Current Journal of Applied Science and Technology

Volume 43, Issue 6, Page 61-77, 2024; Article no.CJAST.116979
ISSN: 2457-1024
(Past name: British Journal of Applied Science & Technology, Past ISSN: 2231-0843,
NLM ID: 101664541)

Data Security Framework for Protecting Data in Transit and Data at Rest in the Cloud

Percy Nathan Swanzy [a], Arnold Mashud Abukari [b*] and Edward Danso Ansong [a]

[a] Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.
[b] Department of Computer Science, Tamale Technical University, Tamale, Ghana.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/cjast/2024/v43i64387

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/116979

Original Research Article

Received: 05/03/2024
Accepted: 08/05/2024
Published: 13/05/2024

ABSTRACT

Data stored in the cloud is particularly vulnerable to attacks, especially when at rest or in transit. This makes the security of data in the cloud in terms of its integrity, confidentiality and availability a major security concern. While existing studies on cloud data security have garnered attention from cybersecurity researchers, there has been limited focus on developing a comprehensive data security framework that integrates both technical and social measures. The general objective of the study was to develop a data security framework for protecting data at rest and data in transit in the cloud. The qualitative research approach was chosen using interviews, archival records and physical artefacts as the source of data for the study. Using the purposive sampling technique, ten cyber security experts within the banking sector with not less than five years of practice were

**Corresponding author: E-mail: amashud@tatu.edu.gh;*

Cite as: *Swanzy, P. N., Abukari, A. M., & Ansong, E. D. (2024). Data Security Framework for Protecting Data in Transit and Data at Rest in the Cloud. Current Journal of Applied Science and Technology, 43(6), 61–77. https://doi.org/10.9734/cjast/2024/v43i64387*

selected. Thematic analysis was used in analysing the collected data which led to the identification of the factors for the development of the framework. The study developed the framework for protecting data at rest and data in motion in the cloud based on the encryption technologies, installation of firewalls and antivirus as well as access control techniques. First Homomorphic encryption technologies were implemented in the framework to secure both storage devices and web connections. Other security factors were installation of firewall and antivirus. The findings revealed that access and usage control strategies integrate user identification and authentication. Additionally, these strategies incorporate safeguards for confidentiality, data integrity, and non-repudiation, securing both data-at-rest and data-in-motion. The findings also indicated that audit trails provide electronic records that offer security support documentation and history that is used to authenticate operational actions and mitigate challenges with non-compliance. Additionally, the findings emphasized the importance of social strategies such as staff training and industry collaboration in enhancing data security. These strategies aim to raise awareness of security threats and inform best practices for securing organizational data. The study recommends that banks consider both technical and social aspects when implementing data protection security measures especially implementing homomorphic encryption to secure data and implement Cyber Security training policies.

Keywords: Cloud; deployment model; framework; data security; multi cloud.

1. INTRODUCTION

Cloud computing, an emerged technology out of the evolutionary trend and permeation of internet, provides the next generation of internet-based, highly scalable distributed computing systems in which computational resources are offered on demand as a service [1]. Thus, Cloud computing allows data to be processed, stored and accessed over the Internet rather than on the desktop of the user, thus, on premise solution [2,3]. Today, cloud computing has become an emerging computing infrastructure for organizations throughout the world. Organisations now prefer to store their data and applications on the cloud instead of on their desktop computers [4]. This shift to cloud computing is hinged on benefits such as unprecedented scalability, flexible, pay-per-use charging models, and automatic provisioning of (physical or virtual) servers that enable end users to order and provision on-demand platforms at a fraction of the cost and time that would be needed to deploy a comparable, on-premises solution [5,6].

Data stored by organisations can have three forms: data at rest, data in use and data in transit [7]. Data-in-motion refers to data actively moving from one location to another across a network or from a local storage device to cloud storage [8]. These include transactional data such as transfer of funds over a network and data moving across cloud servers. On the other hand, Data-at-rest is data sitting on a computer, a server or somewhere in the cloud [9]. It includes archived data, data on off-site backups and data on physical storage devices such as hard drives and USB flash drives. Data-in-use refers to data that is being processed by one or more applications and not just stored passively on a hard drive [7]. Data is considered the new oil in the modern economy due to the insight and knowledge that can be extracted from it [10].

Cloud Computing, the highest progressive innovations of the century, delivers computing services such as storage, servers, software, networking and more over the Internet to help manage the increasing volumes of data. Networks have moved worldwide and data has been considered in the digital form of bits and bytes with critical data being stored, refined and sent in digital form via networks [11]. It is estimated that the creation of data is multiplying every 18 months [12]. Further, the International Data Corporation (IDC) predicted that from 2013 to 2020, the digital universe would expand by a factor of 10 - from 4.4 trillion to 44 trillion gigabytes and the data volume handled by organizations is increasing 50 times (IDC, 2013, cited in [13]. Consequently, the use of conventional data to store and process data will be increasingly expensive [14]. This coupled with security concerns make organisations unwilling to migrate to the cloud. [15] argue that large organizations are reluctant to switch to cloud services because they have threat of their data being maltreated. This calls for more attention and patronage to cloud computing services with its attendant security challenges to data access, modification and interruption. Data security is an essential challenge concerning the adoption of cloud services.

Organizations face threats posed internally by end users of online systems and externally by hackers, malware, and criminal syndicates. This highlights the need for cloud systems managers to adopt strategic measures that aim to proactively guard against breaches targeted at both data-in-transit and data-at-rest in organizations. Failure to proactively adhere to cybersecurity measures has led to the loss of financial and information resources of organizations. Institutions, particularly, financial and health institutions, are the attractive targets and most vulnerable to cyber-attacks due to their role in intermediating funds and data. The IMF estimates annual potential losses from cyber-attacks on the net income of banks to be around $100 billion globally [16]. Cyber-attacks on firms could result in economic, social and organisational damage which adversely affect the trust of customers [17]. This calls for the adoption and effective implementation of cybersecurity measures to safeguard organizational data. Hence, there is the need to develop an encryption framework that protects data in cloud from interception, modification, and unauthorized access. Existing studies have looked at only the technical dimensions of protecting data in the two states with little or no attention to both the technical and social dimensions of securing data in the cloud. This, therefore, draws the attention to the need for an efficient and wholistic data security framework for protecting data at rest and data in transit in the cloud. Hence, this study attempts to develop data security framework for data at rest and data in transit in the cloud to enhance the security of data at rest and data in transit in the cloud and also ensure high performance. The objective of this study is to develop data security framework for protecting data at rest and data in transit in the cloud.

2. STATES OF ORGANISATIONAL DATA

Data is characterized by three main states; Data-in-motion, Data-at-rest and Data-in-use. Data in each of these states should be protected to prevent security breach [8]. Data-at-rest refers to data residing on a device or a network endpoint. It includes data stored on hard drives, databases, backup tapes, data stores or mobile devices [8]. Data is at rest when it is inactive and not currently being transmitted across a network, actively being read or processed by any application [18]. When data reaches its destination and is at rest, it may be secured by deploying security layers such as database encryption, multi-factor authentication and access controls. Data in motion refers to data that is currently travelling across a network such as data sent through e-mails, instant messages or peer to peer [8]. Data-in-motion also includes data moving over a network from a firm’s central mainframe to various remote terminals [18]. These data should be encrypted to protect it from being accessed or manipulated by an attacker while it is being transferred between the data’s source and destination. Security solutions such as Secured Socket Layer (SSL) and Transport Layer Security (TLS) can be used to secure data-in-motion. Data-in-use refers to data that is being processed one or more application on a computer. It is data that is not just stored passively on a storage medium but being processed by one or more applications [18]. It includes data being viewed by users accessing it through various endpoints. Data-in-use can be secured by controlling access and authenticating users to ensure that only authorised individuals are able to access and manipulate data.

