Addis Ababa University

College of Natural Sciences

Cloud Data Security Framework for Payment Card System: the case of Ethiopia

Edil Endalew

A Thesis Submitted to the Department of Computer Science in Partial Fulfillment for the Degree of Master of Science in Computer Science

Addis Ababa, Ethiopia

July, 2016

Addis Ababa University

College of Natural Sciences

Cloud Data Security Framework for Payment Card System: the case of Ethiopia

Edil Endalew

Advisor: Mesfin Kifle (PhD)

This is to certify that the thesis prepared by Edil Endalew, titled: *Cloud Data Security Framework for Payment Card System: the case of Ethiopia* and submitted in partial fulfillment of the requirements for the Degree of Master of Science in Computer Science complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the Examining Committee:

	Name	Signature	Date
Advisor:	Mesfin Kifle (PhD)	_____	
Examiner:	Mulugeta Libsie (PhD)	_____	
Examiner:	Solomon Atenafu (PhD)	_____	

Acknowledgment

First and foremost I am grateful to God, who kindly helped me to complete my thesis. Without his blessings I wouldn't have been writing a single word.

Then I would like to express my special appreciation and thanks to my advisor, Dr. Mesfin Kifle for the continuous support of my research, for his patience, motivation, enthusiasm, and immense knowledge. I am grateful to the department of computer science that allowed me to proceed unfailingly on my thesis. I would like to thank the staff of Premier Switch Solution (PSS) S.C., and IT professionals at Nib International Bank, Awash International Bank and Enat International Bank for the invaluable assistance they have provided me during the process of information gathering and analysis. My research would not have been possible without their help.

A special thanks to my family. Words can‟t express how grateful I am to my mother and my father for all of the sacrifices that you have made on my behalf. Your prayer for me was what sustained me thus far. I would also like to thank my fiancé and all of my friends. They were always supporting me and encouraging me with their best wishes towards my goal, without whose love, encouragement, and prayer I would not have finished this thesis.

Abstract

A cloud computing is an emerging model for the provisioning of dynamically elastic and often virtualized resources at the levels of infrastructures, platforms and software. It is becoming a possible choice for the banking industry to benefit out of its advantages. Banks are attempting to shift their services to the cloud even though there are business risks related to data security. Data security is the science and study of methods of protecting data in computer and communication systems.

Within the banking modules, this thesis concerns on the payment card system data security since fraud on payment card system is becoming a serious issue for the banking industry and cause an economical crisis. Currently, Ethiopian banks‟ practice with the involvement of third party shows that there is an unsecured way of data transmission between payment applications and an access control issue that leads to internal and external frauds.

The objective of this thesis is to design a cloud data security framework for payment card system of Ethiopia in order to contribute data security solutions to the existing payment card system and in the cloud environment. Interview, questionnaire, observation, literature review, designing and simulation are used to carry out the research process.

The proposed framework is about communication between applications throughout the payment card system with the integrated security component. The security component contains the proposed combined algorithm (AES, RSA and SHA2) that ensure data confidentiality and integrity at the time of data transfer into the cloud and selected access control technique is also applied to the databases and library files.

Cryptool2 and CloudSim simulation tools are used to implement the proposed cloud data security components. Cryptool2 is used to generate the combined encryption algorithm and CloudSim simulates the cloud environment for the payment card system and come up with a cloud data security framework for a payment card system. Measuring encryption algorithm performance with various parameters and testing with security threat are some of the recommendations for future work.

Keywords: Cloud Computing, Data Security, Payment Card System, Payment Card System Data Security, Security Component, Data Confidentiality and Integrity on Cloud Computing

Table of Contents

List of Figures

List of Tables

List of Algorithms

Acronyms and Abbreviations

3DES	*Triple Data Encryption Standard*
ABAC	Attribute-Based Access Control
AES	*Advanced Encryption Standard*
ATM	*Automated Teller Machine*
BI	*Business Intelligence*
BPO	*Business Process Outsourcing*
BIAN	*Banking Industry Architecture Network*
CIA	*Confidentiality, Integrity and Availability*
CISP	*Card holder Information Security Program*
CloudSim	Cloud Simulator
CoRBAC	Context-Oriented Role Based Access Control
CPS	*Card Payment Schema*
Crypto Tool2	*Cryptography Tool*
CSA	*Cloud Security Alliance*
CSP	*Cryptographic Service Provider*
DaaS	*Data as a Service*
DAC	Discretionary Access Control
DCsim	Data Centre Simulation Tool
DES	*Digital Signature Algorithm*
DRP	*Disaster Recovery Plan*
dRBAC	Distributed Role-Based Access Control
DSL	*Digital Subscriber Line*

