uses a polynomial function method which alleges that even with complete familiarity of (k–1) clouds, the service provider will not have any awareness of the secret value. The authors further argue that hackers need to recover all the information from the cloud providers to be familiar with the authentic value of the information in the cloud. This, therefore, means that for cloud data, that has been shared among five cloud providers, hacking one cloud may be easy but continued attempt to hack four more is not only hard but labour intensive, hence, chances of success reduces completely, thus, guaranteeing data security. Therefore, the authors despite proposing movement to the clouds owing to its capacity to reduce security challenges that affect single cloud clients, the framework fell short of addressing the current risks, since there was no development and testing to ascertain the claim.

### B. RSA Encryption Algorithm

According to Sengupta (2015) RSA algorithm has been named based on three scientists at MIT that is Ron Rivest, Adi Shamir and Len Adleman in 1977. The author states that RSA applies public key approach for encryption and private key for decryption as required by asymmetric key encryption. It is an old encryption/decryption system which may fail in this era of cloud computing because of the advancement of computation power. The author thus, suggest a hybrid RSA encryption algorithm which makes the data difficult to decrypt by the attacker, arguing that this proposed method will minimize man in the middle attack during the transfer of data in the cloud system.

Thus, the proposed hybrid RSA encryption technique provides higher level of security than only RSA algorithm. This is because in comparison with original RSA model, the number of key generation exponents has been increased in the proposed hybrid RSA hence improves reliability of the cloud computing environments. The author showed the main drawback of the hybrid RSA is the complexity of the hybrid algorithm which includes two phased encryption.

Similarly, Masthanamma and Preya (2015) proposed an efficient data security model in cloud computing by means of RSA encryption algorithm. They proposed RSA algorithm which will be implemented in three parts which is key generation, encryption and decryption, whereby a plain text block is taken as M and cipher text block is taken as C, using the formula $C = M^e \bmod n$. Where e = encryption key and decryption formula $M = e^d \bmod n$. The authors highlighted some key challenges of their proposed system among them are drawbacks in fake public key algorithm, complexity of key generation and speed is low. They noted that future research should focus on longer encryption key with symmetric cipher so as to solve the symmetric key distribution problem. This, therefore, informs us that, despite the benefits derived from RSA algorithm still challenges persist in guaranteeing data security in the cloud.

Meanwhile, Suganya, Boopal and Naveena (2015) argue that several encryption implementations have been tried in attaining data security in the cloud, with mixed results evidenced by leakage of information from cloud providers including big organization like google, facebook among others. The authors propose multi-prime RSA algorithm in the central layer ahead of the data being stored in the cloud, adding that as soon as an authorized client requests the information, it is decrypted before providing it. In their proposal, the authors argue that multi-prime RSA algorithm uses randomly selected prime numbers to create public and private keys which the client can use to retrieve data from user's environment using private keys. They suggest that future research should look at a hybrid algorithm with security-as a service so as to achieve better security.

It is therefore, important to note that despite proposals by Sengupta, Masthanamma & Preya and Buganya, Boopal & Naveena cloud services still remain vulnerable to compromise, hence, the need for a better algorithms that will fit into the planned cloud computing implementation.

### C. Symmetric Key Block Cipher Algorithm

Symmetric Key encryption is divided into stream and block ciphers (Sunil & Manu, 2015). They proposed triple Data Encryption Standard (3DES) which is considered DES three times. They further observe that cryptography is used for secure communication in the presence of third parties to maintain information securities as in confidentiality, verification, data reliability, access control and non-repudiation. This, therefore, highlight the need to employ cryptography in securing cloud data since it involves various actors within the cloud domain, because it provides end to end information security over unsecured communication networks.

Similarly, Sunil and Manu (2015) go further to state that by simply extending the key size from 56 bits to 168 bits (that is 56 x 3 = 168) makes it resistant to brute-force attack. In encryption, the algorithm uses permutation to create 16 48-bit sub keys, one intended for every sequence with an overall 56 bit key. In symmetric key encryption identical key is used to encrypt as well as decrypt data. To decrypt, the same algorithm is used but the order of round keys are in reverse order. The disadvantage of triple DES is slow than other block encryption methods but its reliability due to longer key length reduces many attacks which can be experienced in the cloud. Thus, slowing of the network is still a challenge which may require a remedy.

### D. Multilevel Encryption Algorithm

According to Khan and Tuteja (2015) safety measures of data consist of three points that is: accessibility, privacy and reliability. This, therefore, means that in addressing security challenges in the cloud, the three points are important in guaranteeing data protection. The authors proposed a system that employs multilevel encryption and decryption to provide extra security for cloud storage. It thus, implies that, an algorithm that can address the three concerns is what is missing in the current cloud architecture and algorithm implementation.

In their proposed system Data Encryption Standard (DES) and RSA algorithm is used to create encryption when client uploads text files into cloud storage and inverse DES and RSA algorithm to generate decryption when client download file from the cloud. According to Khan and Tuteja (2015) in encrypting data, DES takes a 64-bit plaintext and creates a 64-bit cipher takes, while during decryption a 64-bit cipher text, creates a 64-bit plaintext using the same 56-bit cipher key for both the encryption and decryption. Similarly, RSA algorithm uses two exponents, e and d where e is public and d is private. Let plaintext be M and C is cipher text, then at encryption

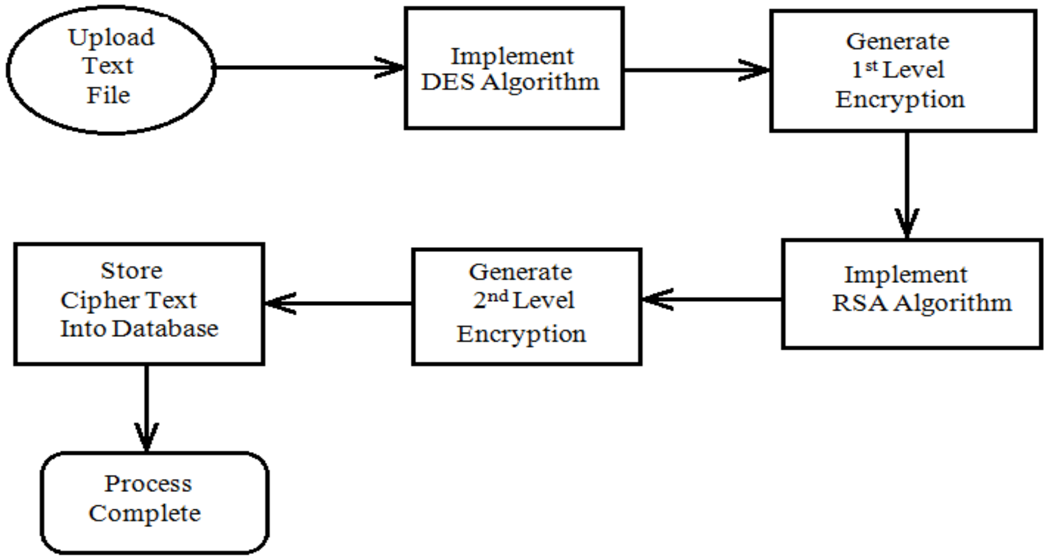
$$C = M^e \bmod n$$

And at decryption side

$$M = C^d \bmod n.$$

Where n is a very large number, created during key generation process.

This is because according to the authors the single level encryption may be cracked by hackers. Thus, the key issue is therefore, to provide a multilevel encryption control in order to harden the system for attackers. The proposed multilevel encryption is shown in Figure 2: 6 below.



Upload Text File
Implement DES Algorithm
Generate 1st Level Encryption
Implement RSA Algorithm
Generate 2nd Level Encryption
Store Cipher Text Into Database
Process Complete

**Figure 2: 6: Block Diagram of Multilevel Encryption (Khan & Tuteja, 2015).**

Similarly, Nigoti, et al (2013) observes that in the current systems no more than single level encryption and decryption is applied to cloud data storage. The authors, therefore, point that the continued use of single level encryption and decryption of data in the cloud will continue to cause concern among users. The authors proposed multilevel encryption promises to reduce data being accessed by an unauthorized user. As Khan and Tuteja (2015) observe that although a hacker gets the data by coincidence or deliberately, he must have to decrypt the data at each level which is exceptionally complicated task without a valid key. The drawback of the proposed system is that it is time consuming in terms of computation. The use of DES and RSA in encryption and decryption creates complexity which in itself is a drawback. Therefore, the authors, Khan and Tuteja as well as Nigoti, et al all agree on the need to use a multilevel encryption as a way of hardening the system for hackers and malicious people.

### 2.3.4 Sample System on Cloud Authorization Access

Cloud authorization is key in this era of rampant breaches of servers by malicious individuals as well as state sponsored attacks. As Sura, et al (2015) observe numerous cloud security complexities is a concern as a result of it's open system architecture. As a response to these challenges, the authors proposed a secure multi-tenancy architecture using authorization model based on Authentication Authorization and Accounting Secure (AAAS) protocol, adding that by using cloud infrastructure and access control numerous cloud information and services can be provided by their suggested authorized system. Similarly, Bajwa, Himani and Sandeep (2015) proposed a model based on the protection of the data by the owner which is achieved by encryption, obfuscation, HMAC and dual authentication and access management technique. The authors go on to state that encryption and obfuscation method is used to guard data during transmission as well as at rest, adding that during transmission of data, reliability plays a vital function, urging the use of hash based message authentication to enhance data integrity.

The model proposed by Bajwa, Himani and Sandeep consists of two keys parts that are: the first stage is uploading and the second stage is downloading. The first phase encompasses: key generation and maintenance, classification of data, data integrity, encipher and indexing. Key generation and maintenance is a function that is carried by third party as Bajwa, Himani and Sandeep (2015) observe that third party recreates the symmetric key and gives the key to data owner for a further process, adding that the data owner divides the keys, keeps one key and store the remaining for future use. The authors go further to state that the data owner encrypt these two keys by passcode and then sends to the third party, where they are kept and accessed when needed. As a result Yangqing and Jun (2015) emphasize that key security was essential for authentication security, since authentication was to identify authenticity of identification, confirming an entity was the entity that was declared. Data which is classified into type 1 and type 0, whereby type 1 is alpha numeric while type 0 is numeric. Despite, classifying data the authors did not give any criteria for that classification. Subsequently, Bajwa, Himani and Sandeep (2015) argue that data owner identifies the type of data and indexes it, if type 1 then encryption occurs, otherwise obfuscation is used. The authors goes further to state that prior to the data being uploaded to cloud, hash based message verification code HMAC is generated so as to verify data confidentiality throughout the transmission of data to cloud. The Figures 2:7, 2: 8 and 2.9 below illustrate.

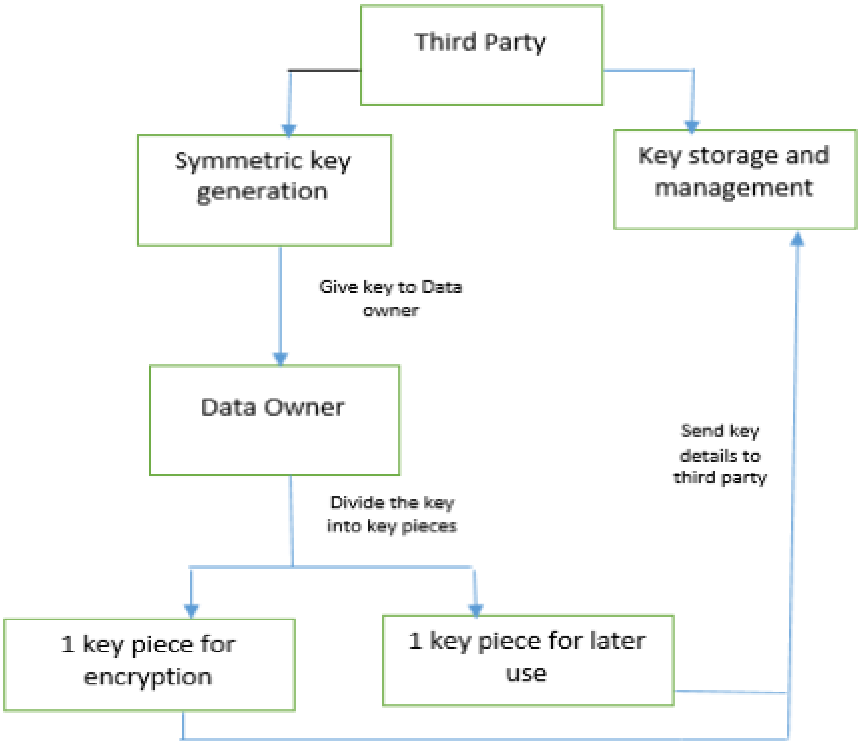

Third Party
Symmetric key generation
Key storage and management
Give key to Data owner
Data Owner
Send key details to third party
Divide the key into key pieces
1 key piece for encryption
1 key piece for later use

**Figure 2: 7: Key Generation and maintenance (Bajwa, Himani & Sandeep, 2015).**

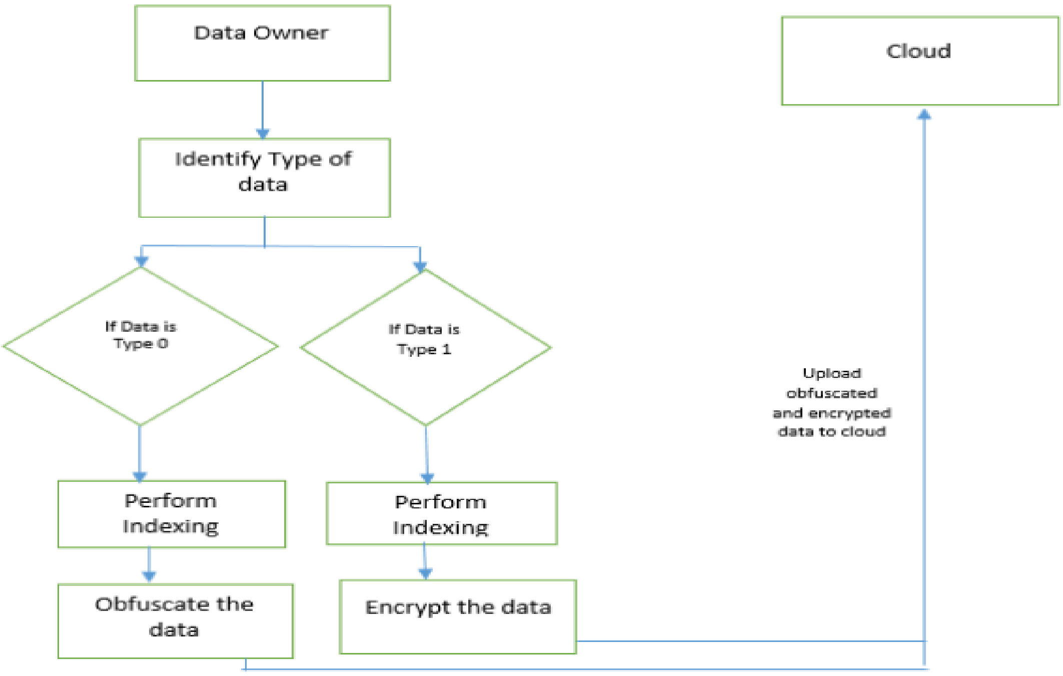


**Figure 2: 8: Encipher and Indexing (Bajwa, Himani & Sandeep, 2015).**

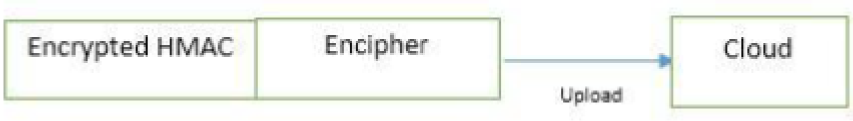


**Figure 2: 9: HMAC Generation for Data Integrity (Bajwa, Himani & Sandeep, 2015).**

Phase two is downloading which consists of dual authentication and access management and HMAC verification. According to Bajwa, Himani and Sandeep (2015) data is secured by having the authenticated user, first get role to access the cloud data before getting permission from the data owner who after verifying the user, he/she issues a digital signature and user id which the user will use to access third party, which after verifying gives corresponding keys for the user to decrypt the data. Thus, HMAC is generated and matched before and after downloading, if it is same then data integrity has been maintained. The Figure 2.10 illustrate.