3. DATA SECURITY THREATS

Data security threats are techniques that attackers use to exploit vulnerabilities in a system [19]. Threats also entail persons, objects or any entity that pose danger to a firm’s asset. These threats may be internal or external to organizations. Internal threats are posed by both well-meaning and disgruntled employees in an organization who have authorized access and privileges to a firm’s computer system. They may accidentally or deliberately modify and destruct data [19]. External threats to an organization’s internal data are posed by competitors, hackers, viruses, and natural disasters. Organizations should be able to track and report relevant information to enable them detect suspicious activity, identify potential threats, and proactively improve data security [20]. For example, an account being disabled due to a certain number of failed login attempts could be a warning sign that a system is under attack. The various attacks deployed to compromise an organization’s data include Denial of Service attacks, malicious codes, phishing, SQL injection attack, spoofing and social engineering.

4. DATA SECURITYY STRATEGIES

A strategy refers to a set of plans or decisions made in an effort to help organizations achieve their objectives. For organizations to keep their technological infrastructure and information resources secured, there must be in place security strategies to serve as a roadmap towards this end. [21] defines information security strategy as an art of deciding the effective utilization of appropriate defensive information security technologies and measures to safeguard an organization's information infrastructure against internal and external threats by offering confidentiality, availability and integrity at minimum cost. Extant literature has classified information security strategies into several categories. These include Deterrence, Prevention, Detection, and Response approaches [22].

5. DETERRENCE APPROACH

The deterrence approach employs disciplinary actions to guide individual behaviour and attitudes towards the use of organizational information systems [23]. Horne et al [21] argues that this is accomplished through the use of Security policies, Security awareness and training programs as well as computer monitoring software. Security policies provide guidelines for the effective use of an organization's IS resources as well as sanctions for breaching security policies. Computer monitoring include tracking employee internet use, performing security audit and recording network activities. The effectiveness of the deterrence approach is influenced by the certainty of sanctions and severity of sanctions. Having a security policy and reinforcing it with training and awareness program has a deterrent effect on employees by increasing perceived threat of punishment for breaching security policies. Similarly, putting in place checks to monitor computer activities increases the perceived chances of detection and punishment for such behaviour [21].

6. PREVENTIVE APPROACH

The preventive approach involves safeguarding an organization's information assets prior to attack by deploying countermeasures against unauthorized access, modification, disclosure or destruction [24]. Some technical preventive strategies include authentication, encryption, firewalls, vulnerability testing and patching. Access control mechanisms aim at enhancing data confidentiality and integrity. It is concerned with limiting the activity of legitimate users of a computer system based on specified by authorizations [25]. It works by checking the rights of users against a set of authorizations defined on the system. The set authorization may allow or restrict users from making changes to information on the system. It is crucial to protect enterprise data from unauthorised parties by encrypting it prior to transmissions beyond the system where it is stored or generated. Encryption is a security tool that converts plain text into non-readable cypher text using complex mathematical formula and a unique key. An encryption key is used to decode data so that it becomes readable to the intended party privy to the information [26]. Data in transit may be protected by encrypting e-mail servers, encrypting web connections using a secured socket layer (SSL) or transport layer security protocols (TLS) as well as making use of End-to-End encryption. Data at rest could be secured by deploying a full disc encryption or File encryption. A full disc encryption (FDE) automatically encrypts all files saved to a hard drive. With file encryption, encryption takes place on a file by file basis. Encryption keys should be protected by using key management systems that separate encryption keys from the encrypted data [18]. By doing so, even if attackers gain access to a database, they will not be able to decipher the encrypted data.

A firewall refers to a network security system that monitors and controls incoming and outgoing network traffic based on advanced and a defined set of security [27]. They are tools that reside at the border of two networks for the purpose of inspecting traffic moving from one network to the other. A firewall prevents unauthorized access to and from an organization's internal network. All data packets that enter or leave an organization's internal network pass through a firewall which examines and block those that do not meet some specified security criteria. It comes as either software or a hardware device. Vulnerabilities are weakness in a network or a software that exposes it to security threats [19]. Weaknesses in a system's security is identified by testing for vulnerabilities. Vulnerability testing is the process of identifying loopholes in a computer system that makes room for a computer system to be exploited [28]. Once vulnerabilities are identified, patches are installed to address them. Wireless network scans, database scans and application scans can be used to identify various weak points that make the system susceptible to attack.

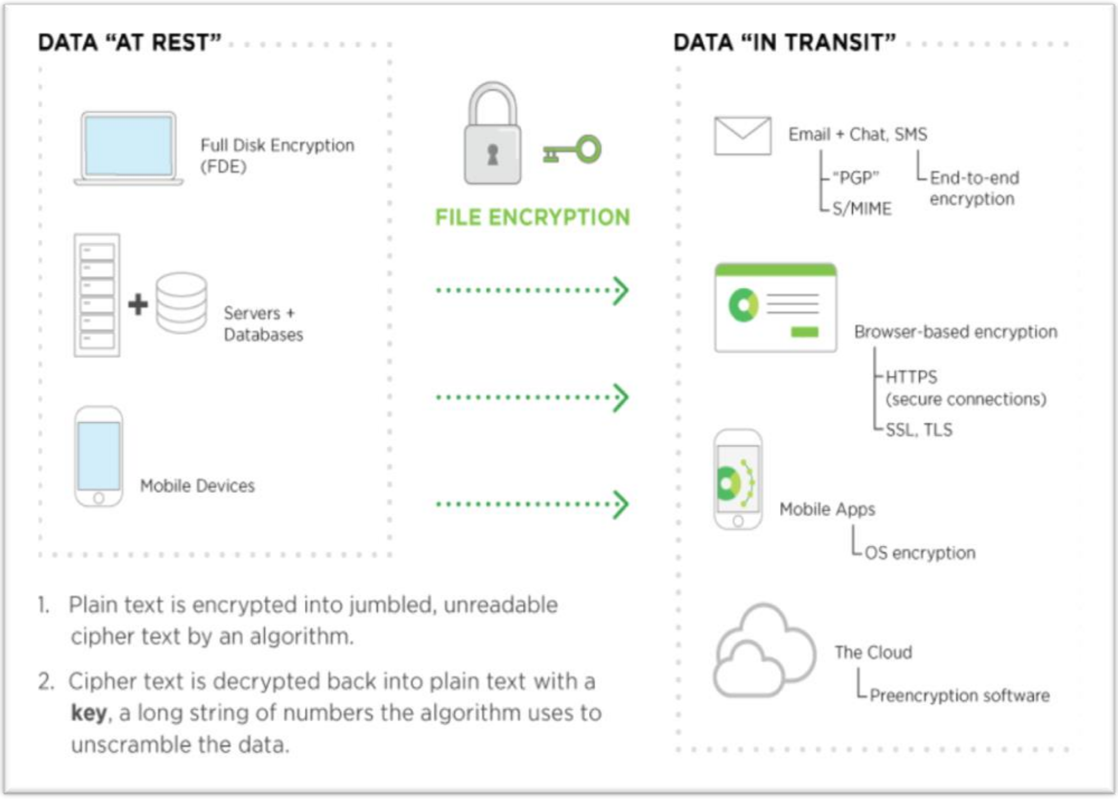
DATA "AT REST"
Full Disk Encryption (FDE)
Servers + Databases
Mobile Devices
FILE ENCRYPTION
DATA "IN TRANSIT"
Email + Chat, SMS
"PGP"
S/MIME
End-to-end encryption
Browser-based encryption
HTTPS (secure connections)
SSL, TLS
Mobile Apps
OS encryption
The Cloud
Preencryption software
1. Plain text is encrypted into jumbled, unreadable cipher text by an algorithm.
2. Cipher text is decrypted back into plain text with a key, a long string of numbers the algorithm uses to unscramble the data.