EAF	*Enterprise Architecture Framework*
EMP	*Electromagnetic Pulse*
FIPS	*Federal Information Processing Standard*
Groundsim	Ground Simulation Tool
IaaS	*Infrastructure as a Service*
IBD	*International Banking Division*
IDRBT	*Indian Reference Architecture Banking Technology*
NIST	*National Institute of Standards and Technology*
NIST RA	*National Institute of Standards and Technology Reference Architecture*
MAC	Mandatory Access Control
MD5	Message-Digest Algorithm
MIRA-B	*Microsoft Industry Reference Architecture for Banking*
MR-CloudSim	MapReduce Cloud Simulation Tool
PaaS	*Platform as a Service*
PCI	*Payment Card System Industry*
PCI DSS	*Payment Card System Industry Data Security Standard*
PCI SSC	*Payment Card System Industry Security Standards Council*
PKI	*Public Key Infrastructure*
PSS	Premier Switch Solution
RAID	*Redundant Array of Independent Disks*
RC2	*Ron's Code 2*
RC6	*Rivest Cipher 6*

RSA	*Rivest-Shamir-Adleman*
SaaS	*Software as a Service*
SABSA	*Sherwood Applied Business Security Architecture Framework*
SBP	*Service-Based Business Processes*
SET	*Secure Electronic Transaction*
SHA-2	*Secure Hashing Algorithm 2*
SMD	*Smart Mobile Device*
Smartsim	Smart Cloud Simulator
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TOGAF	*The Open Group Architecture Framework*
UML	*Unified Modeling Language*
VPN	*Virtual Private Network*
ZKM	*Zelix Klass Master*

Chapter One: Introduction

1.1 Background

Data security is the science and study of methods of protecting data in computer and communication systems [1]. Protecting data means such as a database from destructive forces and from the unwanted actions of unauthorized users where protecting a data is defined by a combination of confidentiality, integrity, authenticity and availability (CIA) factors, in accordance with business needs and any legal, contractual, or regulatory requirements and constraints [2, 3].

Data protection often thought of as information asset management spans the entire data life cycle, from creation, use, transfer and store to eventual deletion. At every stage, certain controls must be applied to protect data from unauthorized access and use [3].

In financial institution like banks, data is the lifeblood of their existence. Data include customer financial information, account information, payment card information, transactions and non-public customer personal information. Almost all the information uses by a financial institution are potentially sensitive or private where their data security should be the first concerns.

The nature and techniques of data security should consider the underlying computing platform. In cloud computing, which is the emerging technology and Internet-based computing; large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources [4, 5]. Cloud computing relies on the sharing of resources to achieve cost reduction, greater flexibility and optimal resource utilization [4, 5].

Cloud computing has services like Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Data as a Service (DaaS) implemented through four different deployment modes [17, 52]. These are public, private, hybrid and community cloud that differ on the security level, performance and effectiveness of the cloud technology. Moreover, in all modes, cloud computing provides a lot of benefits like testing and development, big data analysis, files storage, backup and disaster recovery with low cost

through the cloud computing providers such as Amazon, Google, Microsoft, IBM and Sales Force [6]. However, there are also common challenges of cloud computing like security and privacy, interoperability and portability, reliability and availability, performance and bandwidth cost are some of the known lists [7].

Security is one of the main challenges in the data life cycle. The nature of security touches all corners on overall cloud framework such as physical and logical level security, IT infrastructure security, application and process security and data and information security. The main worry is about data and information security [3].

Despite all, companies around the world are increasingly aware of the business value or benefit that cloud computing brings and taking steps towards transition to the cloud. A smooth transition entails a thorough understanding of the benefits as well as the challenges involved.

Financial institutions like banks are potential areas of interest in this regard. The typical banking operations are retail, loan, international banking and e-banking operations. E-Banking operations are banking operations performed electronically, including payment card system, Internet banking and mobile banking [8].

Banks around the world are progressively adopting cloud computing. In 2014, Dutch bank in the Netherlands has managed over €8 billion in assets recently moved its entire retail banking platform to the cloud. The sixth largest bank in Spain, Bankinter uses the Amazon cloud, Suncorp Bank in Australia placed an emphasis on innovation and launched a working virtual private cloud and Zitouna Bank of Tunisia has selected IBM‟s cloud capabilities to host its Temenos banking platform [8].