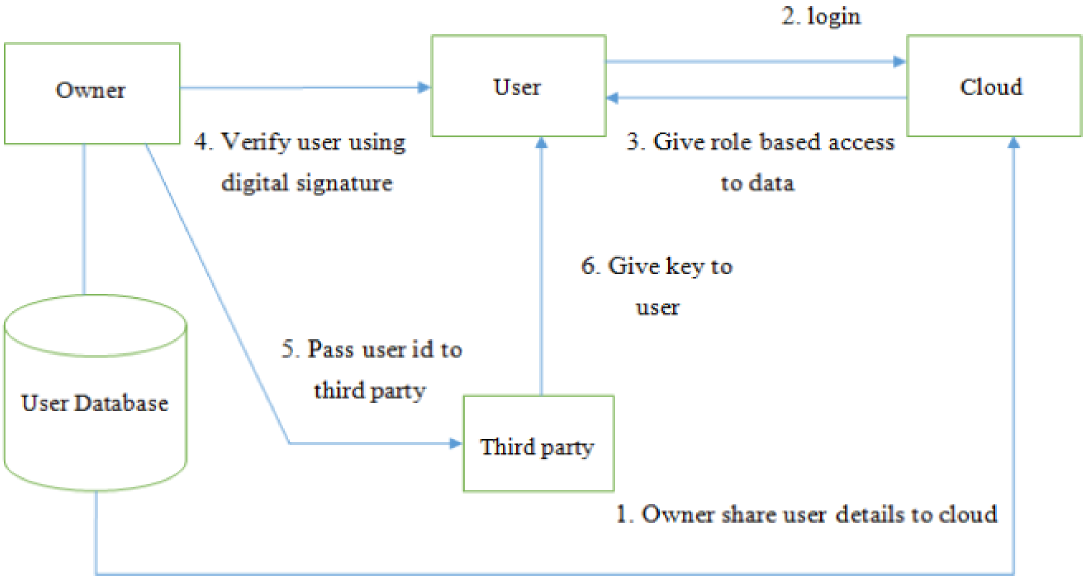

2. login
Owner
User
Cloud
4. Verify user using digital signature
3. Give role based access to data
6. Give key to user
5. Pass user id to third party
User Database
Third party
1. Owner share user details to cloud

**Figure 2: 10: Dual User Authentication (Bajwa, Himani & Sandeep, 2015).**

Finally, while Sura, et al pointed on open system architecture complexities which translate to challenges, Yangqing and Jun, on the other hand, called for key safe keeping. Consequently, Bajwa, Himani and Sandeep despite their proposed model called for future work to concentrate on adding additional security parameters in order create more protected and efficient model. Thus, the authors are of the view that because of extra components required for cloud computing to function like virtualized hypervisor machines, efficient networks, data storage concerns among others, this increases complexity, therefore, becoming a major security challenge which can be mitigated with efficient access management methods.

### 2.3.5 Sample System on Cloud Security Architecture

According to Mrudula and Chandra (2015) cloud computing is a concept of dispersed computing virtualization master plan, which offers computing power, for instance: hardware, software and database on demand, to physically distant clients, using the internet. The authors, went further to argue that one benefit for the enterprises is the reduce cost of new software or hardware infrastructure, which leads to enormous financial benefits to the small and middle level organizations. So Jingxin and Xinpei (2012) observe that the demand of data protection continue to increase, more so in hybrid cloud computing model, because it provides greater flexibility. Similarly, Amir, Rodziah, Rusli and Masrah (2012) calls on cloud providers to implement efficient security measures because of the number of assets within the cloud, such as data, user, technologies and business transactions. This call for secure services is not being met fully, as Jingxin and Xinpei (2012) observes that the challenge of securing client’s data in the hybrid cloud is still a key factor in limiting it’s adoption. The figure 2:11 below shows hybrid cloud.

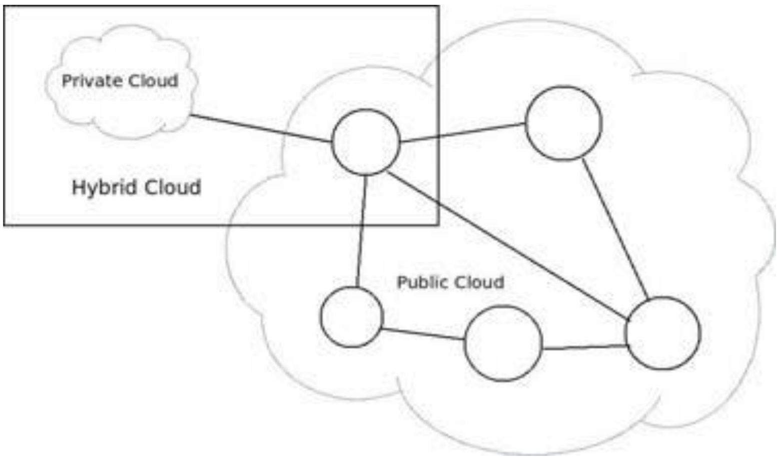


**Figure 2: 11: Hybrid Cloud Computing model (Jingxin & Xinpei, 2012).**

In an effort to improve acceptance of cloud services, Mrudula and Chandra (2015) adopted Jaidhar et al scheme by proposing an improved mutual authentication scheme which is light weight in both client and server side, adding that the new method is resistant to every main cryptographic attacks, for instance: vulnerability to offline password guessing, impersonation, user/server masquerade, framing of session key by adversary and failure to resist parallel session attacks among others. Accordingly, the authors illustrate that Jaidhar, et al scheme has three stages which is registration, login and authentication which is moment bound ticket based verification for cloud environment by means of smart cards. By their analysis, they came to conclusion that Jaidhar, et al used 1872 hash operation while theirs used 26 hash operation, in addition, since Jaidhar, et al used symmetric encryption, exponentiation and hash operations it consumed more computational resources since the proposed system uses only hash operations. In comparing the processing power on client side, Jaidhar, et al observed that it requires 7 hash, 1 exponentiation, 2 encryption operations which is equal to 7 + 600 + 2(60) hash operations = 727, in comparison to only 12 hash operations utilizing XOR in the proposed scheme, reducing it significantly (Mrudula & Chandra, 2015). Despite, utilization of less computational power on both the client and server sides, it's ability to resist various cryptographic attack vectors, the authors fell short of testing the system to ascertain other vulnerabilities.

### 2.3.6 Sample System on Cloud Security Algorithm

Prabu and Vasudevan (2016) observe that providing protection to the client data is a major issue in cloud computing, arguing that for user to effectively use these services, cloud customers require better security solutions that offer ease of storage and retrieval of data. Similarly, Vishwanath and Aniket (2014) argues that security is one of the most tricky undertaking to implement in cloud computing. Equally, Neha, Ajay and Rajesh (2014) notes that there are many security challenges in cloud computing which occurs predominantly during the time of transmission of data, which include: encryption, separation of duties, location of data and intrusion detection and prevention. The authors go on to observe that the sharing of cloud infrastructure may perhaps lead to confidentiality concerns, arguing that where data is located influences the privacy obligations. Thus, all the above authors have agreed that the common denominator slowing the migration to cloud by organization holding sensitive data is confidentiality challenges within the cloud environment.

To address these challenges brought about by cloud computing, Vishwanath and Aniket (2014) proposed a hybrid encryption algorithm using RSA and AES algorithms for providing user data protection in the cloud, adding that the two algorithms generates three keys: public key for encryption, private keys and secret key for decryption. According to the authors after uploading the data, it is stored in an encrypted form and can only be decrypted by private and secret key of the client, thus, ensuring that data is very secure in the cloud. In addition, the proposed system which consists of two modules: upload and download modules, if a client wants to download data, he/she will specify the filename to be downloaded and also AES secret and RSA private key which is kept by the client. While upload module consists of: authentication, upload, key generation and encryption; download module, on the other hand consist of: decryption and download. The Figures 2:12 and 2:13 below show the upload and download processes of the proposed system.

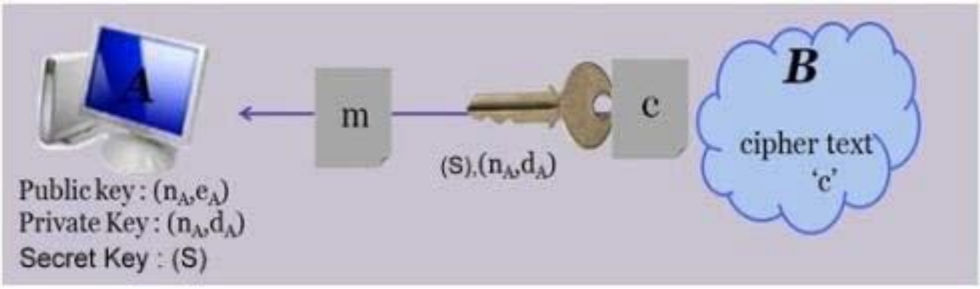


**Figure 2: 12: Data Uploaded in Cloud (Vishwanath & Aniket, 2014).**

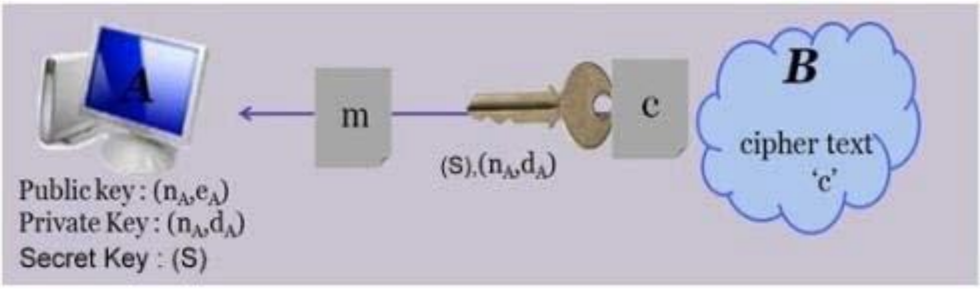


**Figure 2: 13: Data Downloaded from Cloud (Vishwanath & Aniket, 2014).**

### 2.4 Proposed Work

The proposed framework is a system that will use enhance cloud data confidentiality using authentication and encryption. The concept of authentication and php's mcrypt encryption algorithm will be designed on client-server model and will be anchored on both the virtualization hypervisor (Type 2) within the SaaS and PaaS layers. Firstly, the client facing part of the application for instance Graphic User Interface (GUI) will being hosted on application layer of OSI model, while it will also sit on SaaS stack of cloud infrastructure.

Secondly, the system application server and database will reside within the PaaS layer of the cloud environment. Similarly, the Infobip API gateway has been employed to enhance ease of integration of the proposed system with different pieces of software enabling it to utilize sender ID provided by Safaricom to sent mobile or e-mail alert notification in real time to client to further authenticate himself/herself or system administrator when an account is hacked into. This would add to the layered security implementation strategy, which will guarantee adequate security and practical efficiency in the cloud storage, thus, enhancing data confidentiality.

Thirdly, the proposed solution is also a candidate for SaaS because it is a 'vanilla' offering. According to Kepes (2017) 'vanilla' offerings, is where what is offered is to a great extent undifferentiated, meaning that it includes, for instance e-mail, where various rivals adopt the similar software in particular because it is indispensable for doing business, since it does not by itself offer a strategic advantage. Similarly, it is good to be in SaaS because the application has significant need for web or mobile access, in accessory it will enable real time alert when attempt to access into client account is being carried.

On the other hand, PaaS is ideal for application server and database because it will require integration with some web services as well as the use of common databases. This layer is also good because at some point the applications will require processing of real time data. Similarly, the API gateway has been employed to make it easy to be deployed across a wide range of platforms. Consequently, in addition to resolving security and privacy threats in the cloud, the application can also be extended to offer authentication using biometric features especially for clients who may require enhanced identity management mechanisms.

Finally, the proposed scheme will consist of three major modules: administrative module (for adding, deleting, updating and searching of users), User module (GUI used to interact with clients) and encryption/decryption module (allows for encryption/decryption using mcrypt algorithm). Conceptual Architectural framework has three layers which include user, security and cloud storage layers. The Figure 2:14 below shows the layers of the proposed solution.

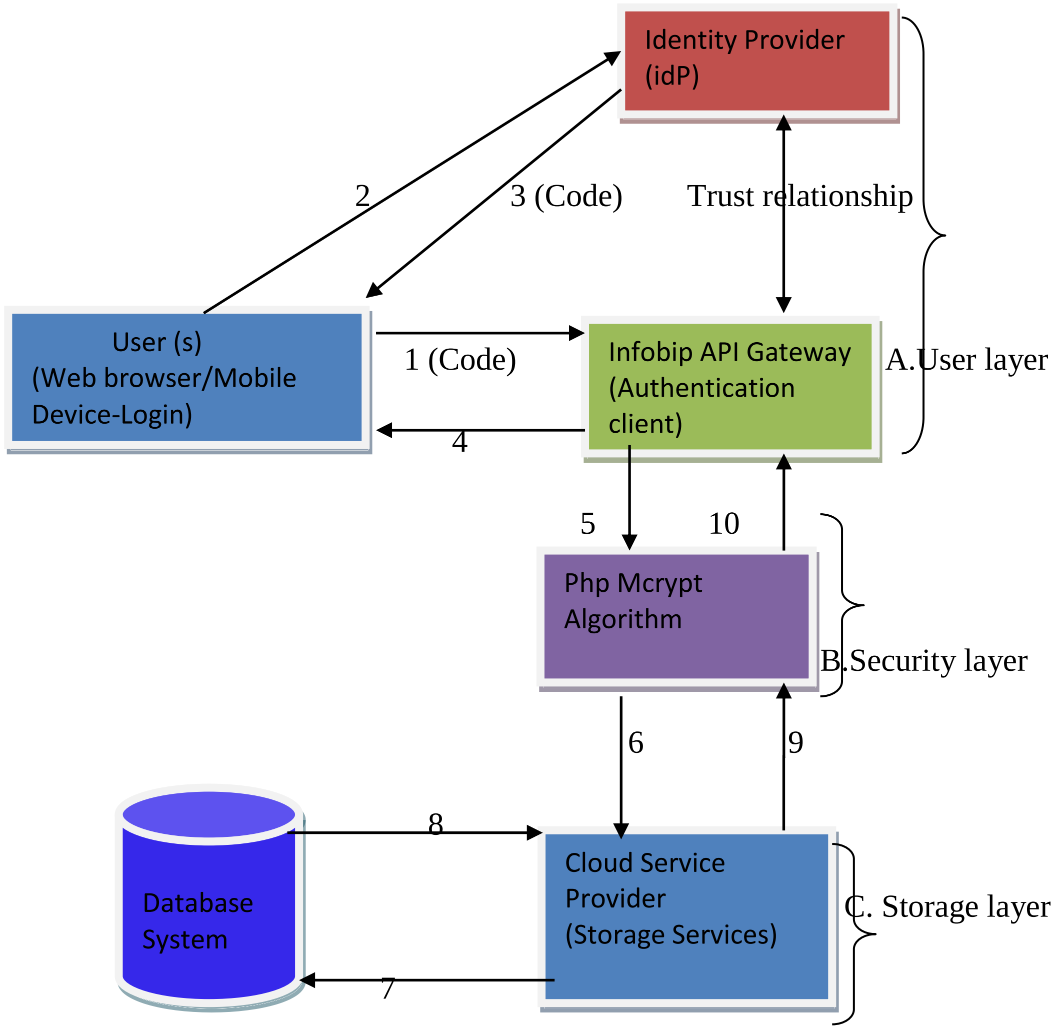


**Figure 2: 14: Conceptual Architectural Framework.**

### A. User layer

The user layer is responsible for session login and identity provider management. As the figure 2:14 shows; when the user logs into the system, the credentials (i.e. username and password) are forwarded to identity provider who verifies to ascertain the authenticity. Once verified, the user receives a code through mobile or e-mail notification for the second round authentication, before being granted access to proceed to security layer. If the client is a new user, he/she is supposed to fill his/her registration information and submit the same for processing. The two round authentications is to address the concept of low hanging fruit that encourage hackers to break into system, thus, enhancing cloud data confidentiality.