Fig. 1. Encryption data protection methods for data-at-rest and data-in-motion

7. DETECTIVE APPROACH

When an attacker is able to penetrate a system, the next line of defence is detection. The detection approach aims at pinpointing specific security behaviours to enable organizations react to them [23]. Detection takes the form of identifying malicious behaviour, intrusion, misuse and attacks against servers [23,24]). Some detection tools include intrusion detection systems, audit trails, antivirus software and Vulnerability testing. Attackers may employ an intrusion attack to compromise an organization's networked system. An intrusion attack refers to any unauthorized activity on a computer network that violates the security policies of a networked information system. These attacks are made known to network administrators through the use of an intrusion detection system. An intrusion detection system monitors activity on a networked system to identify suspected intrusions using anomaly detection and misuse detection [29]. Anomaly detection builds profiles for normal activities and issues alerts when an activity deviates from the normal operations of the system. Misuse detection, on the other hand, construct patterns based on known attacks and vulnerabilities and report alerts when monitored activities matches the known pattern [29]. Anti-virus software is a malware detection and removal tool used to protect computers. Anti-virus software detects malware using a signature dictionary. The signature dictionary contains patterns of known codes that enables the recognition and detection of viruses. It is important that antivirus software is regularly updated in order to detect newly developed malware. Audit trails refer to information provided by a computer system concerning its inner workings and behaviour [30]. Audit trails enables the detection of system misuse by generating evidence of records that chronologically shows the activities of system users. Each user activity is recorded which enables the identification of individuals who modify data or misuse the system.

8. RESPONSE APPROACH

The response approach aims at taking appropriate corrective actions against identified attacks [23]. The response to the attack entails two phases; the reaction phase and the recovery phase [31]. The reaction phase is where appropriate action is taken against the attacker. For instance, blocking an attacker's IP address or dropping a connection. The recovery phase is where the situation is restored to its original state. For example, restoration of back-up data [23].

8.1 Cloud Computing

The emergence of Cloud Computing (CC) is increasingly becoming an important consideration for Governments and enterprises. A recent study has described cloud technology as one of the most significant disruptive technologies which will develop over the next two decades, with major implications for markets, economies and societies. There seem to be varied definitions of CC. For instance, the US National Institute for Standards and Technology (NIST) defines CC as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. Also, cloud computing is where dynamically scalable, device-independent and task-centric computing resources are obtained over the internet, with any charges being on a per-usage basis. Out of these two definitions, the widely used and acceptable is that of NIST. Therefore, in this study, CC is described as a computing environment where software applications, computing hardware and other resources are provisioned to authorized users via a network instead of these resources residing on the local devices and location of users. This will allow any internet-enabled computer or a smart device to access resources on the cloud platforms without any other connection to the hardware that holds the resources.

8.2 Cloud Service Model

The NIST definition of cloud computing defines three cloud service delivery models.

Software as a Service (SaaS): This model is the uppermost layer in the cloud structure which affords consumers the ability to access cloud applications from multiple client devices and interfaces. There is much limitations on a SaaS as users are restricted very few user level customizations such as operating systems, servers, storage, or network [4]. SaaS has become very popular with the deployment of enterprise systems as it off-loads the burden of system upgrades and maintenance for businesses. Some common SaaS include, Workday, Concur, Google Apps, Dropbox, Cisco WebEx, Salesforce, GoToMeeting.

Platform as a Service (PaaS): As a middleware (or middle layer) PaaS presents users with an Integrated Development Environments (IDE) comprising of development tools, framework, architecture and programs which enables the user to build, test, run and deliver web-based applications. PaaS has better controls than the SaaS this is also limited to only user-developed application. Examples of PaaS include Google App Engine, Windows Azure, Heroku, AWS Elastic Beanstalk and OpenShift.

Infrastructure as a Service (IaaS): As the bottom layer, IaaS deals with computer hardware (network storage, virtual server/machine, data center, processor, and memory) as a service. IaaS supports the revolution in the business investment in IT infrastructure. The capability provided to the consumer is the provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)”. This allows the users various virtual computing resources such as storage, servers, processing, or networks. It lets the user run arbitrary software, including operating applications and systems. The user has full control of storage and operating systems. He also has a control over the applications of a certain limit of control over the networking facilities.

[15] identifies *a fourth* cloud service delivery models namely;

Anything as a service (AaaS): This refers to the collective varied service that runs can be provisioned over a virtualized system. [15] marks all such variabilities as “X” which may refer to anything or everything as a service. In this finding service becomes substitutable in cloud landscape. The cloud system can support the large resource to specific, personal and granular requirements using Storage as a Services (StaaS), Data as a Service (DaaS), Communication as a Service (CaaS), Security as a Service (SecaaS), Routing as a Service (RaaS) [15].

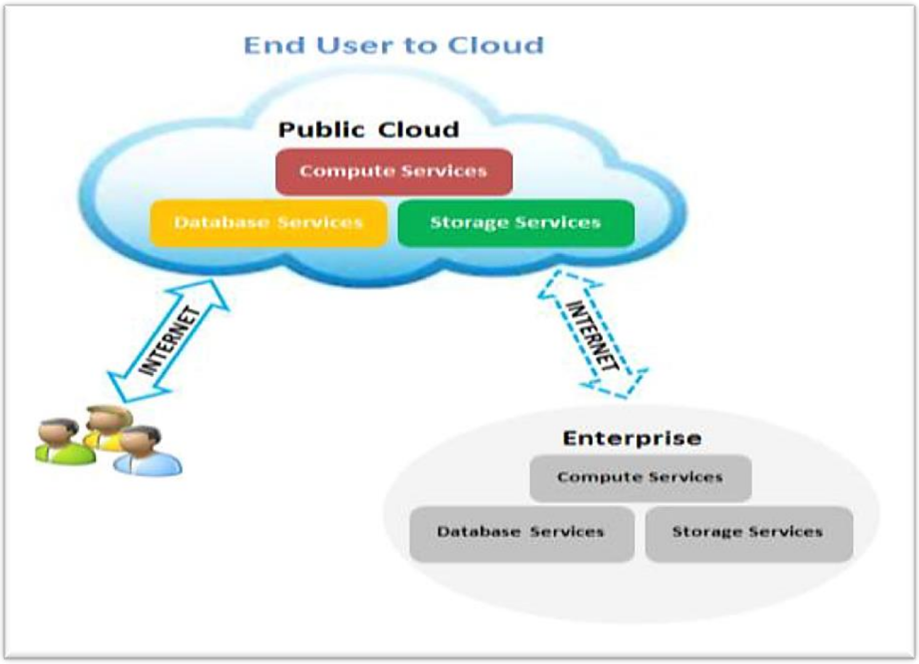

Fig. 2. Public cloud deployment model [4]