The number of private and corporate financial transactions that are done electronically is growing rapidly. The payment card system is one of them. In the recent trend its share is growing since, from a user's perspective, efficiency and flexibility are becoming clear advantages of existing and emerging electronic payment systems [10].

According to the information gathered from the interview in June, 2015, among 19 banks in Ethiopia, half of them are providing payment card system services to their customers. Out of

those six of them outsourced the payment card system operation to a third party called Premier Switch Solution (PSS) which is working as a payment card system service provider. There are also banks on testing stage where the payment process is handled by the third party.

Based on the questionnaire replies, the PSS payment card system flows from terminal, to PSS server and then to the bank and a message is returned back to the terminal on a similar path. An encrypted data with Zelix KlassMaster (ZKM) scripting language is transferred from the Automated Teller Machine (ATM) terminal to the PSS servers and plain text goes to the core banking system which is unsecured way of communication. There are also library files which need an access control method on the core banking side.

Regarding cloud computing practice of Ethiopian banks, there is a swift operation using the service. But on Core banking, ATM, Internet banking and mobile banking operations, the banks are hesitating to move to the cloud. Among the reasons, the question of data security on the cloud takes its part. Thus, the research focuses on data security of payment card system.

1.2 Motivation

In September 2014, there was an event by North West based IT Support, IT Services & IT Solutions Company in Addis Ababa for Ethiopian banks on cloud computing area to motivate the banks to move their data centers to the cloud. But the banks have questioned on the data security of their confidential data. That was the biggest security issue raised by the bankers‟ side. On the other hand the experiences of some of Ethiopian banks on the payment card are controlled under the third party. Thus, these scenarios motivated us to work and contribute on the cloud data security issue, especially for the payment card system module.

1.3 Problem Statement

Industries, companies and financial institutions are outsourcing their private and confidential data over the cloud and add the benefit of cloud computing [9]. However, cloud computing suffers from various security issues as data owners store their data on external servers, there

have been increasing demands and concerns for data confidentiality, integrity, authentication, availability and access control [9].

Banks demand to have a secure way of storing and transacting data. When it comes to payment card system the security level should be more critical since the nature of payment card system transactions is sensitive to fraudulent.

Around the world due to payment card system frauds, countries are losing millions of dollars. For instance, the U.S. accounted for 51% of global payment card system fraud costs in 2013, according to BI Intelligence estimates [10].

In case of Ethiopia there are a few researches on the area, [11, 13]. But they are not directly related to the payment card system module and their data security aspect.

Based on the interview and questionnaire conducted, the trend of Ethiopian banks of payment card system shows that six banks are providing card payment service for their customers under a control of third party with their existing security issues such as an access control method on library file, an unencrypted way of communication between the payment card and core banking system.

In recent years there are a few reference architectures used in mapping banking industry in the cloud such as Microsoft Industry Reference Architecture for Banking (MIRA-B), ORACLE Retail Banking Reference Architecture, IBM Banking Industry Framework and HP‟s Banking Reference Architecture which is based on their own company standard and regulations in favour of their product [13,14,15,16].

National Institute of Standards and Technology Cloud Computing Security Reference Architecture (NIST RA) is the recent work on cloud security and there are a few related works on the area [3, 17].

Thus, in this research, data security framework for the payment card system is developed to address the existing payment card system security issue in combination with existing security reference architecture and framework on a cloud.

Accordingly, the research attempts to answer the following research questions:

- What are the data security techniques that can be implemented to secure payment card system data and the payment process in a cloud environment?
- How to develop cloud data security framework for the payment card system?

1.4 Objectives

General Objective

The general objective of the thesis is to design a cloud data security framework for payment card system, for Ethiopia.

Specific Objectives

To achieve the general objective of the thesis, the following specific objectives are identified.

- Understand the existing system practice on the security mechanism, measures and analysis gaps on payment card system architecture.
- Review related work on cloud data security for payment card system.
- Design cloud data security framework.
- Test the security component in the proposed framework using simulation tools.

1.5 Methods

In order to achieve the general and specific objectives mentioned above, we use the following methods.

- Data collection and analysis: - will be conducted through interviews, questionnaire and observation on the payment card system security techniques and measures throughout the business processes and analysis on case based analysis technique to understand the existing scenario.
- Literature review: - cloud reference architecture for banking industry, data security frameworks, cloud data security solution and related work will be reviewed to have knowledge of the components of the cloud data security framework.
- Designing a data security framework: - visual paradigm will be used to design the data security framework.