In addition, the API gateway will provide support by integrating in-house systems that offer management of clients/users accounts as well as management of seamless communication with partner organizations. The gateway will provide the runtime engine for API transfer of services as well as a distinct set of infrastructure that will support many domains. Finally, the API gateway is to strengthen security within the edges of the system by providing efficient integration mechanisms.

### B. Security layer

Php mcrypt algorithm provides the encryption of cloud data since its implementation will enhance cloud data confidentiality, therefore, enhancing security. Giorgio (2017) observes that the use of CBC (cipher block chaining) uses the result of the encryption of block N in the computation of the encryption of block N + 1, so that two equal blocks are effectively mapped to different encrypted versions. This therefore assures cloud data confidentiality since during decryption, an initialization vector is required, otherwise it renders the output non predictable even for perfectly identical plain text. According to Giorgio (2017) in symmetric cryptography, the key for encrypting and decrypting data is the same and is shared between parties while being kept secret. The author goes to state that despite encrypting and decrypting data, mcrypt extension also generates configuration and reflection of algorithms like the length of their keys.

### C. Storage layer

The Storage layer serves cloud data after the user as met the required permissions and roles to access the resource, after providing his/her proper credentials. The storage of data in different servers enhances security in case whereby unforeseen circumstances like floods or earthquake occur hence will provide of guarantee security of data in such events.

## 2.5 Summary

Cloud Computing has promised the concept of shrinking and expansion of resources in a way that was not thought for before. This shrinking and expansion of resources according to users' demand is breathing life to small and medium sized companies who have been struggling to offer their customers' better IT services as well as maintaining IT staff who sometimes demand high salaries at such competitive market rates. This demand for Cloud services has therefore been steadily rising among small and medium sized companies.

As demand rises so are threat to the Cloud environment, thus, there is need for a proper security implementation that will encourage the usage of the cloud services. Intel (2014) observes that cloud service providers that have incorporated security during the design and development of their infrastructure and platform as well as within the application layers can offer greater assurance. The current cloud security models, architectures and algorithms despite their advantages still fall short of guaranteeing adequate security in an ever evolving Cloud computing platform, especially as this concept move to the Internet of Things (IOT). Therefore, there are still numerous concerns that need to be addressed to offer effective and real time Cloud security to the various data types in the cloud storage. The question, thus, remains is there a proper way to safeguard the various data types?

## Chapter 3: Research Methodology

### 3.1 Introduction

This section will illustrate on how data will be gathered and analysed, in order to meet the criteria set out in research questions as well as attain the intended objectives. The objective is to develop a scheme for enhancing cloud data confidentiality using Authentication with encryption. The section, therefore, will delve into the research methodology used and how it is applied in solving the research problem.

### 3.2 Research Design

The study will take the design of both descriptive research (what is going on) as well as explanatory research (why it is going on) perspectives. The descriptive research is fundamental to proper understanding of the context and how it will inform the filling of existing gaps. Similarly, explanatory research will endeavour to highlight on "why Cloud security?" This, therefore, helps in examining the trends and how it will inform in answering the research objectives. In essence, why Cloud security will involve development of casual explanation on why a certain security threat is happening more in the Cloud than in traditional computing models. This, therefore, will give an insight on the reasons that may be fuelling this trend.

The use of descriptive and explanatory research fits into the research because description will help in uncovering existing gaps within cloud security domain. On the other hand, explanatory research methods will help give reasons why such challenges are happening. The proposed scheme will consist of three major modules: user (client), administrative and encryption/decryption. The main key components will be the User (human being or an application), text file (in Cloud storage) and the method of accessing the data. The method may be required to six digit code alert via mobile or e-mail notification in real-time to allow the user proceed to 2nd authentication using the code in order to access Cloud data. The failure for the user to use the code will, enable Yeomen system to deny him/her access even if the 1st authentication was genuine, hence, offering cloud data confidentiality.

Systematic Literature Review (SLR) as well as survey will be the main research methodology that this Dissertation will employ. The choice of SLR is to give a summary of the literature related to the study inquiry so as to identify the key words that will form the foundation of the study topic. These keywords will be used in Google Scholar, IEEE explore among other University online resources to identify papers related to the research questions. The analysed literature will guide in answering the research questions. The literature review will be on published Journals as well as other research papers on the research topic.

Survey methodology is essential in designing questionnaire that will be distributed to Cloud users, especially those that use Cloud storage for their data. This, therefore, will involve use of random sampling in the identification of organizations as well as individuals who are either using Cloud computing storage services or are planning to do so in the next six months. Prepared questionnaires will be forwarded to the respondents after a sample population is first ascertained. The questionnaires will be forwarded either physical or through e-mails.

In addition, since administrative, user and encryption/decryption are key modules, in which major class will be based, these classes will incorporate alert functions in order to detect in real time when account is accessed whether by legitimate owner or not. It is also of essence to note that a ‘user’ may certainly not only be a person, but also mean an application that may try to access Cloud data. For instance, if an application tries to access Cloud data, notification code will be given via mobile or e-mail to the user to authorize further authentication, thus, enhancing cloud data confidentiality.

### 3.3 Population and Sampling

Population is all members that meet a set of specifications or a specified criterion (Corinna, 2014). When a small set is selected from population it is called a sample. According to Corinna (2014) a sample is a subgroup of the whole population that will provide data for the research. Similarly, Singh and Masuku (2014) define sampling as the selection of a subgroup of individuals from within a population to approximate the characteristics of whole population. From the above authors, there is an agreement on having a subset, apart from acting as a representative of the population; it also saves on wastage of time, resources, and money if we were to employ the whole population. It therefore, means that the search for precision is what informs the sample size among other considerations.

According to Singh and Masuku (2014) sampling can fall into the following categories, the random sampling, purposive sampling, cluster sampling, quota sampling, spatial sampling and independent sampling among others. This research will use random sampling because each elementary entity in the population will have equal probability of being selected. Since, random sampling will being used, Slovin's formula is ideal, because according to Ellen (2016) Slovin's formula is employed when nothing regarding the behaviour of a population is known at all. In addition, Slovin's formula is useful because it does not require the use of the mean in determining sample size as other formulas require. The formula below is attributed to Michael Slovin in his publication of 1960.

**Slovin's Formula:**

$$\mathbf{n = N/(1 + Ne^2)}$$

Where;

**n =** number of sample size
**N** = total population
**e** = confidence level.

In the formula above, confidence level can be figured out by research supervisor or the researcher according to the desired expectations. As expectations of this research confidence level of e = 0.02 was used, this, therefore, provided level of accuracy of about 98 percent, which would reflect the true picture of the threats within the cloud environment. As Ellen (2016) argues that the use of Slovin's formula grants a researcher to sample the population with a desired degree of accuracy. Thus, the formula ensure that the researcher can decide on what level of accuracy it's results will be. The confidence level is allowed probability of committing an error in selecting a small subset from the population. For instance, if 95 percent confident level was desired for the data to be reflective of the entire population then: 1 – 0.95 = 0.05, thus, e = 0.05. Using the above formula, a population size will be 30 respondents will be interviewed from various targeted organizations, thus, this create a sample size of 29.6. The reason for adoption above formula was for the researcher to interview respondents, a number close to the total population in order to avoid biases attributed to interviewing few people.

The sampled population will consist of employees within different companies in mobile telecommunications, banking services, retail/supermarkets services, health services among others in Nairobi which utilizes Cloud storage services; a company being a sampling unit. In performing an analysis of access to Cloud data storage, there is need to monitor on how the login authentication will guarantee that the genuine user will get code notification via mobile or e-mail so as to offer further authentication before proceeding to security layer. In addition, users sampled may be required to decrypt their data before accessing it in Cloud storage. Slovin’s formula was used whereby we assume that order in which companies or organizations are identified does not matter. The Slovin’s formula was chosen since it gives the population equal chance of being picked, hence lacks biasness.

## 3.4 Data collection method and procedure

The results from the respondents are gotten through the sampling unit which consist of the various companies that utilize cloud storage services in one way or another. The semi-structured questionnaire as well as structured questionnaire was the main method of data collection. Information security managers/officers and System administrators shall be interviewed on the various threats to data stored in the Cloud. The collected data assist in highlighting the kinds of threats and attacks that System administrators as well as Information security managers/officers experience in the management of data in the Cloud storage.

## 3.5 Data analysis

According to UNICEF (2014) data analysis techniques must be selected to match the specific assessment in terms of its key evaluation questions and the resources available. It goes further to state that the techniques must be able to complement each other's strength and weaknesses, in order to fill the existing gaps with the existing data. Therefore, since resources and other factors influence the choice of methods to analyze data, the researcher will concentrate on what will utilize less resources as well as meeting the intended objectives of the research. Data will be analyzed after the first interviews on the information security managers/officers and System administrators, since it will easy work on the researcher.

The research will use content data hermeneutics analysis whereby data is done in two ways that is as fundamental philosopy ( concept) and a type of examination. In the philosophical context the use of cloud data threats drives towards understanding the how the system administrators perceive the consequences of security threats, since they are key in supplying answers to our research questions in order to give room for interpretation. On the other hand, a type of examination allows for understanding the textual data that has been collected from respondents.  The examination of this data informs in gaining insights on cloud data threats, thus, enabling the researcher to conceptualize on the best way of addressing the challenges.

### 3.6 Research Validity

Research validity is when data measures what they are intended to measure (UNICEF, 2014). In order to meet validity criteria precision, reliability, integrity among other factors are important in order to guarantee good research validity. Precision is when data have sufficient detail while reliability is an aspect of consistency when measurements are repeated. On the other hand, integrity is when data is protected from deliberate bias or manipulation for political or personal reasons (UNICEF, 2014). Thus, according to the above explanations of validity, the proposed system achieved research objectives whereby it was able to sent six digit code after first round of authentication to client mobile or e-mail in all situations during testing. Of importance in research is to realise that interviewee's can be affected by work environment, hence, such kind of biases can influence their research input.

This study shall interview mutliple people in different identified companies that consume cloud storage services in order to guarantee that the data collected is reliable, it will also involve a phone call in order to urge respondents to give their honest input to assure precision of the research results.

### 3.7 Summary

In conclusion, therefore, the research methodologies highlighted in this section will inform how research will be carried out in order to address the objectives of the study. It is therefore of importance to note that the employment of descriptive as well as explanatory research methodologies was done so that each will complement the other, in order to give better understanding of the study topic, hence enabling the researcher to develop a scheme for enhancing cloud data confidentiality using authentication with encryption.

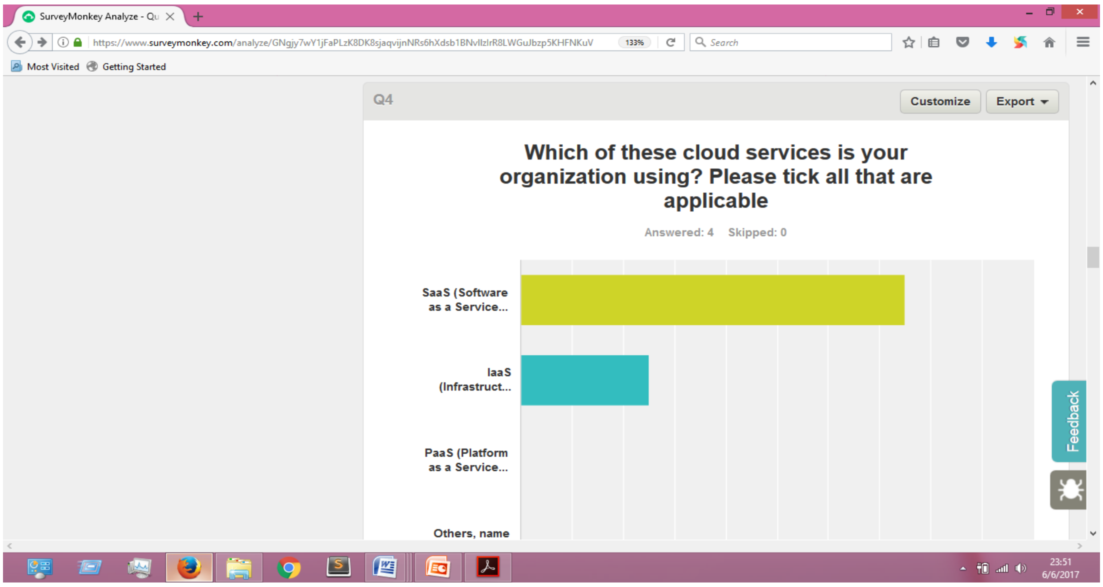
# Chapter 4: System Analysis, Design and Architecture

## 4.0 Introduction

This section involves the presentation of the online survey carried out among system administrators of various organizations involved in administering Cloud services at their companies. While undertaking the survey, the main aim was to gain a deeper insight into barriers to cloud services adoption as well as the trust that system administrators have in data confidentiality offered by cloud providers to their organization. In addition, the system functional and non-functional requirements will be discussed, including a description of inputs and outputs.