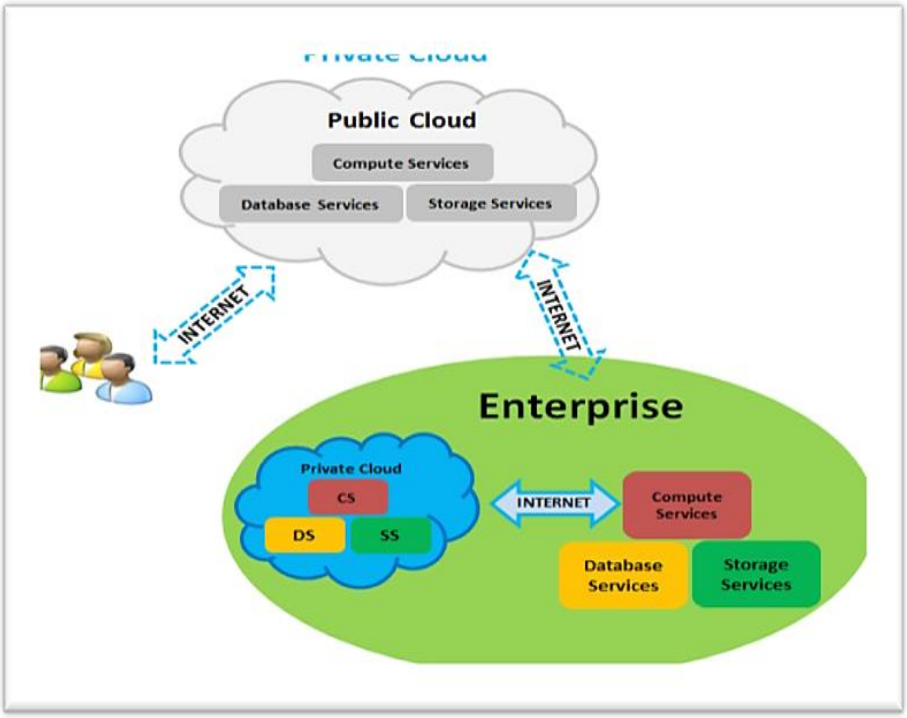

Fig. 3. Private cloud deployment model [4]

8.3 Cloud Deployment Models

There are four cloud services models that can be deployed within the cloud community; these are public, private, hybrid, and community cloud [3].

Public Cloud Deployment Model: Public cloud deployment model makes the cloud infrastructure available to the public via the internet. The infrastructure of public cloud deployment is owned by an organization that provides cloud services or by some business, government or academic institution. It is worth knowing that the term “public” does not connote free. Running and managing public cloud services requires significant amount of investment and thus the reason for its ownership by usually by large corporations. This model enables clients to set their required security levels and negotiate for Service Level Agreements (SLA) [3]. Examples of public cloud service providers include Amazon Webs Services (AWS) deploying Elastic Compute Cloud EC2, Google App-Engine, and Force.com [4].

Private Cloud Deployment Model: The private cloud deployment model makes the cloud service infrastructure available to specific organisations on a more private basis. The ownership, management and control of the infrastructure can be done by either the focus organization itself or by a third party. Again, the infrastructure can be set within the organizations’ premises or away from the premises. There are several reasons for setting up a private cloud within an organization; these are (i) High-security considerations with concerns of data trust and privacy, (ii) Optimization of the usage and allocation of internal resources and (iii) The cost effectiveness compared to data transfer between local IT infrastructure and a public cloud.

Hybrid Cloud Deployment Model: The “Hybrid Cloud” deployment model refer to the combination of two or more separate clouds models (private, community or public) amalgamated by common technology that enables data to be seamlessly portable within the service. This cloud deployment model is particularly signed onto to by firms that have an aim to make effeicient use of system resources, improving core competencies through outsourcing minor business functions onto the cloud as well as maintaining its core activities within the premises through the private cloud [4]. According to the Cloud Security Alliance (CSA), deploying a Hybrid cloud model system is aimed at resolving issues that pertain to standardization and the need to create cloud interoperability. Fig. 4 shows Community Cloud Deployment Model.

Community Cloud Deployment Model: Deploying a community cloud model is meant to provide support to certain types of communities which are similar in terms of requirement, examples of which include security requirements, policies and compliance considerations, such that the infrastructure of the community cloud is made available across several organizations at te same time [4]. The infrastructure for a community cloud model may be set up within or outside the premises of an organisation and managed by the organization itself or be entrusted in the care of third-party organisation for its management. Up to a certain level, the cloud community behaves with demographical

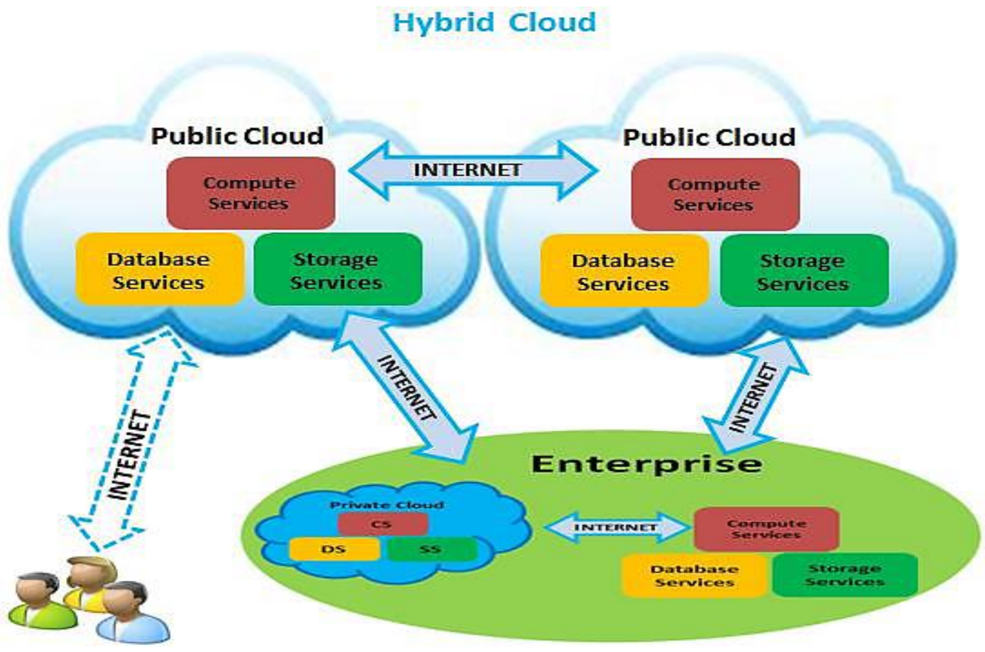

Fig. 4. Hybrid cloud deployment model [4]

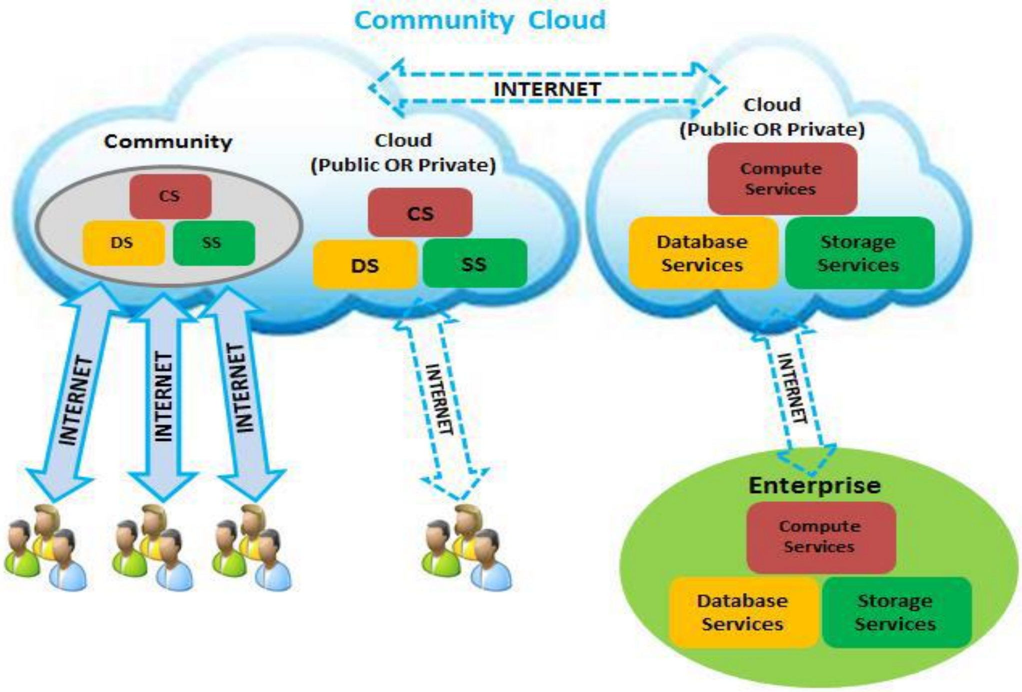

Fig. 5. Community cloud deployment model [4]

balance and economic scalability [4]. For instance, cloud services offered by government organizations such as Passport services, Revenue Authority, National ID, Electoral Commissions as well as Visa and Immigration may deploy a community cloud. As such citizens can access the relevant information related to the above-mentioned services at various department levels (Local governments, state or regional) via the internet. The figure shows Community Cloud Deployment Model.