- Testing data security framework component: - Cryptool 2.0 and CloudSim 2.1.1 will be used. Cryptool 2.0 is a tool for analyzing, learning and implementing algorithms with usual and practical manner. These tools enable us to create analysis and implement the combined encryption algorithms [38]. CloudSim-2.1.1 integrates as a library file in Eclipse, which is an extensible simulation toolkit that enables modeling and simulation of a cloud computing environment [18].

1.6 Scope and Limitations

This thesis aimed to develop a cloud data security framework for the payment card system. It particularly focuses on data on transmission between the applications related to payment card system specifically on debit card in a cloud computing environment. It doesn‟t include loan, retail, international banking, mobile and Internet banking services and the different related security issues like card cloning and identity thefts. It focuses on securing the data on transmission and stored data confidentiality, integrity, and availability of payment card system in a cloud computing environment.

1.7 Application of Results

The result of this research will contribute to the ongoing researches in this domain area. It will be an input for different stakeholders, researchers and students. Likewise, it provides its own contribution to the beneficiaries like banks, cloud providers on the acceptance of cloud computing services.

1.8 Organization of the Rest of the Thesis

The rest of the thesis is organized as follows. Chapter Two explains the issue on data security, payment card system, cloud computing, banking reference architectures on cloud and cloud simulation tools from a range of literatures. Chapter Three reviews related works that have been conducted on data security framework on the cloud. Chapter Four will be all about the empirical findings on the existing payment card system and the proposed solution. Chapter Five will present simulation results. Finally, Chapter Six will contain the conclusion, recommendation and future work.

Chapter Two: Literature Review

2.1 Overview

The objective of this Chapter is to give a description of the research area on data security, payment card system, cloud computing with its security concerns, cloud data security solutions, different security reference architectures for banking industries, simulation tools of cloud computing environment and cryptography. Data security is one of the main challenges on cloud computing that results in limitation of confidentiality, integrity and availability of the data in cloud services. Details on data security aspects, cloud service delivery models, cloud deployment models, aspects considered on cloud data security and existing works on cloud security reference architecture are presented in a way to explore the research area and to understand the need and the importance of such a study.

2.2 Data Security Aspects

The term data security means protecting data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity and availability for the users [21].

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for data/information security within an organization. The elements of the triad are considered the three components of security. Let‟s look at them separately.

Confidentiality ensures that data is not disclosed to an unauthorized person. Confidentiality loss occurs when data can be viewed or read by any individual who is unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers are not encrypting their communications [22].

A good example of methods used to ensure confidentiality for a data like account number when banking online is encryption. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor

authentication is becoming the norm. Other options include biometric verification and security tokens [31].

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle [31]. Integrity makes sure that data held in a system are a proper representation of the data intended and it has not been modified by an unauthorized person [22]. Some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crashes. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state [31].

Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems [22]. Redundancy, failover, *Redundant* Array of Independent Disks (RAID) even high-availability clusters can mitigate availability problems. Fast and adaptive disaster recovery is essential for the worst case scenarios [31].

2.3 Payment Card System

One of the electronic transactions is a payment card transaction. An application that performs the operation is referred to an electronic payment card system [23].

The underlying model of a payment card system consists of three parties: a bank, a customer, and a shop. There are three different types of transactions within the system: withdrawal involving the bank and the customer, payment involving the customer and the shop, and deposit involving the shop and the bank. The customer's account is debited during withdrawal, and the shop is credited during deposit. The three transactions take place simultaneously or separately, depending on the payment system [23].

Payment Card System Industry Data Security Standard (PCI DSS) is the global data security standard adopted by the payment card brands for all entities that process, store or transmit card holder data [24]. It consists of common sense steps that mirror security best practices.

There are security controls for using payment card systems when dealing with payment (credit/debit) cards. Some of the controls mentioned from PCI Data security standard are applicable at the network level, but can be incorporated in the application too.

The oversight framework for card payment schemes-standards: - is the majority of European Union central banks already have an ad hoc oversight policy for Card Payment Schema (CPSs). Almost all central banks directly oversee CPSs as far as security issues are concerned, with the objective of maintaining public assurance in means of payment and thus ultimately in money. The framework can be applied to all card payment schemes, including three-party CPSs providing card payment services either by debit and/or credit card [29].

The oversight standards for euro retail payment systems are a logical model for the standards, but they have been adapted to the specificities of CPSs, especially with regard to security and operational issues. The Oversight framework for card payment schemes-standards are shown in Figure 2.1 [29].