## 4.1 Survey

The online survey carried on system administrators dealing with cloud services among various companies within Nairobi were aimed at getting general information on cloud computing within their organization, before delving deeper into what the administrators thought was the greatest barrier to the adoption of cloud services within their organization. Similarly, the research would endeavour to get what the system administrator feel is the greatest threat to cloud data confidentiality in their organization. According to respondents, there was more use of Software as a Service (SaaS) and Infrastructure as a Service (IaaS) by organization adopting cloud services. The Figure 4: 1 below illustrate.



https://www.surveymonkey.com/analyze/GNgjy7wY1jFaPLzK8DK8sjaqvijnNRs6hXdsb1BNvllzlrR8LWGuJbzp5KHFNKuV

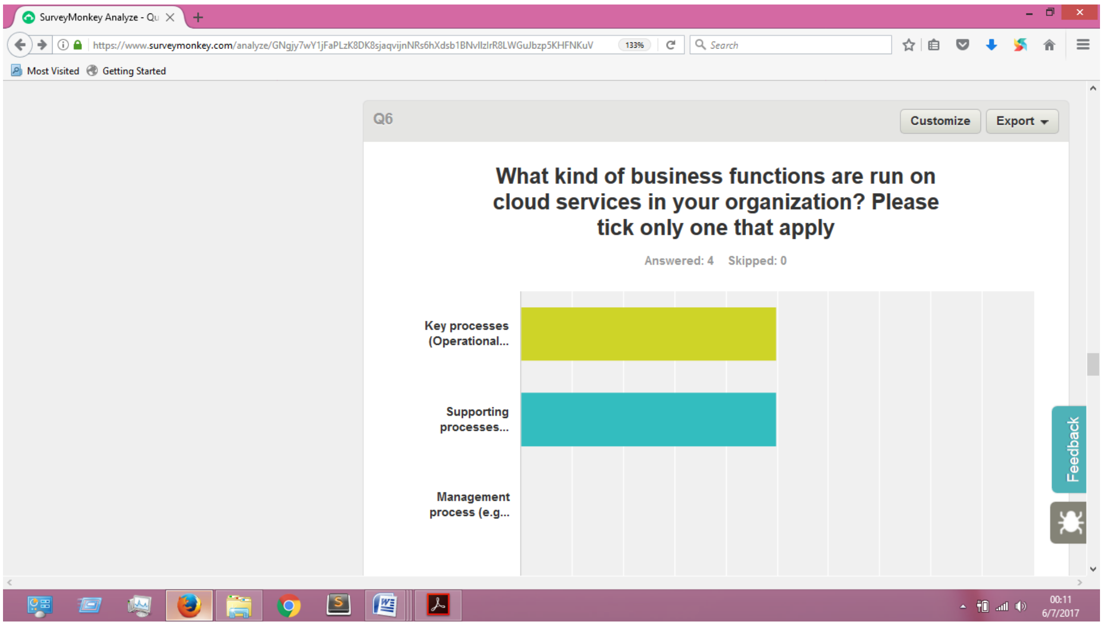
Q4

Which of these cloud services is your organization using? Please tick all that are applicable

Answered: 4 Skipped: 0

**Figure 4: 1: More use SaaS**

The respondents had an understanding of the positive impact of cloud computing to organization baseline as well as it's strategic advantage that can offer to companies. This is because according to the Figure 4: 2 below it illustrates on how cloud computing services support key processes (operational) and supporting processes (like human resource management) in day to day organizational operations.

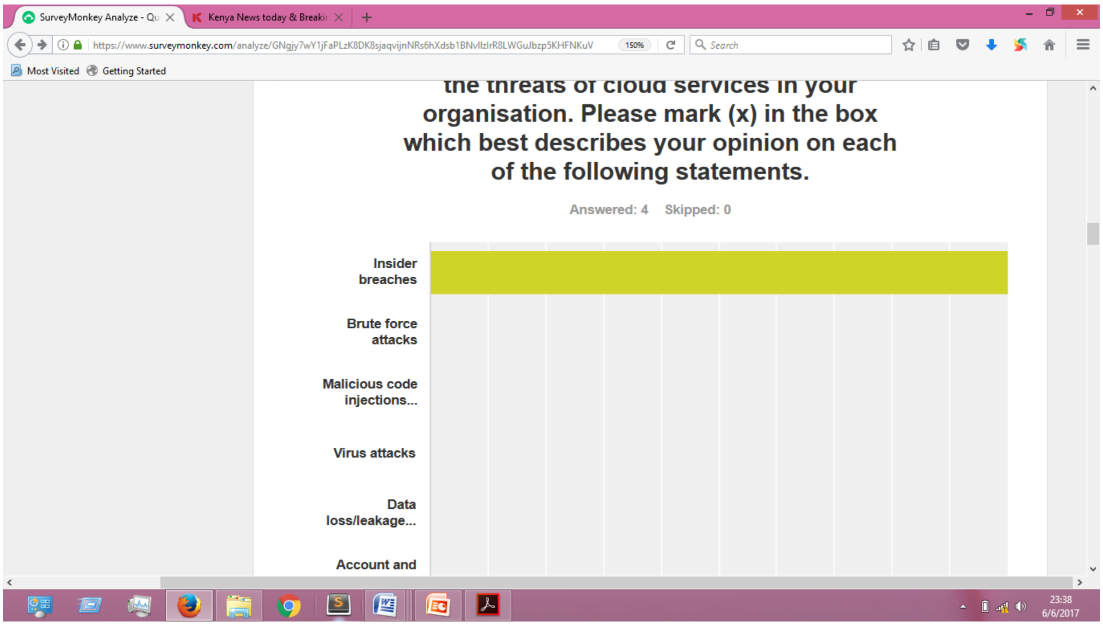

SurveyMonkey Analyze - Qu
https://www.surveymonkey.com/analyze/GNgjy7wY1jFaPLzK8DK8sjaqvijnNRs6hXdsb1BNvllzlrR8LWGuJbzp5KHFNKuV
133%
Search
Most Visited
Getting Started
Q6
Customize
Export
Key processes (Operational...
Supporting processes...
Management process (e.g...
Feedback
00:11
6/7/2017

What kind of business functions are run on cloud services in your organization? Please tick only one that apply

Answered: 4 Skipped: 0

**Figure 4: 2: Cloud Computing Supporting Key Processes**

In addition, they highlighted that insider breaches were the main forms of vulnerabilities to organization data within the cloud environment. As shown by the Figure 4: 3 below.



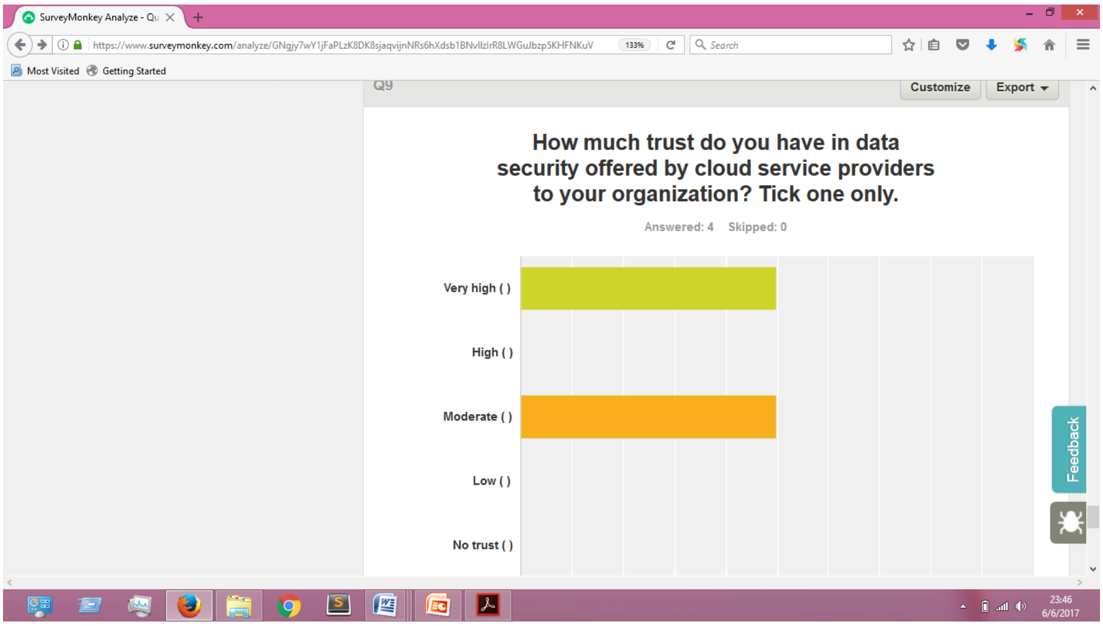
the threats of cloud services in your organisation. Please mark (x) in the box which best describes your opinion on each of the following statements.

Answered: 4 Skipped: 0

SurveyMonkey Analyze - Qu
Kenya News today & Breakir
https://www.surveymonkey.com/analyze/GNgjy7wY1jFaPLzK8DK8sjaqvijnNRs6hXdsb1BNvllzlrR8LWGuJbzp5KHFNKuV
150%
Search
Most Visited
Getting Started
Insider breaches
Brute force attacks
Malicious code injections...
Virus attacks
Data loss/leakage...
Account and
23:38
6/6/2017

**Figure 4: 3: Insider breaches as main threat**

Out of a total of 4 respondents who participated, two respondents said that they had moderate trust on data security offered by cloud service providers despite their organization using cloud services. On the other hand, two respondents said they have high level of trust on data security offered by cloud service providers, this view contradict the earlier perception by their colleagues. The divergent views offered by the system administrators can be attributed to lack of proper involvement in the rolling of cloud services within the organization. Another reason could be because of poor training by the companies on cloud services and how the company can leverage in gaining strategic advantage within the market. The Figure 4: 4 illustrate.



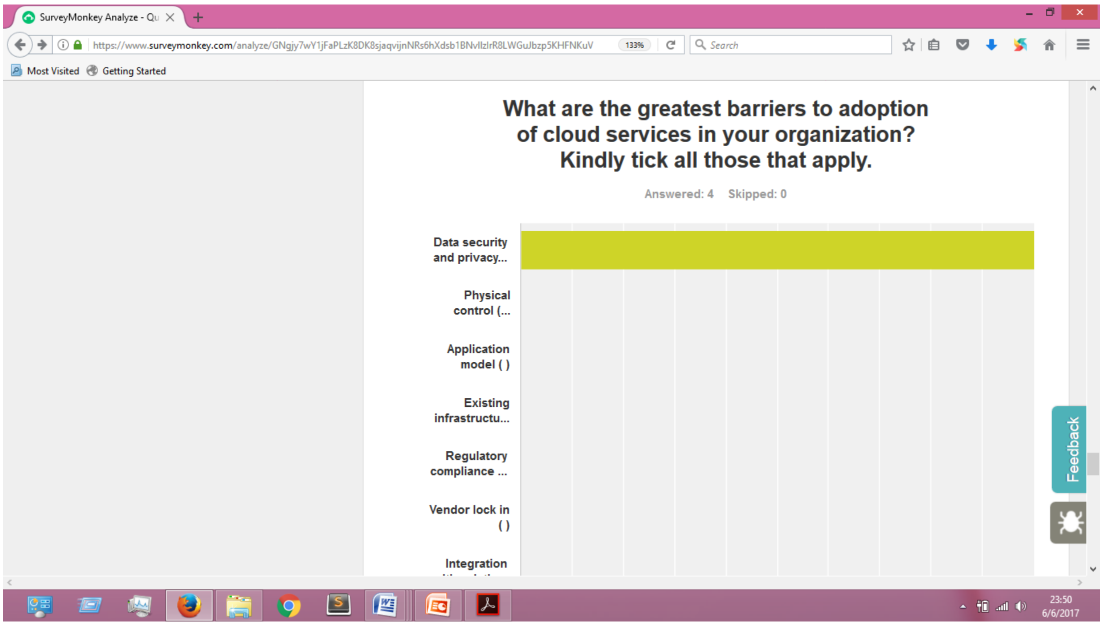
How much trust do you have in data security offered by cloud service providers to your organization? Tick one only.

Answered: 4 Skipped: 0

SurveyMonkey Analyze - Qu
https://www.surveymonkey.com/analyze/GNgjy7wY1jFaPLzK8DK8sjaqvijnNRs6hXdsb1BNvllzlrR8LWGuJbzp5KHFNKuV
Most Visited
Getting Started
Q9
Customize
Export
Very high ( )
High ( )
Moderate ( )
Low ( )
No trust ( )
Feedback
23:46
6/6/2017

**Figure 4: 4: Level of Trust on Cloud Services**

In a nutshell, the survey confirmed that despite rapid growth of cloud computing, data confidentiality in the cloud servers was still a big challenge and there is need for continued research on how best to secure data within that environment. The Figure 4: 5 shows.



What are the greatest barriers to adoption of cloud services in your organization? Kindly tick all those that apply.

Answered: 4 Skipped: 0

SurveyMonkey Analyze - Qu
https://www.surveymonkey.com/analyze/GNgjy7wY1jFaPLzK8DK8sjaqvijnNRs6hXdsb1BNvllzlrR8LWGuJbzp5KHFNKuV
Most Visited
Getting Started
Data security and privacy...
Physical control (...
Application model ( )
Existing infrastructu...
Regulatory compliance ...
Vendor lock in ( )
Integration
Feedback
23:50
6/6/2017

**Figure 4: 5: Data Security and Privacy are Greatest Barriers to Cloud adoption**

## 4.2 System Analysis and Design

### 4.2.1 Functional Requirements

The data collected and analyzed informed the requirements of the proposed system which will be called Yeomen, is aimed at addressing threats attributed to stolen user credentials either by malicious insiders or outsiders.

a) **User layer**

***Informal description:*** The user layer is responsible for session login and identity provider management. The client starts account login procedure by keying in their usernames and passwords, which gives them authorization to access Cloud Storage services based on their roles and permissions. The Cloud Service provider will redirect the user to Identity Provider, which will issue a six digit code notifying the genuine user via either mobile or e-mail notification that his account is being accessed, urging him/her to use the code provided for second round of authentication. With successful the use of the six digit code provided the user will proceed to the dashboard, where he/she can operate on his/her cloud data. Otherwise, in case of use of wrong six digit code, the user will be notified to try again, before redirecting him/her to login stage.

In case of wrong credentials the user is informed that the provided credentials do not match. In this, case therefore, a login interface will notify the user that credentials provided do not match, urging him/her to try again. In addition, the system will sent mobile or e-mail notification to the system administrator notifying him/her of attempts to breach the system, using a certain user account. In addition, for a new user, he/she is supposed to contact system administrator for him/her to fill his/her registration information and submit for processing.

***Pre-condition:*** It is assumed that the user is registered member with various roles and access rights.

***Post condition:*** The client has effectively logged into the system and can be able to perform a number of functions. In case of a new user he/she has filled registration form and it been processed successful.

### b) Security layer

***Informal description:*** After successful two round authentication, the process of Mcrypt Rijndael 256 Algorithm occurs using cipher block chaining (CBC) mode, an initialization vector (iv) is also required for encryption if he/she wants to store his/her data in the cloud environment. After the process, the data is kept into Cloud storage (database) in cipher text format.

In case, whereby the user wants to access his Cloud storage account to carry out some task in the stored data, the user logs into the Cloud storage using his/her credentials for authentication. The login interface will redirect the user to identity provider who issues a six digit code, notifying the genuine user via mobile or e-mail notification, to use the provided code to further authenticate himself/herself. If successful, the system will proceed to the dashboard where he/she can employ Mcrypt Rijndael 256 Algorithm using cipher block chaining (CBC) mode with an initialization vector (iv) to decrypt the cloud data. After successful decryption process, the database will serve the user with plain text or structured cloud data.

Otherwise, if first authentication fails, the user is notified to try again with notification being sent to system administration of attempted breach of the system. In case whereby the second round authentication fails, user is notified to try again while the system administration is notified that there was attempted breach of the system with certain user account.

***Pre-condition:*** A user must have logged in successfully.

***Post Condition:*** The user has roles and permissions to edit data in cloud storage.

### c) Storage layer

***Informal description:*** The cloud service provider database provides cloud storage services which serves data as required by the user after successful meeting the login requirements.

***Pre-condition:*** The user is assumed to have legally accessed the system and database system administrator has given him/her some roles and permissions to access and edit stored cloud data.

***Post Condition:*** The user can edit cloud data.

### 4.2.2 Non-Functional requirements

**a) Usability**

i. The Graphical User Interface for the system should offer ease of use in order to enable the system administrator to assign roles and permissions to the various cloud users.

ii. The system administrator will be capable of monitoring users' according to particular permissions and roles in addition to addressing challenges emanating from the genuine users who have been locked out of their accounts because of the various issues.

iii. The user interface should be clear, consistent, uncluttered and efficient. A keyboard and mouse in addition to mobile virtual keyboard will be used, because the permissions and roles of different users need to be tested.