9. MULTI-CLOUD INFRASTRUCTURE

Multi-Cloud refers to the synchronised use of multiple cloud computing platforms, providers, and/or offerings in a single heterogeneous architecture. Or simply put, the right cloud for the right purpose. The term “multi-cloud” is comparable to the terms “interclouds” or “cloud-of-clouds”. These terms suggest that cloud computing should not end with a single cloud. In a multi-cloud deployment model, a cloudy sky integrates a number of shapes, colours and nature of clouds which leads to different implementations and administrative domains. Most studies done recently have been focused on the multi-cloud environment which control several clouds and avoids dependency on any one individual cloud. Moving from single clouds or inner-clouds to multi-clouds is reasonable and important for many reasons. Additionally, over 80% of company management “fear security threats and loss of control of data and systems”. Researchers are of the assertion that the main purpose of adopting to multi-cloud service platform is to make improvement on the service offered by single clouds services by enabling distributing reliability, trust, and security among multiple cloud providers.

10. METHODOLOGY

This study employed both primary and secondary data. Researchers postulates that evidence for finding studies may come from six sources namely documents, archival records, interviews, direct observation, participant-observation, and physical artefacts. Further, according to literature, observation (fieldwork), interviews, documentation and the researcher’s impressions and reactions are the main data sources used in qualitative research. The source of data for this study were interviews, archival records and physical artefacts. Firstly, primary data that provide important and relevant data sources was used to gather first-hand data that has not been generated by others. Through semi-structured interviews primary data was gathered. Moreover, documents and records from the finding organisation were also examined to aid in better development of the encryption framework.

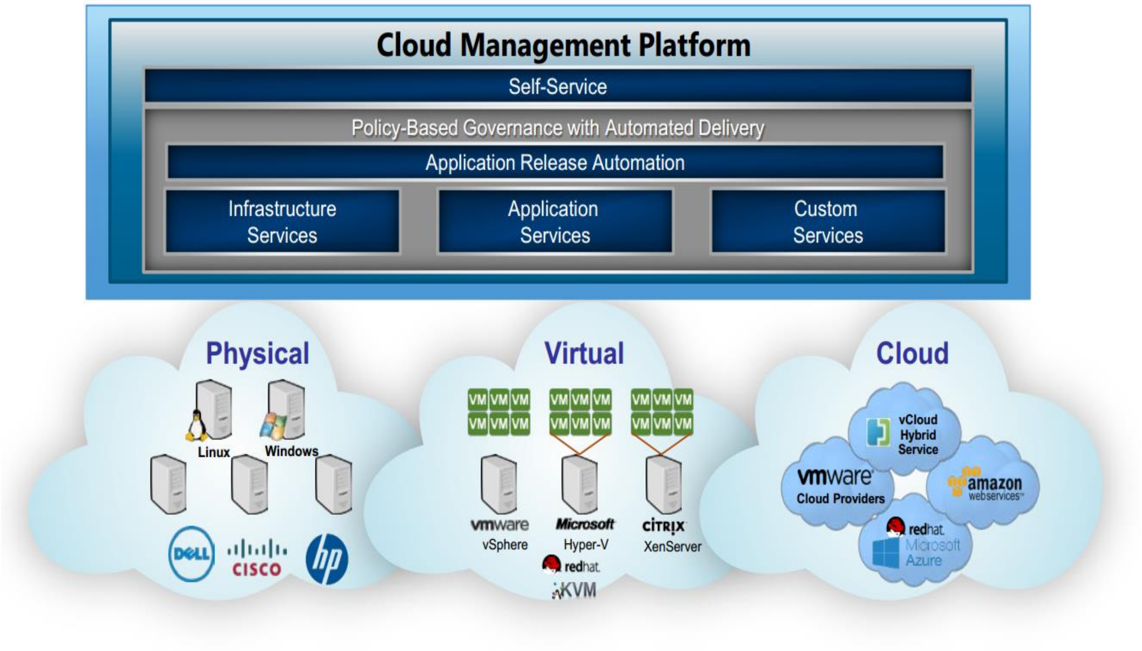

Fig. 6. Multi-cloud Infrastructure

10.1 Sampling Technique

Sampling is defined as a process of selecting or choosing samples from a group or population to become the foundation for studying a total or mass population in order to attain data capable and reliable enough to solve or address the research problem. A sample is a subset of a larger population. A population is a complete group of entities within which the researcher wants to explore, understand or project a social phenomenon. Researchers often make conclusions on a total population by studying or investigating a sample. In qualitative research the objective of the researcher is to study a phenomenon from the perspective of a sample that has experienced the phenomenon. Qualitative research is much more focused on samples which improve understanding rather than representativeness. Therefore, qualitative researchers often use a non-probability sampling approach in which the probability of selecting a particular member or respondent is unknown. For the purpose of this study, a purposive sampling technique was selected to sample the respondents. The study adopted a purposive sampling technique in order to select ten (10) Cyber security and information technology experts within the banking sector with not less than five years experience. The purposive sample is seen as an appropriate sampling technique because it is often used in exploratory research, for selecting particular findings for an in-depth investigation. This helped the researchers to obtain information that is peculiar to data at rest and in transit protection in the banking sector.

10.2 Data Analysis

Data analysis is a “systematic and essentially taxonomic process of sorting and classifying collected data”. The research assert that data analysis involves three main processes which are data reduction, data display, and drawing and verifying conclusions. Data condensation as “the process of selecting, focusing, simplifying, abstracting, and or transforming the data that appear in the full corpus (body) of written-up field notes, interview transcripts, documents and other empirical materials”. This research further asserts that a “display is an organised, compressed assembly of information that allows conclusion drawing”. Meanwhile the data reduction and demonstration help in drawing meaningful conclusions from the data. The initial findings and conclusion from the data condensation and display stage were verified through pattern-matching of themes and ensuring that the conclusion or finding is representative of the data. Conclusions were finally presented in the form of findings reflecting the development of the encryption framework.

11. RESULTS AND DISCUSSION

11.1 Technical Data Protection Measures

Technical mechanisms encompass the technology that is the hardware and software security mechanisms instituted as well as the tasks performed by these systems in the organizations efforts to protect its sensitive data. The analysis of the findings revealed that banks as part of their data security strategy in compliance with the regulations of the bank of Ghana put in place a number of technological solutions that are logically or physically set up to secure both data at rest and data in motion.

A key security measure towards securing data was the control of access to information internally among the various departments. In a discussion with an IT security expert, he explained that

> *"Am in the corporate communication and management department and we have a departmental drive containing all our files. There are separate drives for IT, retail, communication and other units, which stores departmental data such as memos, files, artworks, downloaded attachment, company proposals, and any other files. So, if someone is at retail or HR, that person cannot get access to our department's drive. All those in our department have access to our drive but if you are not from the department, you won't have access."*

The respondent emphasised that all employees have a unique ID and password which is required to log into computers. Employees can only access content from a department's drive only if they are from that department. Otherwise, they can only get access to the universal drive unless an IT person is authorised to map their departmental drive to that particular computer before they gain access.