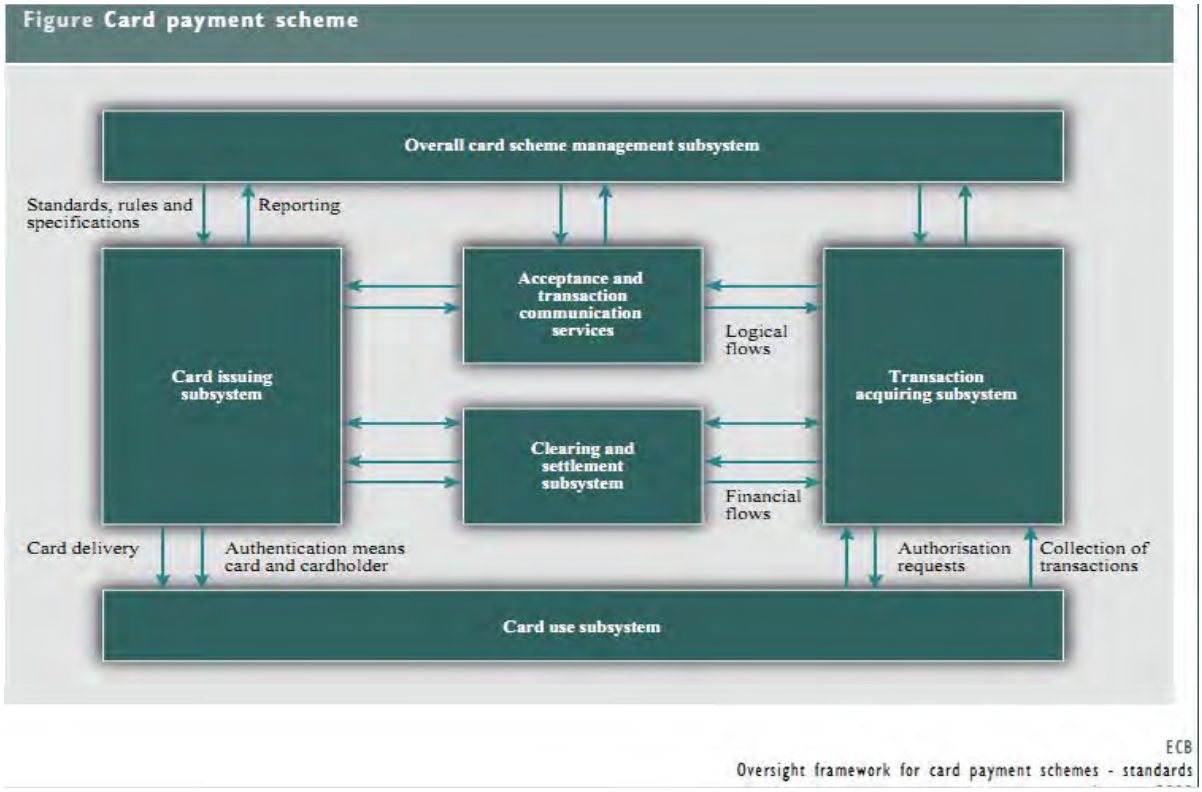


Figure 2.1: Oversight Frameworks for Card Payment Schemes- Standards

There are different industrial standards and practices of payment card. Some of them are as follows:-

- Card holder Information Security Program (CISP):- instituted by Visa USA, the program‟s objective is to protect card holder data by enforcing a high information security standard [25].
- Payment Card System Industry Data Security Standard (PCI DSS):- this standard mandates the requirements as set by MasterCard International and Visa which focuses on both network and application security. For application security the standard mandates development based on secure coding guidelines such as the Open Web Application Security Project guidelines [24].
- Electronic Commerce Security Architecture Best Practices – MasterCard: - presents architecture, methodologies, and best practices for establishing a secure electronic transaction through a card [25].

Among these, PCI Data Security Standard is a common practice in payment card system data security. The PCI Data Security Standard specifies 12 requirements for compliance to protect payment card system transactions, organized into six logically related groups called "control objectives". Each version of PCI DSS has divided these 12 requirements into a number of sub-requirements differently, but the 12 high level requirements have not changed since the inception of the standard.

The most related issues are protecting card holders‟ data and implement strong access control measures. Protect stored card holder data prevent their unauthorized use – whether the data is stored locally, or transmitted over a public network to a remote server or service provider. Access control allows merchants to permit or deny the use of physical or technical means to access *Permanent Account Number* (PAN) and card holder data. Access must be granted on a business need to know basis. Physical access control entails the use of locks or restricted access to paper-based card holder records or system hardware. Logical access control permits or denies the use of *Personal Identification Number* (PIN) entry devices, a wireless network, PCs and devices.