**b) System Performance and Reliability**

i. The system shall be able to give real time alerts via mobile or e-mail notification to the user when he/she is logging into his/her account.

ii. Any form of rejection by the user that he/she is not accessing his/her account will allow for denial of access even if the user credentials are correct, an alert will be sent to system administrator in real time to check for intrusion by unauthorized users.

iii. The system requirements should be able to work on a server costing less than Kshs. 150,000.

iv. The system should not use more than a quarter of bandwidth provided.

v. The system failures shall be no more than an hour for every 60,000 hours. Failure of the system is when it crashes, whereby 60% of the data is lost or corrupted.

**c) System Scalability and Modifiability**

i. The system should allow for increasing and decreasing of companies operations without seriously affecting the response time of the application.

ii. The extensibility of the application is necessary. The system should be able to give alerts via mobile or e-mail notification in case the cloud storage account is being accessed. In addition, it should be modified to use finger print sensing for mobile devices with such features in order to lock out unauthorized users from the cloud system using biometric features.

**d) Portability**

Use of computer and mobile device testing of the system will be necessary in order to assure for portability in various hardware platforms which run on various operating systems including: Linux, Windows NT, Ubuntu OS and MacOs. The application should also run on android Operating system among other OS used on mobile devices.

**e) Security**

Security as a requirement, a user, will log into the system in order to test whether the system will issue a notification to the cloud account user through mobile or e-mail as envisaged in the system design. In addition, unauthorized user will log into the system in order to test whether it will sent an alert through mobile or e-mail to the system administrator.

## 4.3 Feasibility

### 4.3.1 System economic and technical feasibility

The system is economical viable because of the rising adoption of cloud services by organizations and individuals interested in storing their data in the cloud environment because of high cost of buying anti-virus software. In addition, the continued growth of social media and a steady move into the Internet of Things is one encouraging factor to embrace better secure systems in the cloud.

The requirements needed in the development of the system include knowledge of various open source technologies that include: Bootstrap (responsive system), JQuery, Ajax, Html, Cascading style sheet, JavaScript, toastr (used to push notification about success or failure of a request), Sublime text editor, Font awesome, Datatables, WampServer 2.5, API gateway integration and MySQL. The system also requires to run on a computer with a 64-bit operating system, Processor Intel Core i3 CPU @ 1.90 GHz, 4 GB of RAM, disk space of 80 GB, Hard drive of 250 GB, Hypervisor supported network interface card, Internet bundles and a server. The Figure 4: 6 below illustrates how system architecture is.

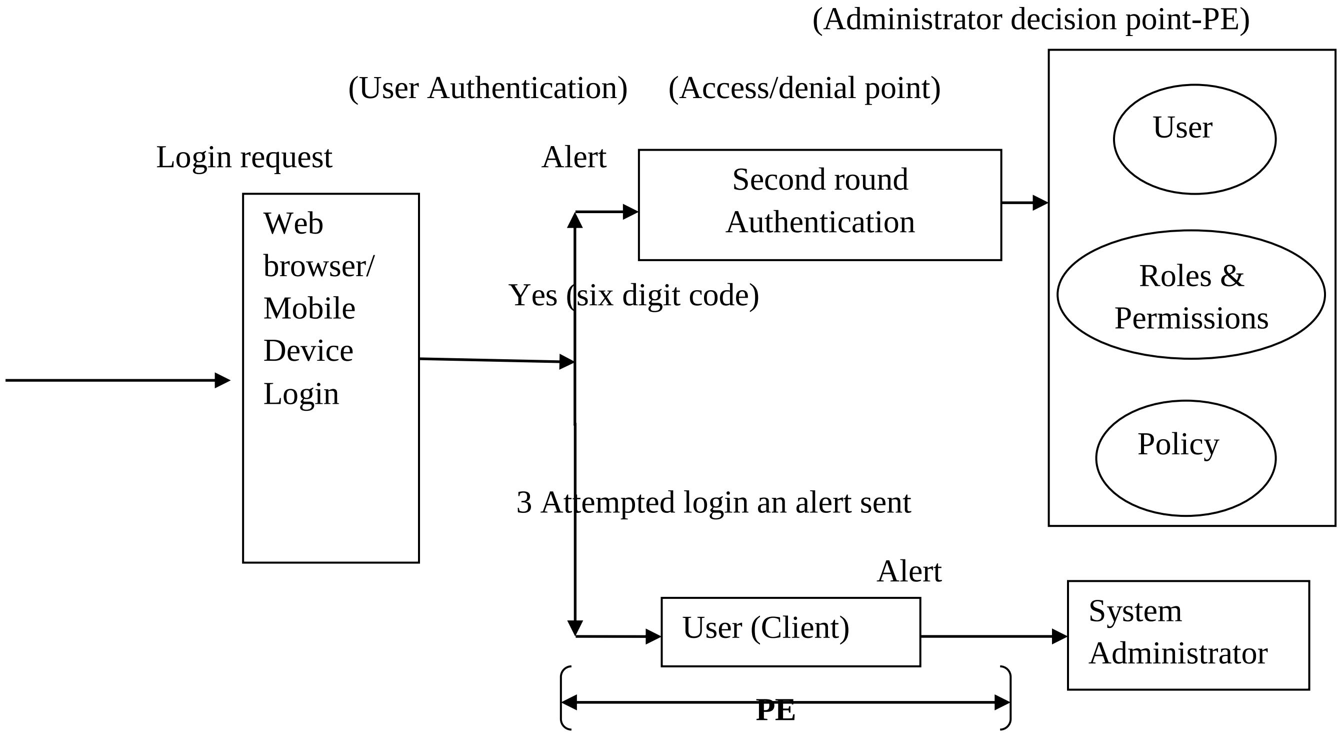


**Figure 4: 6: System Architecture**

Key

**PE** - Policy Enforcement

### 4.3.2 Policy Enforcement (PE)

The Policy Enforcement section of the system allows and disallows certain permissions of the users while logging into the system. Being the edge in which other systems connect to the cloud storage system requires proper management of policy in order to curtail those with ill intentions.

### 4.3.3 Access/denial point

In this section when a user has been granted access to the system, he/she can operate on cloud data depending on permissions and roles he has been granted. In addition, the denial of access will prompt the system to send an alert to the system administrator that a client/unauthorized user have been denied access.

### 4.3.4 User, Policy, Roles and Permissions

This is the administrator platform for users to be assigned roles and permissions that the system will use. It is also a point of policy creation in order to be applied in enforcement stage. The system context diagram will highlight system inputs and outputs and how they are passed from one stage to the next. The figure 4: 7 below illustrate it's working.

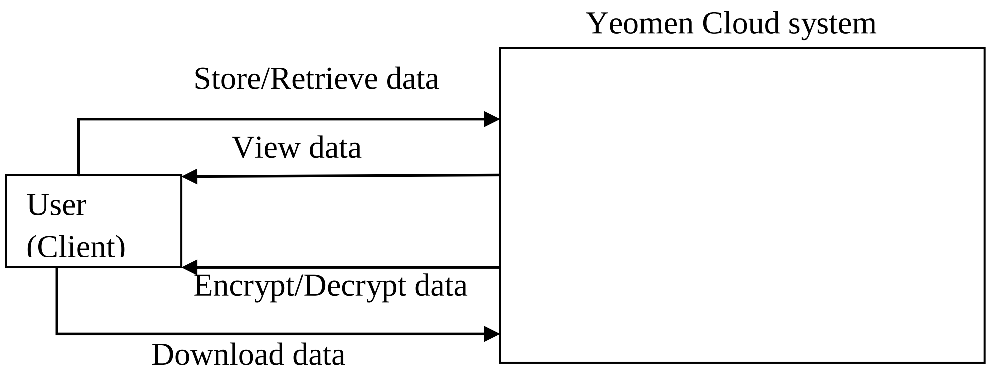


**Figure 4: 7: System context diagram**

The system Data flow diagram consist of three main modules that is User, Administrative and Encryption/decryption modules which interact to retrieve, store and process data from the database system. The Figures 4: 8 and 4: 9 below illustrates the flow of information within the system and system data flow chart respectively.

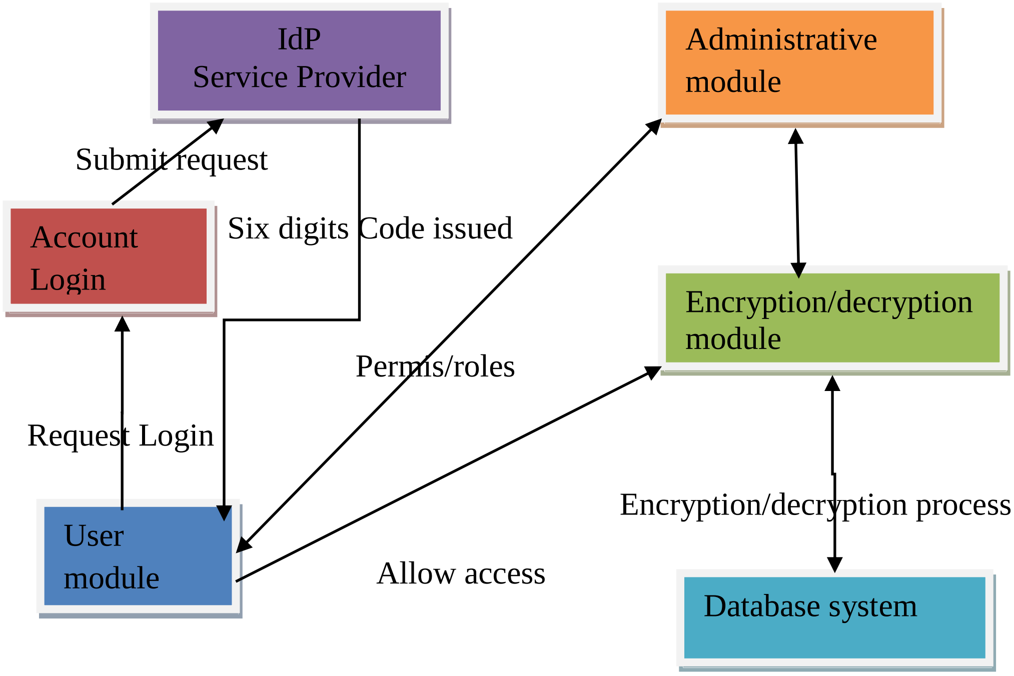


**Figure 4: 8: System Data Flow diagram**

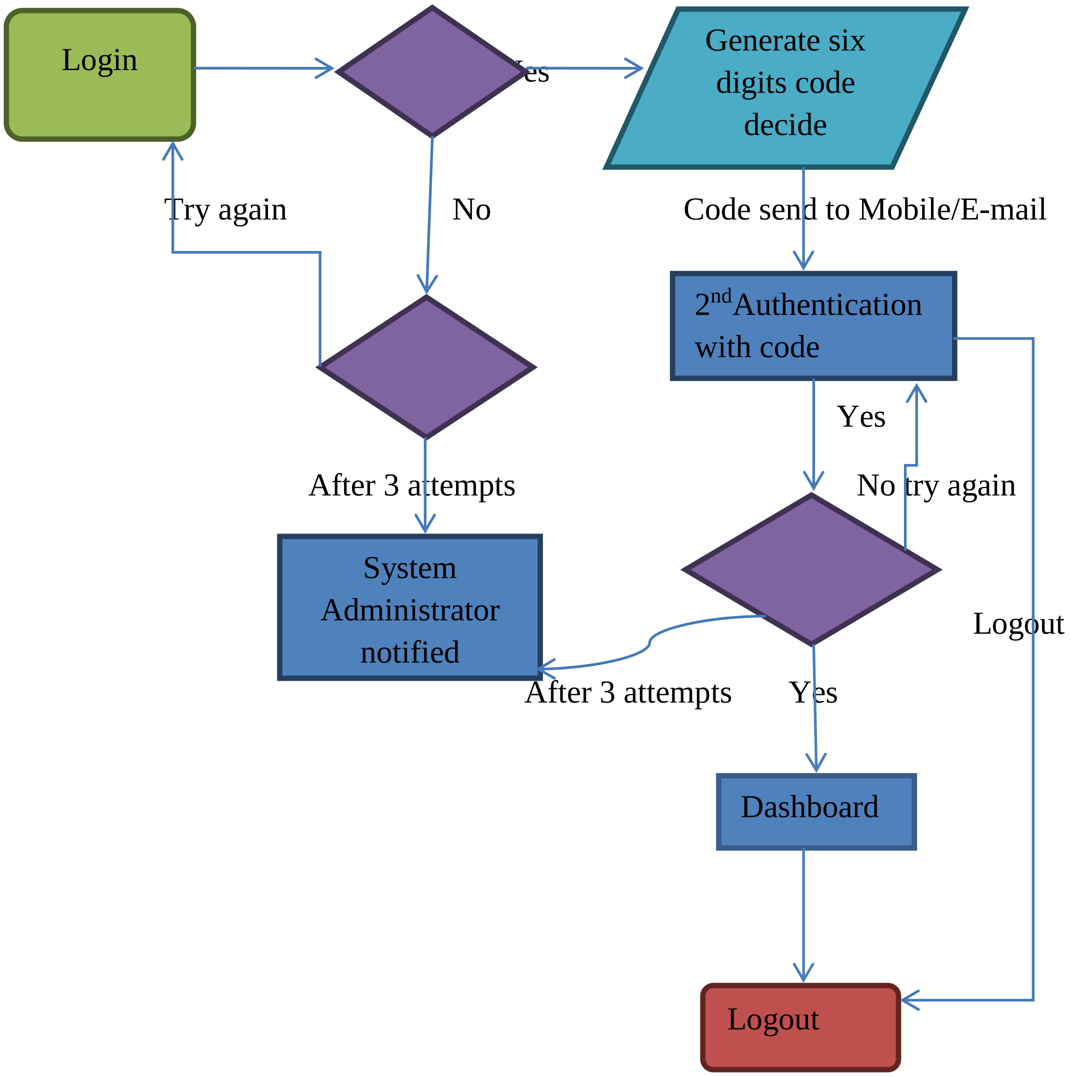

Login
Yes
Generate six digits code decide
Try again
No
Code send to Mobile/E-mail
2nd Authentication with code
Yes
After 3 attempts
No try again
System Administrator notified
Logout
After 3 attempts
Yes
Dashboard
Logout

**Figure 4: 9: System Data Flow Chart**

### 4.4 Database

The database system design will be a three-tier database server architecture whereby the client is responsible for input/output processing logic and application server will be responsible for business rules logic. The Database server will act as cloud storage as well as Database Management system that queries and retrieves the requested data to the users. The Figure 4: 10 below illustrate the architecture.