> *"if I come to audit department and log into the system with my details, the departmental drive will not show. I will only have access to the universal drive. All the drives are networked, so if I want to use another computer away from my department, someone from IT has to map my department's drive to that particular machine so that I can get access it. But if you are not in that department, you will only have access to the universal drive.*

Another IT security expert indicated further those privileges to information are defined based on an employee's role in the bank and approval is sought if an employee has to access some information above their set privileges. The respondent noted that

> *"If it is not inline to your job, you don't get access to the core banking application or main databases. A teller will have access to the main core banking application. A teller will be able to able to post transactions, a customer service person can't. If somebody has to do an activity above their privilege, they are required to seek approval to perform that extra role"*

To authenticate and control access to data, the banks have integrated an IT security solution known as "Safe-T" with the T24 banking application and internet banking. This application is used to enforce two-factor authentication associated the internet banking and also monitor data exchange to ensure that only the requested information is generated for users on the system.

Another mechanism that is used to detect data breach is the use of system logs. According to an IT manager of a bank, the Temenos T24 banking system logs all user activities on the network and should any employee manipulate or breach their privileges, it can be traced back to them by the audit or IT team. With respect to external intrusions, the banks have been experiencing a number of intrusion and spoofing attempts by outsiders. The banks firewall help identify and block attempts by outsiders who attempt to gain access to bank's systems. One IT security expert stated that

> "*We see people trying to hack into the network to get some information, the firewall is helpful in blocking them. we get notifications and the system collects all logs as people try to access the network.*

There have also been several findings where employees receive malicious e-mails from outsiders to solicit sensitive information. Some attackers are able to send messages from addresses that appear to be coming from the bank's domain e-mail system. This is intended to lure employees to believe they are receiving the message from a fellow employee from the bank. Most of these emails contains embedded links that redirect to web pages that request for sensitive information. A cyber security expert explained that usually in the banking sector all suspicious emails received are quarantined until their authenticity is verified. He added:

> "*When we quarantine those address, we inform the employee of the email sent and convey our suspicion to them just to verify from them if they know the person".*

Banks also deploy surveillance measures in the form of CCTVs to monitor and record on-premise activities. In finding of a breach, the recorded footage is reviewed to identify events that led to the breach. Moreover, the various entrance to sensitive bank premises is secured with biometric doors to prevent unauthorised entrance to the premise. To secure data on banks' network, personal computers and external devices that are connected to bank's network port is blocked. Moreover, antivirus software is installed on all computers to protect against malware. The encryption protocol restricts access to the bank's network where only computers that are listed on the banks network domain with updated antivirus software can connect to the network. A cyber security expert indicated that:

> *"Port log" is responsible for the network ports. It checks the domain of the pc being used and whether it has an antivirus. Antiviruses are installed on all servers and systems. These are the policies we've set. If somebody puts in the cable in a computer which is not on the domain name list, it shuts off the network for that pc and the person can't have access to the network. So, when a network service person realise that a port is supposed to be active but if it is off, he can check and find that the PC is not in the domain or the antivirus is not updated which is why it is off."*

11.2 Data at Rest Security Measures

Despite the technical security controls, attacks can be carried out by targeting the banks' employees by means of social engineering techniques. Employees are, therefore, trained to create security awareness. Thus, the security of data can be tampered with by the employees of an organisation. The protection of data at rest at the organisation then usually has social dimensions. With respect to the social dimension of data security, banks carry out training and has a general policy to ensure conformity to established standards. There is also legal regulations and policies that govern acceptable use of organisational computing resources and data protection. The analysis of documents revealed that when new employees are recruited into the banking sector, they sign an agreement form that acknowledges their responsibility towards protecting any information which they are privy to by virtue of being employees from outside parties. With respect to training, seminars are held to educate employees on cybersecurity. However, there is no fixed schedules for such training. An IT expert iterated that:

> *"We once in a while engage E-crime and few other bodies to do general cybersecurity training of employees. This quarter there was one training for about 3 days on cybersecurity stuff".*

The findings further revealed that employees in the banking sector receive IT security tips in their e-mails and this makes up for new or existing employees who were not around during the training. There is also system auditing. The IT security expert explained that banks systems are audited every 6 months and the system logs helps trace individual activities on the banks network.

> *"Every six months, there is audit done across the various departments and we look at the logs and all posted transactions and if something looks fishy or a person has more privileges than assigned, they look into it. But there hasn't been internal breach anyway."*

It also found that in the event of an internal breach, culpable employees are referred to a disciplinary committee for appropriate actions to be taken. However, there is no clearly spelt out sanctions to serve as deterrence to employees. With respect to how customers are protected against cyberthreats, it was identified that e-mail alerts are sent to them periodically on protect themselves against cyberattacks. A Cybersecurity expert explained that:

> *"Customers are informed on measures such as checking for "https" on the address bar when using the internet banking service and also to avoid sharing or writing down account numbers and pin codes in insecure places"*.

Regarding measures are in place should attackers be successful in their attempts to breach the banks security protocols, the Cybersecurity expert noted that:

> *"Though there have not been successful attacks yet, there is an incidence response policy that specify how to investigate and take corrective actions should such breaches occur. We will try to find out how the incident occurred and prevent its occurrence in the future".*

11.3 Analysis of Findings

From the Findings, access control mechanisms and responsibility matrix were built into the Temenos T24 enterprise software which integrates the activities of all the functional units of the bank. The solution being hybrid cloud-based application with an on-premise data backup connected all the four branches of the bank gives real-time data access and visibility. The findings further revealed that the enterprise system supported other legacy systems still in use at banks. The provision of online services and the constant transmission of data across departments and branches heightened the risk of losing sensitive financial, transactional and customer data to intruders. Ensuring that the right user gains access to the relevant information pertaining to their functions and needs became critical. Hence, from the findings, it was revealed that banks applied the Safe-T Zero Trust security architecture. Safe-T zero trust architecture according to the finding had three core security functions namely, Adaptive Access to Data, Data Usage Control as well as Data Usage Audits and Reports. The Safe-T Zero trust security architecture performed tasks such as user authentication and verification. This solution was not only applied to the functional control systems and modules but also the front end online and mobile banking for customers. The finding revealed that customers had to go through a two-factor authentication where the customer enters their unique user's name and passcode as well as verify their identity by entering a code sent to their mobile devices. With a user signed into either the online, mobile or even the departmental functional systems, the system performed a task of data usage control. Based on the organizational acceptable use policy for governing banking activities the solution managed allowed usage methods as well as detect usage associated risks. Finally, the findings revealed that the security solution also performed audits and presented audit reports per user and application for appraisal and risk assessment.

As part of the technical data security measures, the finding revealed that banks in their bid to secure both data at rest and data in motion is leveraging the capabilities of antivirus programs, hardware and software firewalls and Encryption methods. There are many threats plaguing the financial sector including, phishing attacks, cracking, ransomware, malware and the like which has the potential to compromise data integrity, availability and confidentiality. banks as such from the finding uses the Kaspersky Enterprise Security Anti-virus which provides preventative and detective security for the bank. The finding revealed instances where staff against company policy insert infected foreign flash drives into workstations. However, due to the system antivirus, the malicious contents are usually quarantined and neutralised before any data get destroyed or compromised.