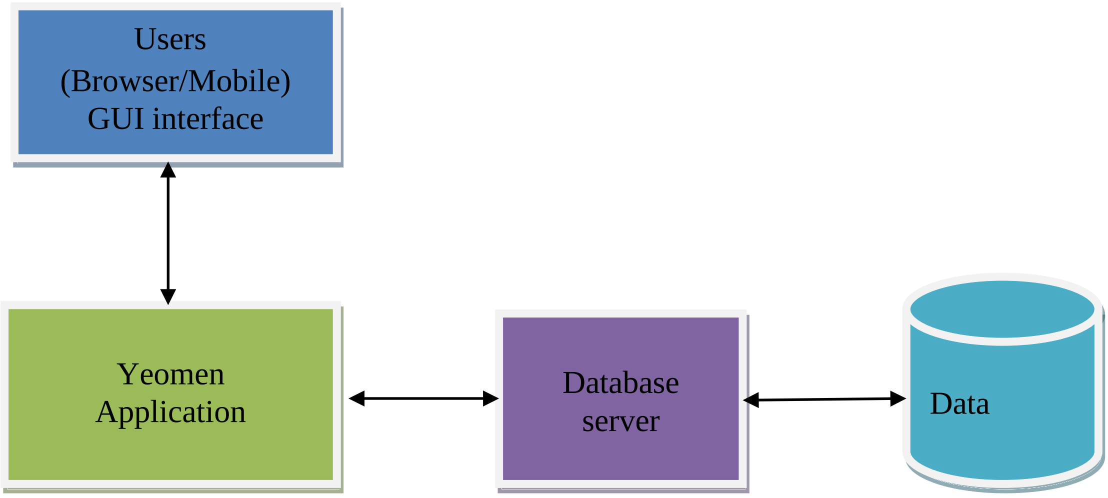


**Figure 4: 10: Three-Tier Server Architecture**

### 4.5 System Pseudocode

The complete refinement of pseudocode is shown below.

```
i.     Start
ii.    Initialize successful login to zero
iii.   Initialize login failures to zero
iv.    Initialize user counter to one
v.     While user counter is less than or equal to 3
vi.    Prompt the user to enter the next try of username and Password
vii.   Input the username and password
viii.  If the user succeed
ix.    Add one to successful login
x.     Else
xi.    Add one to failures
xii.   While user as successful logged in, go to xiv
xiii.  Else, go to vi
xiv.   Add one to user counter
xv.    Sent a six digit code to user mobile and E-mail for second round
       authentication
xvi.   System administrator receives mobile or e-mail notification of attempted
       access
xvii.  If yes
```

xviii. Print “Welcome to Cloud Storage”

xix. Else go to vii

xx. If failed attempts is equal to 3 go to xvi

xxi. Print “Please contact the System Administrator”,

xxii. Stop

### 4.6 Summary

In summary, the security of cloud data is strongly dependent upon how people, applications and processes interact in order to offer the best desired environment for adequate security. The promise of the scheme to deliver depends on how it’s functional as well as non-functional requirements are developed in order to enhance cloud data confidentiality so as to solve the desired challenges within the cloud storage environment.

# Chapter 5: System Development, Implementation and Testing

## 5.0 Introduction

System development involves different tasks and methods used in coming up with a system and it can take various routes i.e. in-house, sub-contracting or packaged software product depending on various factors. According to Himadri and Birendra (2015) Software development methodology maps the diverse activities performed on a software product from its initiation to retirement. Implementation is actually building the system, testing, doing installation work and any post-implementation support or improvement.

## 5.1 System Development

The Yeomen system was developed using the following open source technologies: Html, Bootstrap, Toastr, Ajax, Cascading Style sheet, JQuery, Font Awesome, Sublime, Php, WampServer and MySQL. The Yeomen Systems consists of three main modules that include: administrative, user and encryption/decryption. Some code of user (client) module and administrative module will be shown. The database was developed using MySQL, is managed using WampServer, which also offers PHPMyAdmin and SQLiteManager. The Yeomen system was developed to allow for expansion depending on the needs of the organization.

The first part to be developed was administrative module for adding, deleting, updating and searching through a list of user information. The second module in the development line, was the client (user) module, this is the Graphic user Interface, which would be used to interact with clients. This is the module whose code and its connection with the database will be shown. Some working of the administrative module would be shown during the development of the system. Encryption/decryption module was the third module to be developed, this module allows for the use of PHP mcrypt Rijndael 256 cipher which uses CBC with initialization vector (iv) for both the cloud data encryption/decryption.

### 5.1.1 User (Client) Module

The client (user) module comprise of Login class, CloudStorage class, Client class among others. In order to implement the module properly, class specification was necessary. Client class maintains information on individual cloud users (clients), since system will be dealing with many instances of this class. The figure 5: 1 shows User module.

The diagram for User (Client) module is shown below.

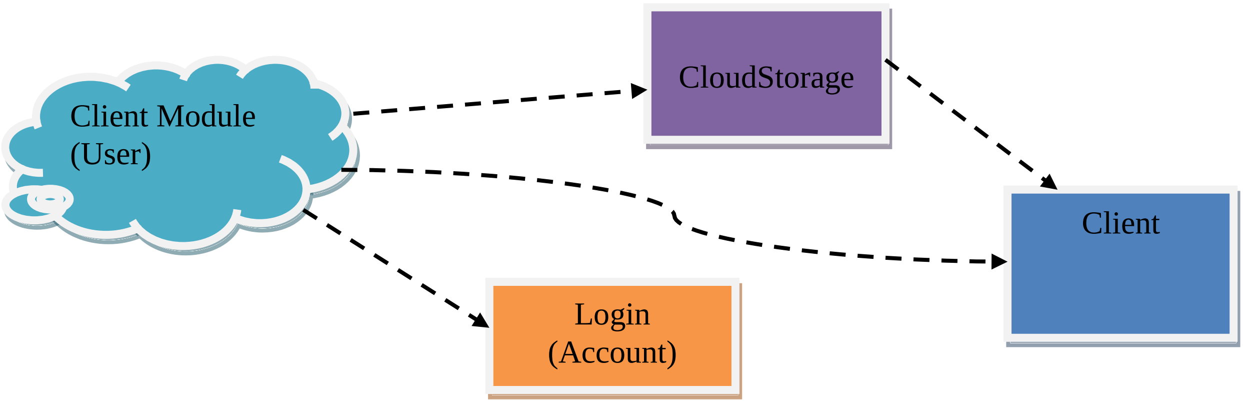


**Figure 5: 1: User (Client) Module**

The CloudStorage class were thought to be a helper class that is used to manage a list of Client objects. It was also meant to provide for addition, deletion, updating and retrieval of Client objects. The class through its connection to the database would enable the saving of an object as well as reading an object from a file. Having a file input and output features would enable Yeomen system to work with different lists of users (clients).

In addition to classes defined above, the program requires a controller class named AccountMonitor, whose instance would be to manage all other objects. AccountMonitor would also be the main class. The Graphic User Interface would require an InputHandler class, whose instance, would allow the client (user) to enter his or her username and password. When the input data are entered by the user (client), an AccountMonitor checks for the validity of the input with the help of CloudStorage object. If the CloudStorage object confirms the input data, the controller then instructs another service object, an instance of Login (Account), to allow access.

### 5.1.2 Administrative Module

The Administrative module comprise of the following classes: cloudStorage and client. The module is responsible for adding, removing updating of client information, searching and retrieval of cloud users.

### 5.1.3 Encryption/Decryprion Module

The Encryption/Decryption module is composed of the following classes: encryptionKey, client and cloudStorage. The module provides to the client ability to encrypt or decrypt his/her cloud data.

### 5.1.4 Configuring Yeomen System

Configuring Yeomen system involved three steps; first would be to configure the virtual server to process authentication requests received from some Cloud Service Providers. The second would enable authentication for individual users (clients) to one or more of the Cloud Service Providers, cloud users (clients) require resources outside the cloud in which their data would be resident. The third step would entail the provisioning rules that determine the roles and permission that govern users or clients and other services within the Yeomen system.

## 5.2 Implementation Algorithm

Implementation is the action that must be followed in order for something to actually happen. When a user (client) logs into the Yeomen system, the system sends the authentication credentials to the Identity provider who verifies if the user (client) has provided proper credentials or not. In case of successful login, a designed function shuffle numbers 0 to 9 to produce a six digit code, which is sent via mobile or e-mail notification to the user (client) that will be used for second round authentication. In cases, whereby reply is not done or delayed for one reason or another, permissions would not be granted even if the first credentials were authentic.

In the event of successful authentication, the user (client) is proceeds to the dashboard where he/she can use PHP mcrypt Rijndael 256 with initialization vector to encrypt cloud data before storing in the cloud. Similarly, he/she can use PHP mcrypt Rijndael 256 with initialization vector to decrypt cloud data if he/she wants to access it within his/her cloud storage account. When a user (client) fails three attempts to access his/her cloud storage account whether by mistake or by having a malicious intent, the system administrator would be notified through a SMS via mobile or e-mail notification that there were some attempts to breach security by unauthorized user.

### 5.3 Testing

The testing process is to analyse whether the Yeomen system support the validation and verification objectives. During testing of the system scheme, there were several attempts to access real cloud storage accounts and the system always responded by sending six digit code SMS notification to the client (user) through mobile or e-mail for second round of authentication to enable him/her to access cloud account. The system also responded when a wrong username or password was entered three times, it sent an SMS notification to system administrator that unauthorized user was trying to breach cloud storage security. The two messages below shows when the six digit code generated randomly and an alert send to system administrator when a user (client) attempts three without success to log into the system.

YEOMEN
Hi tikwang, Please use the following Code: 819275 to authenticate your access.

YEOMEN
There might be some attempts to access Tikwang Iriale account illegally. Please alert.

# Chapter 6: Discussion of Results

## 6.0 Introduction

This chapter would evaluate the objectives set out at the beginning of the research and analyse whether the literature review supported the realization of the stated objectives with regard to the study outcomes.

## 6.1 System Strength and Weaknesses

The objective of the research was to develop a scheme for improving cloud data confidentiality. According to reviewed literature, it was realized that data security and privacy were the key challenges to wider adoption of cloud services with insider threats being the most prevalent. Similarly, online survey conducted also confirmed the same fears, with 100% of the respondents citing insider breaches as the main threat to their organization data. Equally, 100% of respondents also cited data security and privacy as the greatest barriers to the adoption of cloud services in their organization.

Consequently, therefore, in order to address the above threats especially attributed to stolen user credentials it was seen prudent to offer a two way authentication, in addition to encryption of stored cloud data. To defeat use of stolen user credentials, after successful first round of authentication, a function shuffle numbers between 0 to 9 before producing six digit code that is sent to client mobile or e-mail for the second round of authentication. In addition, the PHP mcrypt Rijndael 256 using cipher block chaining (CBC) with initialization vector (iv) was used to encrypt stored cloud data.

The PHP mcrypt Rijndael 256 using CBC with initialization vector (iv) formed the foundation for how the system was modelled, in order to address the problems attributed to insider breaches and man in the middle attacks during the transfer of data within the cloud environment, thus, enhancing cloud data confidentiality. The attack modes that were discussed include multi-tenancy, insider attacks, elasticity, outsider attacks and governance. It is interesting to note that hackers are busy crafting new ways of attacking cloud services as measures are put in place to mitigate against already known vulnerabilities.

Insider attacks and multi-tenancy risk due to data leakage whereby a co-subscriber would accidentally or through malicious intent get another client (user) authentication credentials, an attempt to access a cloud storage account would trigger real time alert element of the Yeomen system that would notify the genuine client account holder providing his/her with a six digit code for further authentication to his/her cloud account in order to be granted access. If three attempted login are done without success, the system administrator would receive an alert indicating that there was attempted breach of system. This would allow the system administrator to follow up the matter of the breach of security within the organization cloud storage assets. Thus, this enables hardening of Yeomen system using other methods, other than those already provided by the system.

Similarly, during the testing of the Yeomen system, it was realized that in case of area with poor mobile network, the system was slow in sending six digit code to user, therefore, in such case, e-mail notification was essential to be used since it was not affected by poor mobile network connection in all the cases tested. In addition, multi-tenancy by its nature allows users (clients) to create and modify their own virtual server's which opens a window of opportunity for hackers, which the real time mobile or e-mail alert element of the system can mitigate for a secure cloud environment.

Yeomen system architecture with its Infobip API gateway provides a seamless way of integrating the system with other organization online and offline applications. In addition, API gateway improves security by curtailing side channel attacks when properly integrated with other system that can be a source of vulnerability. This enhances cloud data confidentiality, encouraging adoption of cloud services by organizations.

The Yeomen system is a fully function application since all its modules were fully developed and integrated together to offer a functioning system ready for deployment within the cloud storage environment. In addition, the system was tested in real Cloud computing environment and met all the intended objective of enhancing cloud data confidentiality; as such, its shortcomings, when exposed to other attack modes were not explored in order to give insights on the system weaknesses.

In a nutshell, Yeomen system through proper security protocols, authentication, data encryption and API gateway can provide a defence in depth platform that would allow for seamless working of the Yeomen system with other applications within and without organization's online and offline core assets. Therefore, this system also moves from defense to detection through situational awareness offered by the mobile or e-mail real time alert feature.

## 6.2 System Efficiency and Reliability

The Yeomen system performed successful in: addition, deletion, updating and searching of cloud users (clients) within the cloud storage database. In addition, the system successful sent SMS via mobile or e-mail alerts when clients were logging into it their cloud storage account. Hence, in summary, it met it's intended objective both in sending mobile or e-mail alerts notification as well as in accuracy of it's results.

# Chapter 7: Conclusion and Recommendation

## 7.0 Conclusion

This dissertation was aimed at developing a scheme for improving data confidentiality in the cloud computing environment by addressing a threat to client account attributed to stolen user credentials. The unauthorized access to client cloud account using stolen user credentials either by malicious insiders or outsiders as discussed in this dissertation has been a major challenge to organization. In trying to address this threat of using stolen user credentials, several cloud security models, architectures and algorithms were reviewed to establish the best way of securing data confidentiality in cloud storage. The shortcomings indentified informed the development of the Yeomen system which improved the security of cloud data confidentiality by sending a six digit code in real time to client mobile or e-mail when their accounts are accessed, whether by unauthorized user or malicious insiders within the organization. In addition, it provided a secure cloud environment by having two way authentication and encryption using PHP mcrypt Rijndael 256 using CBC with initialization vector (iv) implemented together in a seamless way to provide adequate data confidentiality in the cloud. The use of Infobip API gateway would provide ease of integrating the Yeomen system with other applications within the web.

## 7.1 Recommendation for Future Research

Since data confidentiality is essential in provision of information security in the cloud, this dissertation propose the development of better cryptographic algorithms, in order to provide for proper encryption methods, because with the growth of computing power application are constantly being developed that can compute the encryption keys being used by the various algorithms currently in use. In addition, the research ought also to be directed on coming up with systems that will possess self-hardening elements, by use of artificial intelligence, whereby a system will proactively detect and learn a malicious intent to hack it, and on it’s own, take countermeasures to protect itself by having prior knowledge on various attack profiles and how to mitigate against such attacks, hence, offering confidentiality to user data. Finally, Cloud Service Providers may consider easy to use steps on how clients can ensure security of their data in the cloud environment by providing short time trainings.

# References

Amir, M. T., Rodziah, T., Rusli, A. & Masrah, A. A. M. (2012). Security Framework of Cloud Data Storage Based on Multi Agent System Architecture – A Pilot Study.

Bajwa, M. S., Himani, & Sandeep, S. K. H. (2015). An Enhanced Data Owner Centric Model for Ensuring Data Security in Cloud. 2015 Second International Conference on Advances in Computing and Communication Engineering.

Bartock, M. et al. (2015). Trusted Geolocation in the Cloud: Proof of Concept Implementation. National Institute of Standards and Technology.

Beal, V. (2015). Data. http://www.webopedia.com/TERM/D/data.html. Accessed 20.09.2015.

Britt, P. (n.d). Cloud Security vs. Security in the Cloud: What's the difference? Similar Sounding Cloud Security has a very different Meaning. Accessed on 16.09.2015.