Also, banks use a next-generation firewall (NGFW) which according to the findings combines data packet inspection and keeps track of whether or not each packet is part of a Transmission Control Protocol (TCP). Also, it includes some variety of deep packet inspection, as well as network security systems, such as intrusion detection and prevention systems, denial of service attack protection and malware filtering. The NGFW serves as a bridge inserted inline across a network connection and looks at all the traffic passing through that point to ascertain source and destination legitimacy. Finally, internal and external email communication, file sharing and web services are protected by encryption technology. The finding indicated that banks has a Secure Socket Layer (SSL) which secures web traffic from their banks web servers to other systems and devices. The SSL was noted to be using strong Transport Layer Security (TLS). To ensure authenticity and security certificate verification BANKS website runs on the Secure Hypertext Transfer Protocol (HTTPS) which encrypts data in transit from the banks online servers helping prevent Browser Exploit Against SSL/TLS (BEAST) attacks and Man-in-the-Middle attacks. Finally, banks have a Full Desk Encryption (FDE) protecting the hard drives in the on-premise servers given full protection to data as they rest on these storage devices.

With increasing cyber threats, banks had put in place a lot of technical security measures which as identified encompasses hardware and software performing various tasks to assist in achieving total data security. From the finding, it was realised that physical access to the banks facilities, server rooms and computing devices by unauthorised personnel posed a threat to the integrity, availability and confidentiality of data-at-rest. Again, it was revealed that much of the organizational strategic data that assured the bank some competitive advantage and could not be accessed remotely, needed protection as well. In response to that, the bank has surveillance system and authorized entry check systems that ensured real-time recording and logging of all movement on all banking facilities. These included CCTV camera's, fire detection systems and biometric door access to server rooms and other sensitive rooms in the Bank.

The findings revealed that banks have a strong organisational structure that helps them thrive to offer a variety of financial services. End users of the banking enterprise system covers staff from all functional units including, retail department, corporate communication and brand management, human resource, Information Technology, Risk department, Audit, Finance, Legal, Underwriting, Treasury and Collateral Management departments. Again, the Chief Executive Director, Executive director for business and the executive director for operations also interfaced with the Executive Support systems as well as the Decision Support Systems for oversight, planning and monitoring. The management of banks bank according to the finding came to a realization that despite the robust technological security protocols implemented to safeguard organizational data, the vulnerabilities of the internal staff presented the greatest that could defuse the technical endeavours.

The finding revealed that as part of the responsibilities of the Human Resource Management department in collaboration with the information technology department new recruits were taken through training on acceptable use as well as sensitization on security threats and how to safeguard against them. From the finding, both old and new staff were given periodic cybersecurity training usually by cybersecurity experts. These trainings were however not structured meaning they are organized haphazardly and are usually targeted at equipping staff and management with new threats in the cyberspace and how they can mitigate human errors that usually can lead to data leakage, social engineering and hack attacks. These trainings are mandatory for all staff with strict managerial enforcement.

Finally, the finding revealed that customers themselves present another vulnerability to banks as the limited know-how of some customers on cybersecurity issue could expose them to cyber-attacks which would invariably affect the credibility and service quality of the bank. As such banks IT departments and the customer relations team through traditional and social media, email and word of mouth continue to sensitize unsuspecting customers of the threats that looms online as they utilize mobile and online banking services. Alerts are sent to customers who have opted for email notification every month on phishing attacks, social engineering and do's and don'ts that can protect them from cyber-attacks. The finding reports of instances where some customers had their monies stolen due to negligence and cyber illiteracy, however, such occurrences have drastically dwindled as a result of the sensitization campaigns. It was also mentioned that the Central Bank of Ghana is also supporting these efforts with public releases and cautions to the public.

11.4 The Proposed Framework

The researchers based on the findings in the study have proposed a framework for both data-in-motion and data-at-rest for the consideration of organisations intending to safeguard their data in the cloud. The proposed framework presented in this research aims to improve security of data in the cloud by leveraging on the potentials of Homomorphic Encryption as presented by [32].

Table 1. The proposed framework implementation measures

Measures	Data-in-Motion	Data-at-Rest
Training	✓	✓
Physical Security	✗	✓
Industry Collaboration	✓	✓
Legal and Regulatory Structures	✓	✓
SSL	✓	✗
Antivirus	✓	✗
Encryption of Data	✓	✓

Table 2. Security attributes of the proposed framework

Approach	Data state	Attributes
Multi-Factor Authentication (MFA)	Data-at-rest	Confidentiality
Homomorphic Encryption	Data-at-rest (Cloud), Data-in-transit	Confidentiality, Integrity
Data Loss Prevention (DLP)	Data-at-rest, Data-in-transit	Confidentiality, Availability
Data Migration Framework	Data-in-transit	Confidentiality

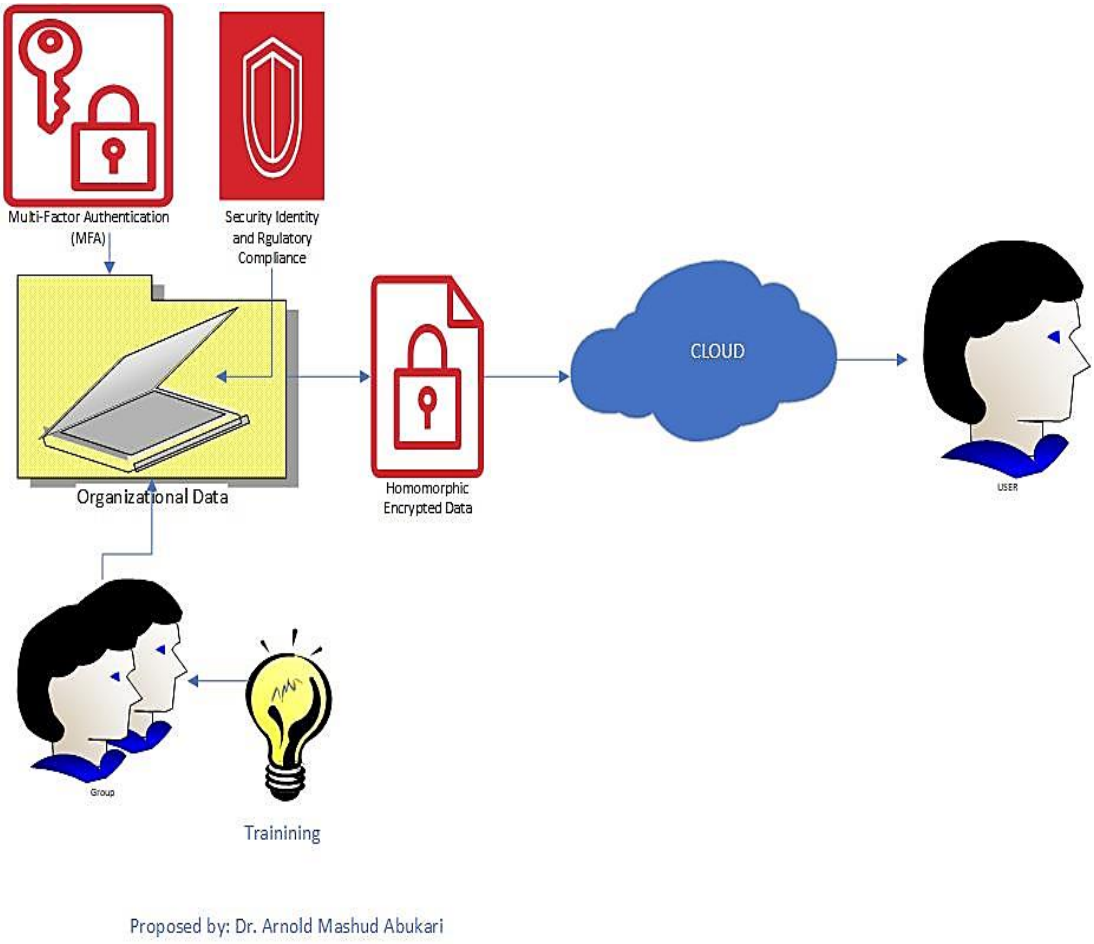
Multi-Factor Authentication (MFA)
Security Identity and Rgulatory Compliance
Organizational Data
Homomorphic Encrypted Data
CLOUD
USER
Group
Trainining
Proposed by: Dr. Arnold Mashud Abukari

Fig. 7. The proposed framework

The proposed framework adopted Homomorphic Encryption, Multi-Factor Authentication (MFA), Data Loss Prevention (DLP) and Data migration concepts to ensure a secured data-at-rest and data-in-transit.The security attributes of the proposed frame is presented in Table 2.