Cisco Systems, Inc. (2016). Cisco Global Cloud Index: Forecast and Methodology, 2015 - 2020 (White Paper).

Corinna, F. 2014). Sampling and its Relevance for Sound Data Collection. Data Network for Better European Organic Market Information. University of Kasel.

Cloud Security Alliance (2016). The Treacherous 12 Cloud Computing Top Threats in 2016. Top Threats Working Group.

Cloud Standards Customer Council (CSCC) (2016). Practical Guide to Hybrid Cloud Computing.

Cobb, S. & Lee, A (2014). Malware is Called Malicious for a Reason: The Risks of Weaponising Code. Cycon 2014: Sixth Annual International Conference on Cyber Conflict NATO Cooperative Cyber Defense Center of Excellence, Tallin, Estonia, June, 2014.

Crawford, A. & Johnstone, B. (2012) *"Cloud Computing",* http://meseec.ce.rit.edu/756-projects/spring2012/2-6.pdf Accessed on: 8 May, 2014.

Crowe, H., Warren, C., Eugene, L. & Heidi, P. (2012). Thought Leadership in ERM, Enterprise Risk Management for Cloud Computing. Research Commissioned by Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Dahshan, M. M. (2013). Data Security in Cloud Storage Services.

Daylami, N. (2016). Cloud Computing: Demystifying the Elephantine Concept. California Lutheran University.

Dogra N. & Kaur H. (2013). Cloud Computing Security: Issues and Concerns. *International Journal of Emerging Technology and Advanced Engineering. ISSN 2250-2459, ISO 9001: 2008 Certified Journal, Volume 3, Issue 3, March, 2013.*

El-Hoby, H. M., Salah, M. A. F, & Suhaimi, M. A. (2014). Aligning Cloud Computing Security with Business Strategy. *International Journal of Computer Trends and Technology (IJCTT), Volume 7, Number 1, Jan, 2014.*

Ellen, S. (2016). Slovin's Formula Sampling Techniques. http://sciencing.com/slovins-formula-sampling-techniques-5475547.html [Accessed on: 24.01.2016].

Feldman, A. J. (2012). Privacy and integrity in the untrusted cloud. Mountain view, California, USA.

Gartner. (2013). 2013 Gartner Magic Quadrant for User Authentication. Digipass by Vasco, The Authentication Company.

Gupta, G., Laxmi, P. R., & Sharma, S. (2014). A Survey on Cloud Security Issues and Techniques. *International Journal on Computational Sciences & Applications (IJCSA). Vol. 4, No, February, 2014.*

Grance, T. & Mell, P. (2011). National Institute of Standards and Technology: The NIST Definition of Cloud Computing. NIST Special Publication 800-145.

Harris, T. (n.d). Cloud Computing - An Overview.

Hashizume, K., Rosado, D. G., Medina, E. F., & Fernandez, E. B. (2013). An Analysis of Security Issues for Cloud Computing. *Journal of Internet Services and Applications: A Springer Open Journal.*

IBM (2015). IBM 2015 Cyber Security Intelligence Index. Analysis of Cyber Attack and Incident Data from IBM's Worldwide Security Services Operations.

Intel Coroporation (2014). Security in the Cloud for SAP HANA. Intel, Vormetric, Virtustream, and SAP Deliver Enterprise-Class, Customer-Controlled Data Security.

Jingxin, K. W. & Xinpei, J. (2012). Data Security and Authentication in Hybrid Cloud Computing Model. 2012 IEEE Global High Tech Congress on Electronics.

Kaur, N. & Tejinderdeep, S. K. (2015). Intended Approach for the Detection and Prevention of SQL Injection Attacks. *International Journal of Advanced Engineering Technology*.

Kepes, B. (2017). Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS. Executive Summary. https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/ [Accessed on 14/02/2017].

Khan, S. S., & Tuteja, R. R. (2015). Security in Cloud Computing Using Cryptographic Algorithms. *International Journal of Innovative Research in Computer and Communication Engineering. Vol. 3, Issue 1, January, 2015.*

Marsh, S., Basu, A. & Dwyer, N. (2013). Theories and Intricacies of Information Security Problems: Security enhancement with Foreground Trust, Comfort, and Ten Commandments for real people.

Masthanamma, V. & Preya, G. L. (2015). An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm. *International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4 Issue 3, March, 2015.*

Mrudula, S. & Chadra, S. V. (2015). A Robust Mutual Authentication Scheme for Data Security in Cloud Architecture. Future Information Security Workshop, COMSNETS 2015.

National Institute of Standards and Technology (2016). Cloud Computing Standards – A NIST Perspective.

Naresh, R. A. & Sai, K. R. (n.d.). Future of Cloud Computing Architecture.

National Institute of Standards and Technology (2014). NIST Special Publication 800 – 137: Information Security Continuous Monitoring for Federal Information Systems and Organizations. FISSEA 27th Annual Conference.

Neha, A. P., Ajay, R. K., & Rajesh, C. D. (2014). Deployment of Application on Cloud and Enhanced Data Security in Cloud Computing Using ECC Algorithm. 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

Ngo, H. B., & Tran, D. T (2015). Multi-Tenant Web Application Framework Architecture Pattern. 2015 2nd National Foundation for Science and Technology Development Conference on Information and Computer Science.

Nigoti, R., Manoj, J., & Singh, S. (2013). A Survey of Cryptographic Algorithms for Cloud Computing. *International Journal of Emerging Technologies in Computational and Applied Sciences, Vol. 4, pp. 141-146, March-May, 2013.*

Nilesh, R. P., & Rajesh, D. (2016). Secured Cloud Architecture for Cloud Service Provider. 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16).

Palande, A., Rao, C., Rodi, P. & Bhusari, V. (2015). Self-Destructing Data System Using Shamir Secret Sharing Algorithm. *International Journal of Applications or Innovation in Engineering & Management (IJAIEM), Volume 4, Issue 1, January, 2015.*

Paritosh, M., Roshan, M., Vishal, S., Dipak, S., & Vipin, W. (2015). Multi-Cloud Data Security Using Shamir Secret Algorithm. *International Journal of Modern Trends in Engineering and Research (IJMTER), Volume 2, Issue 7, July, 2015.*

Prabu, G. K. & Vasudevan, V. (2016). Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

Rajkumar, B. (2013). Introduction to the IEEE Transactions on Cloud Computing. IEEE Transactions on Cloud Computing, Vol. 1, No. 1, Jan-June, 2013.

Rashmi, R. R., Sahoo, G. & Mehfuz, S. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. *International Journal on Cloud Computing: Services and Architectures (IJCCSA), Vol. 3, No. 4, August, 2013.*

Roy, N. & Rishabh, J. (2016). Cloud Computing: Architecture and Concept of *International Journal of Science, Technology & Management, Volume No. 04, Special Issue No. 01.*

Sachdev, A. & Bhansali, M. (2013). Enhancing Cloud Computing

Security Using AES Algorithm. International Journal of Computer Applications (0975-8887), Volume 67, No. 9, April, 2013.

Samson, T. (2013). 9 Top Threats to Cloud Computing. Infoworld, Feb 25, 2013. http://www.infoworld.com/article/2613560/cloud-security/cloud-security-9-top-threats-to-cloud-somputing-security.html. Accessed on 20.10.2015.

Singh, A. S. & Masuku, M. B. (2014). Sampling Techniques & Determination of Sample Size in Applied Statistics Research: An Overview. *International Journal of Economics, Commerce and Management, United Kingdom. Vol. 11, Issue 11, Nov, 2014 ISSN 2348 0386.*

Seema, S. S. & Shaikh, N (2014). *Cloud Computing: Data Separation Issues. International Journal & Magazine of Engineering, Technology, Management and Research A Monthly Peer Received Open Access International. ISSN No: 2348-4845.*

Sengupta, N. (2015). Designing of Hybrid RSA Encryption Algorithm for Cloud Security. *International Journal of Innovative Research in Computer and Communication Engineering. Vol. 3, Issue 5, May, 2015.*

Siemens AG. (2010). Cloud Computing Architecture. Corporate Research and Technologies, Munich, Germany.

Suganya, N., Boopal, N. M. E., & Naveena, M. (2015). Implementing RSA Algorithm to Enhance the Data Security in Cloud Computing. *International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 1, January, 2015.*

Sunil, M., & Manu, S. (2015). A Critical Analysis of Some Symmetric Key Block Cipher Algorithms. *International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (1), 2015, 495-499.*

Sura, K. A., Rawai, T. S., Al-Haddad, S. A. R., Hashim, F., Azizol, B. H. J. A., & Salman, Y. (2015). Cloud Computing Security Risks With Authorization Access for Secure Multi-Tenancy Based on AAAS Protocol.

Symantec (2014). Security Response. The Continued Rise of DDOS Attacks.

Theodoros, M., Angelos, M., & Dimitrios, D. V. (2016). Security Architecture Based on Defense in Depth for Cloud Computing Environment. IEEE INFOCOM First International Workshop on Big Data Sciences, Technologies and Applications (BDSTA 2016).

Tirthani, N. & Ganesan, R. (n.d). Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography.

Twinkle, G. F., & Prema, P. (2015). Secure Collaborative Privacy in Cloud Data with Advanced Symmetric Key Block Algorithm.

United Nations Children's Fund (UNICEF). (2014). Overview: Data Collection and Analysis Methods in Impact Evaluation. UNICEF Office of Research, Methodological Briefs. Impact Evaluation No. 10.

Vishwanath, S. M. & Aniket, K. S. (2014). Enhancing the Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm.

Weiss, A., (2016). How to Prevent SQL Injection Attacks. http://www.esityplanet.com/hackers/how-to-prevent-SQL-injection-attacks.html [Accessed on: 29.08.2016].

Wooley, P. S. (2012). Identifying Cloud Computing security risks. University of Oregon: Applied Information Management.

Yangqing, Z. & Jun, Z. (2015). Research on Data Security Access Model of Cloud Computing Platform. 2015 2nd International Conference on Information Science and Control Engineering.

Zoltan, B. & Milan, T. (2016). *Modeling of Data Security in Cloud Computing.*

## Appendix A: Questionnaire

**Researcher**: Tikwang Iriale Fabiano

**Degree**: MScBIS, Strathmore University

This dissertation questionnaire will be used for academic purpose only. The objective is to identify threats to cloud data. Kindly answer the following questions as honestly and accurately as possible. The information given will be treated with a lot of confidentiality. Please do not write your name anywhere on this questionnaire. You are encouraged to give your honest opinion.

**Survey to determine Cloud computing security implementation among companies**

1. Name of the organization......................................................................

2. Services offered

   I. Telecommunications services ( )

   II. Banking services ( )

   III. Retail / Supermarket services ( )

   IV. Health services ( )

   V. Others ( )

   Name them.........................................................................................

**3. Adoption of cloud services**

This Section is concerned with assessing the extent on the adoption of cloud services by your organisation. Please mark (x) in the box which best describes your agreement or disagreement on each of the following statements.

| **Statement** | **Yes** | **No** |
|---|---|---|
| Discussion stage | | |
| Trial stage | | |

| | | |
|---|---|---|
| Implementation stage | | |
| Currently on use | | |
| Advances usage | | |

4. Which of these cloud services is your organization using? Please tick all that are applicable

   i. SaaS (Software as a Service examples CRM online, salesforce.com, etc) ( )

   ii. IaaS (Infrastructure as a Service examples private cloud, VMware, etc) ( )

   iii. PaaS (Platform as a Service examples Windows Azure, Force.com, Google engine, etc) ( )

   iv. Others, name them.........................................................................

5. What kind of business functions are run on cloud services in your organization? Please tick only one that apply

   i. Key processes (Operational processes) ( )
   ii. Supporting processes (Secondary processes like Human resource management, safety, etc) ( )
   iii. Management process (e.g. governance, budgeting, strategic planning, etc) ( )
   iv. Others, name them……………………………………….

**6. Cloud Services Threats**

This Section is concerned with assessing the threats of cloud services in your organisation. Please mark (x) in the box which best describes your opinion on each of the following statements. The choices given are: 1=Very frequent, 2= Frequent, 3== Moderately Frequent, 4=Less Frequent and 5=Not at all

| **Statement** | **Very Frequent** | **Frequent** | **Moderate frequent** | **Less Frequent** | **Not at all** |
|---|---|---|---|---|---|
| Insider breaches | | | | | |
| Brute force attacks | | | | | |
| Malicious code injections | | | | | |
| Virus attacks | | | | | |
| Data loss/leakage | | | | | |
| Account and service traffic hijacking | | | | | |
| Insecure programming interfaces | | | | | |
| Shared technology vulnerabilities | | | | | |

7. To what extent do you agree that the following factors influence the adoption of cloud services in your organisation? Use the following likert scale to rate your level of agreement that cloud adoption is driven by the following factors.

| Factors | **Strongly agree(5)** | **Agree(4)** | **Undecided(3)** | **Disagree(2)** | **Strongly disagree(1)** |
|---|---|---|---|---|---|
| Cost | | | | | |
| Scalability | | | | | |
| Availability | | | | | |
| Enabling environment | | | | | |

8. To what extent do the following impacts of cloud computing adoption are realized in your organization? Use the likert scale to rate your agreement.

| **Statement** | **Very Frequent** | **Frequent** | **Moderate frequent** | **Less Frequent** | **Not at all** |
|---|---|---|---|---|---|
| Offer more services to the business | | | | | |
| Increase in training | | | | | |
| IT becoming more strategic | | | | | |
| Increase in outsourcing of IT | | | | | |
| Less time in updating IT infrastructure | | | | | |
| Reduced staff | | | | | |

9. What are the greatest barriers to adoption of cloud services in your organization? Kindly tick all those that apply.

   i. Data security and privacy ( )

   ii. Physical control ( )

   iii. Application model ( )

   iv. Existing infrastructure ( )

   v. Regulatory compliance ( )

   vi. Vendor lock in ( )

   vii. Integration with existing systems ( )

   viii. Geographic proximity ( )

10. How much trust do you have in data security offered by cloud service providers to your organization? Tick one only.

   i. Very high ( )

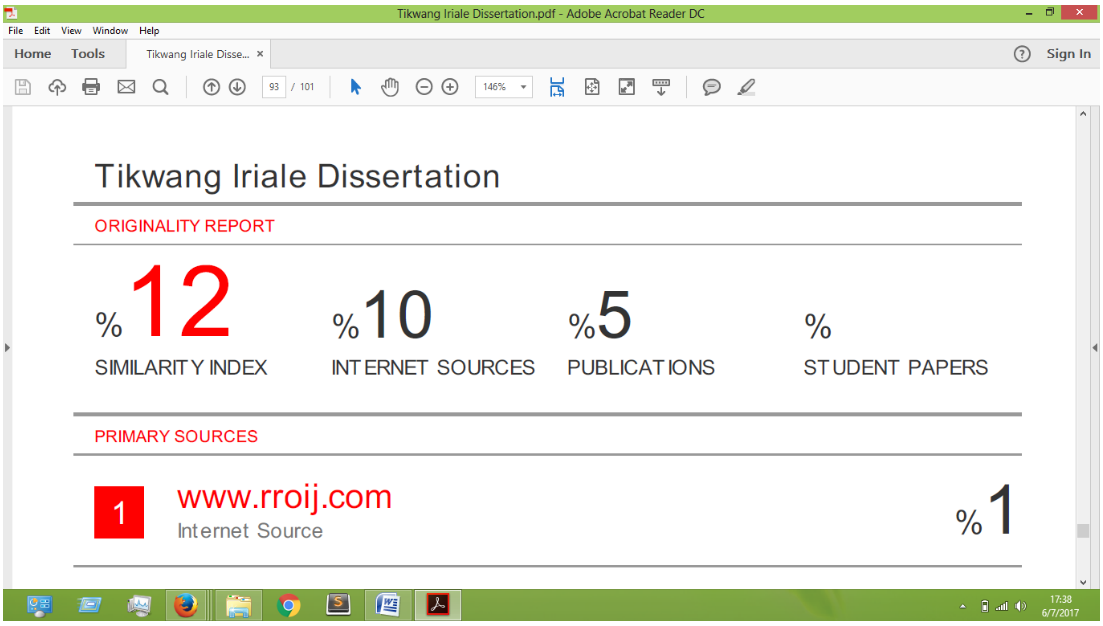
   ii. High ( )

iii. Moderate ( )

iv. Low ( )

v. No trust ( )

# Appendix B: Turnitin Report



Tikwang Iriale Dissertation

ORIGINALITY REPORT

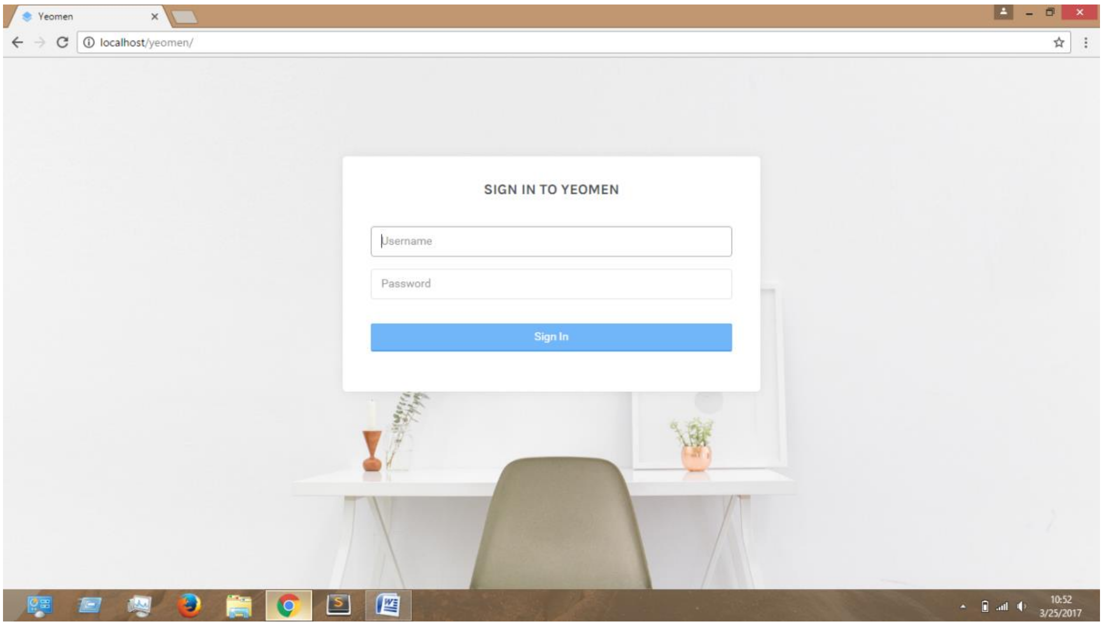
| %12 | %10 | %5 | % |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

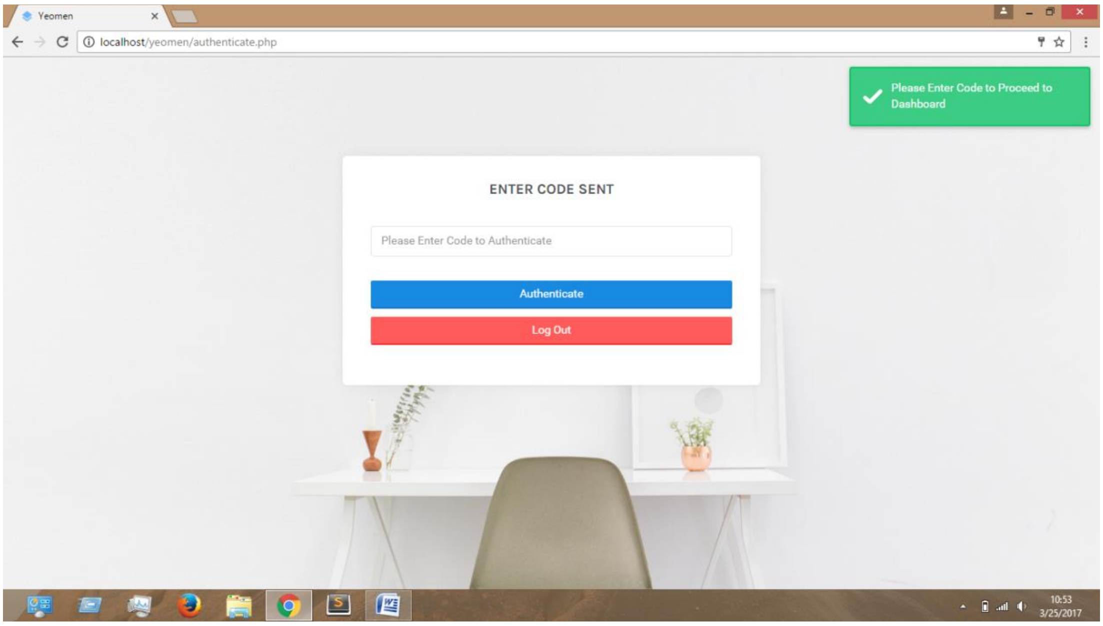
| 1 | www.rroij.com<br>Internet Source | %1 |
|---|---|---|

## Appendix C: Yeomen Screenshots

The screen shot for the Yeomen login system is shown below.



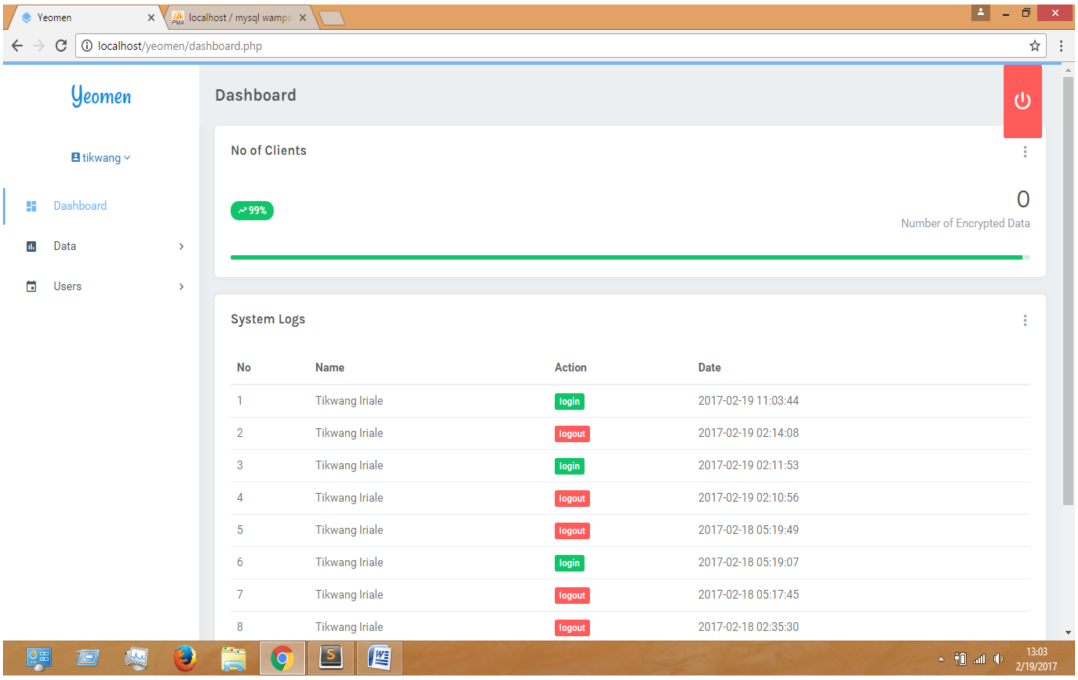
**Yeomen Login Interface**


Please Enter Code to Proceed to Dashboard

Yeomen
localhost/yeomen/authenticate.php
ENTER CODE SENT
Please Enter Code to Authenticate
Authenticate
Log Out
10:53
3/25/2017

**Yeomen 2nd authentication interface after successful log in**

The screen shot for adding, deleting and searching for Cloud clients (users) in the database system.



Dashboard

No of Clients

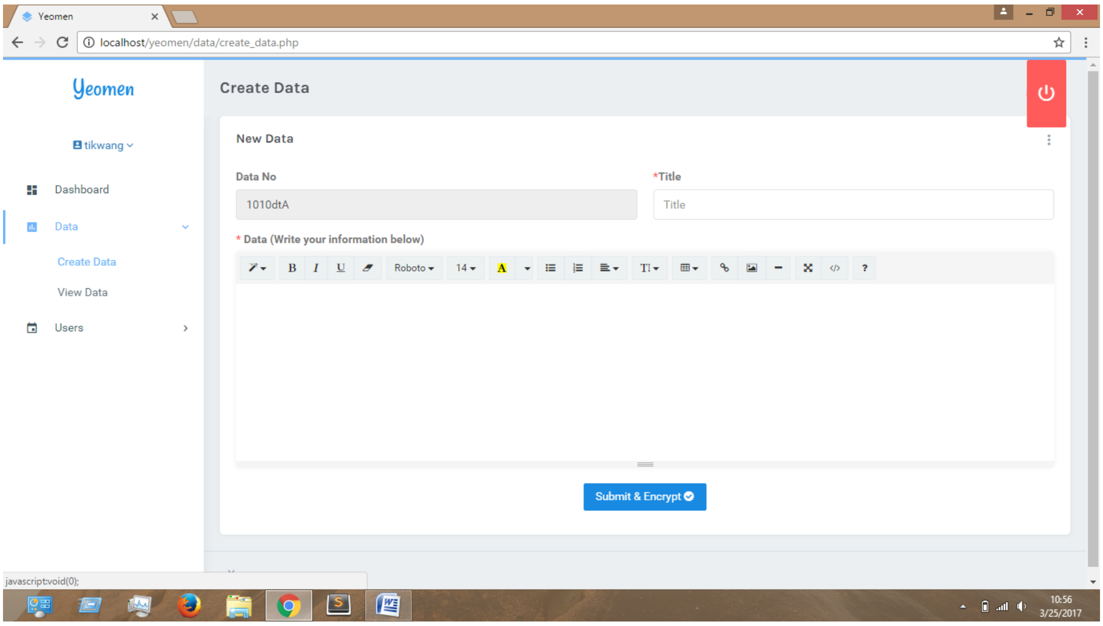
99%

0
Number of Encrypted Data

System Logs

| No | Name | Action | Date |
|---|---|---|---|
| 1 | Tikwang Iriale | login | 2017-02-19 11:03:44 |
| 2 | Tikwang Iriale | logout | 2017-02-19 02:14:08 |
| 3 | Tikwang Iriale | login | 2017-02-19 02:11:53 |
| 4 | Tikwang Iriale | logout | 2017-02-19 02:10:56 |
| 5 | Tikwang Iriale | logout | 2017-02-18 05:19:49 |
| 6 | Tikwang Iriale | login | 2017-02-18 05:19:07 |
| 7 | Tikwang Iriale | logout | 2017-02-18 05:17:45 |
| 8 | Tikwang Iriale | logout | 2017-02-18 02:35:30 |

Yeomen Cloud Dashboard showing system logs.



Create Data

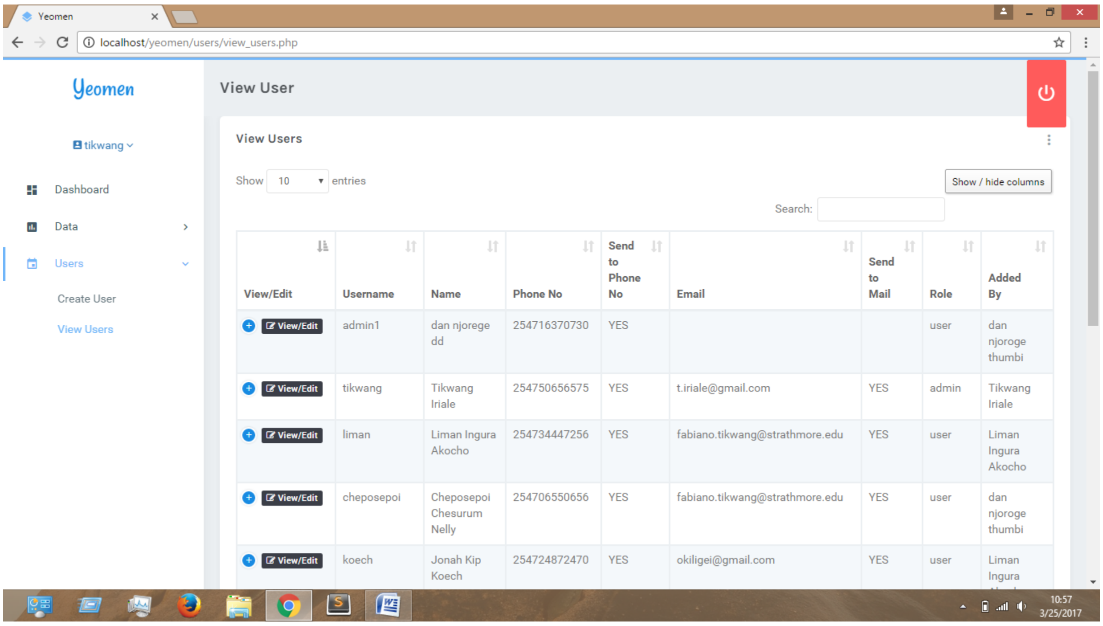
New Data

Data No: 1010dtA

*Title: Title

* Data (Write your information below)

**Yeomen interface for creating data before encryption**



View Users

Show 10 entries

| View/Edit | Username | Name | Phone No | Send to Phone No | Email | Send to Mail | Role | Added By |
|---|---|---|---|---|---|---|---|---|
| View/Edit | admin1 | dan njorege dd | 254716370730 | YES | | | user | dan njoroge thumbi |
| View/Edit | tikwang | Tikwang Iriale | 254750656575 | YES | t.iriale@gmail.com | YES | admin | Tikwang Iriale |
| View/Edit | liman | Liman Ingura Akocho | 254734447256 | YES | fabiano.tikwang@strathmore.edu | YES | user | Liman Ingura Akocho |
| View/Edit | cheposepoi | Cheposepoi Chesurum Nelly | 254706550656 | YES | fabiano.tikwang@strathmore.edu | YES | user | dan njoroge thumbi |
| View/Edit | koech | Jonah Kip Koech | 254724872470 | YES | okiligei@gmail.com | YES | user | Liman Ingura |

**Yeomen interface for viewing, updating data and removing users**

**The Sample of Yeomen system six digit authentication codes sent to both mobile or e-mail depending of choice of the client/user:**

YEOMEN

Hi tikwang, Please use the following Code: 170265 to authenticate your access.

YEOMEN

Hi tikwang, Please use the following Code: 785362 to authenticate your access.

YEOMEN

Hi tikwang, Please use the following Code: 819275 to authenticate your access.

**The Sample of Yeomen system reply to an administrator when a client attempts to log three times into his/her cloud account without success:**

YEOMEN

There might be some attempts to access Tikwang Iriale account illegally. Please alert.