12. CONCLUSION AND RECOMMENDATION

The general objective of the study was to develop a framework for protecting data at rest and data in transit in the cloud. To do this, the data at rest and data in motion activities of banks were assessed together with the various infrastructure used in securing data in these two states. Further, secondary sources such as literature on data at rest and data in motion were studied. To meet the above stated general objective, the qualitative research approach was chosen since the study sought to examine how banks' two states of data in the cloud is secured and also to develop a framework for protecting data at rest and data in transit. The study used interviews, archival records and physical artefacts as the source of data for the study. Using the purposive sampling technique, ten (10) Cyber security and information technology experts within the banking sector were selected to participate in the study.

Thematic analysis was used in analysing the collected data which led to the identification of the factors for the framework. The study developed the framework for protection of data-at-rest and data in motion in the cloud based on the factors and findings. First encryption technologies were implemented in the framework to secure both storage devices and web connections. Other security factors were installation of firewall and antivirus. Also, the findings revealed that access and usage control technical strategies integrate user identification and authentication, confidentiality, data integrity and non-repudiation safeguards in securing data-at-rest and data-in-motion. The findings also indicated that audit trails provide electronic records that offer security support documentation and history that is used to authenticate operational actions and mitigate challenges with non-compliance. Also, the findings revealed that social strategies are needed in the form of staff training and industry collaboration on data security measures to provide guidance and also raise security threats awareness as well as inform best practices to secure organisational data. Data at rest and in transit within the organisation on local area network are also prone to security attacks. Based on the limitations of this study, future studies should focus on banks in Accra and outside Accra to enrich the theoretical generalisation of the findings. Also, mixed methods approach should be used to further enrich the framework application to all sectors of the economy .

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Bittencourt LF, Goldman A, Madeira ER, Da Fonseca NL, Sakellariou R. Scheduling in distributed systems: A cloud computing perspective. Computer Science Review. 2018;30:31-54.
2. Mohamed KS. IOT cloud computing, storage, and data analytics. In The Era of Internet of Things Springer, Cham. 2019; 71-91.
3. Catteddu D, Hogben G. Cloud computing risk assessment. European Network and Information Security Agency (ENISA). 2009;583-592.
4. Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A. Cloud computing—The business perspective. Decision Support Systems. 2011;51(1):176-189.
5. Zerfos P, Yeo H, Paulovicks BD, Sheinin V. SDFS: Secure distributed file system for data-at-rest security for Hadoop-as-a-service. In 2015 IEEE International Conference on Big Data (Big Data). IEEE. 2015;1262-1271.
6. Kaushik S, Gandhi C. Cloud data security with hybrid symmetric encryption. In 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). IEEE. 2016;636-640.
7. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. 2012; 28(3):583-592.
8. Liu S, Kuhn R. Data loss prevention. IT Professional. 2010;10–13. Available:https://doi.org/10.1109/MITP.2010.52
9. Spooner D, Silowash G, Costa D, Albrethsen M. Navigating the insider threat tool landscape: Low cost technical solutions to jump start an insider threat program. In 2018 IEEE Security and Privacy Workshops (SPW). IEEE. 2018; 247-257.
10. Javornik M, Nadoh N, Lange D. Data is the new oil. In Towards User-Centric Transport in Europe . Springer, Cham. 2019;295-308.
11. Chauhan A, Gupta J. A novel technique of cloud security based on hybrid encryption by Blowfish and MD5. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE. 2017;349-355.
12. Krishnan K. Data warehousing in the age of big data. Newnes; 2013.
13. Zeng X, Garg SK, Strazdins P, Jayaraman PP, Georgakopoulos D, Ranjan R. IOTSim: A simulator for analysing IoT applications. Journal of Systems Architecture. 2017;72:93-107.
14. Cárdenas AA, Manadhata PK, Rajan SP. Big data analytics for security. IEEE Security and Privacy. 2013;11(6):74-76.
15. Singh A, Malhotra M. Hybrid two-tier framework for improved security in cloud environment. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). IEEE. 2016;955-960.

16. Lagarde C. Estimating Cyber Risk for the Financial Sector. IMF Blog; 2018. Available:https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/
17. Stewart H, Jürjens J. Data security and consumer trust in Fin Tech innovation in Germany. Information and Computer Security. 2018;26(1):109-128.
18. Hughes C. The Three States of Digital Data - Advanced Software Products Group; 2014a. Available:http://aspg.com/three-states-digital-data/#.XHXoFriny00
19. Jouini M, Rabai LBA, Aissa A. Ben. Classification of security threats in information systems. Procedia Computer Science. 2014;32:489–496. Available:https://doi.org/10.1016/j.procs.2014.05.452
20. Janacek B. Best Practices: Securing Data at Rest, in Use, and in Motion – Data Motion Data Motion; 2015. Available:https://www.datamotion.com/2015/12/best-practices-securing-data-at-rest-in-use-and-in-motion/
21. Horne CA, Ahmad A, Maynard SB. Australasian conference on information systems information security strategy in organisations: Review, Discussion and Future Research Directions; 2015.
22. D’Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse A deterrence approach. Information Systems Research. 2009; 20(1):79–98. Available:https://doi.org/10.1287/isre.1070.0160
23. Atif Ahmad, Sean B, Maynard, Sangseo Park. Information security strategies: Towards an organizational multi-strategy perspective | 10.1007/s10845-012-0683-0. Springer. 2012;1–23. Available:https://sci-hub.tw/10.1007/s10845-012-0683-0
24. Liu S, Sullivan J, Ormaner J. A practical approach to enterprise IT security. IT Professional. 2001;3(5):35–42. Available:https://doi.org/10.1109/6294.952979
25. Bertino E, Sandhu R. Database Security — Concepts, Approaches, and Challenges. 2005;2(1):2–19.
26. Cooper M. Encryption – Information Security - Cardiff University; 2012. Available:http://sites.cardiff.ac.uk/isf/advice/encryption/
27. Comodo. What is a Firewall? Explaining How a Firewall Works; 2017. Available:https://personalfirewall.comodo.com/what-is-firewall.html
28. Herrmann M. Security strategy: From soup to nuts. Information Security Journal. 2009; 18(1):26–32. Available:https://doi.org/10.1080/19393550802656115
29. Kumar RL, Park S, Subramaniam C. Understanding the value of countermeasure portfolios in information systems security. Journal of Management Information Systems. 2008;25. Available:https://doi.org/10.2753/MIS0742-1222250210
30. Debar H, Dacier M, Wespi A. Towards a taxonomy of intrusion-detection systems. Computer Networks. 1999;31(8):805–822. Available:https://doi.org/10.1016/S1389-1286(98)00017-6
31. Armstrong D, Carter S, Frazier G, Frazier T. Autonomic defence: Thwarting automated attacks via real-time feedback control. Complexity. 2003;9(2):41–48. Available:https://doi.org/10.1002/cplx.20011
32. Abukari AM, Gupta V, Madavarapu JB, Manda VK. A homomorphic block approach to block chain and cloud ERP Implementation. Journal of Applied Intelligent Systems and Information Sciences. 2023;4(1):50-59. DOI: 10.22034/jaisis.2023.412311.1066

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/116979