2.4 Cloud Computing

Cloud computing is an emerging delivery model for IT services based on Internet protocols. It typically involves provisioning of dynamically scalable and often virtualized resources at the infrastructure, platform and software levels. Cloud environments are being increasingly used for deploying and executing business processes, particularly service-based business processes (SBPs) that are made up of components that provide business services [26].

2.4.1 Service Delivery Models

As per National Institute for Standards and Technology (NIST), there are three basic types of cloud service models. These models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [17].

Software as a service (SaaS):- application is accessed over the Internet example, Google; Zoho provides a word processor, spreadsheet, presentation and web applications. SaaS applications can be free or paid via subscription. These applications are accessible from any computer connected to the Internet either through thin client interfaces like web browsers or program interfaces [27].

The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it"s running [21].

Platform as a service (PaaS):- the platform is typically an application framework. It provides tools and environment to the users for creating cloud applications. For example, product called App Engine which allows anyone to run applications on Google"s infrastructure [27].

The consumer uses a hosting environment for its applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running [21].

Infrastructure as a service (IaaS):- infrastructure allows running any existing application on the cloud. The consumer uses computing resources such as processing power, storage, networking components or middleware. They can control the operating system, storage,

deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them [21].

Data as a service, or DaaS, is a cousin of software as a service. Like all members of the "as a Service" (aaS) family, DaaS is based on the concept that the product, data in this case, can be provided on demand to the user, regardless of geographic or organizational separation of provider and consumer [52].

In this research software as a service is used since payment card system is software service provided through the cloud computing platform.

2.4.2 Deployment Models

There are four basic cloud deployment models, as outlined by National Institute of Standards and Technology (NIST), based on who provides the cloud services [17].

These deployment models are: Public cloud, Private cloud, Hybrid cloud and Community cloud.

Public Cloud: - public cloud service is open to use for the general public. The service provider makes resources available to the users over the Internet. Services provided by this type of cloud may be free or paid depending on the type of the service they deliver [27]. A public cloud does not mean that a user‟s data is publicly visible; public cloud vendors typically provide an access control mechanism for their users [21].

Private Cloud: - private cloud is owned by a single company comprising multiple consumers, and it may exist on or off premises [27]. A private cloud offers many of the benefits of a public cloud, such as being elastic and service based. The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and selected [21].

Community Cloud: - a community cloud is controlled by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them and the members of the community share access to the data and applications in the cloud [21, 27].

Hybrid Cloud: - a hybrid is a combination of a public and private cloud. In this model users typically outsource non-business-critical information and processing in the public cloud, while keeping business-critical services and data in their control [21]. The major benefit of using private cloud is flexibility and security. On the other hand public cloud offers scalability and accessibility. Both of them have unique benefits, but they also have trade-offs. Hybrid cloud merges the advantages of public and private cloud [27].

For this research, since it is about banking data, hybrid cloud is more convenient to implement and applicable in the case of Ethiopia. Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [14]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid cloud provides more secure control of the data and applications and allows various parties to access information over the Internet [32].

2.4.3 Essential Characteristics of the Cloud

The NIST definition describes five essential characteristics of cloud computing [21].

- Rapid Elasticity: - elasticity is defined as the ability to scale resources, both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing power as they need.
- Measured Service: - it is a measured service; aspects of the cloud service are controlled and monitored by the cloud provider. This is crucial for billing, access control, resource optimization and capacity planning.

- On-Demand Self-Service: - the on-demand and self-service aspects of cloud computing mean that a consumer can use cloud services as needed without any human interaction with the cloud provider.
- Ubiquitous Network Access: - means that the cloud provider"s capabilities are available over the network and can be accessed through standard mechanisms by both thick and thin clients.
- Resource Pooling: - allows a cloud provider to serve its consumers via a multi-tenant model (an architecture in which a single instance of a software application serves multiple customers). Physical and virtual resources are assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).

2.4.4 Data Security Issues

Data security is the number one issue when it comes to cloud computing. Since a third party stores the sensitive and confidential business data, it never known what is going on with the data. Along with the benefits of Business Process Outsourcing (BPO) comes an increased risk of data, unless the organization can protect its data [28, 32].

Data security has played an important role in hindering cloud computing acceptance. According to different research results, the importance of security in cloud out of the other aspects takes the higher part as shown in Figure 2.2 [22].

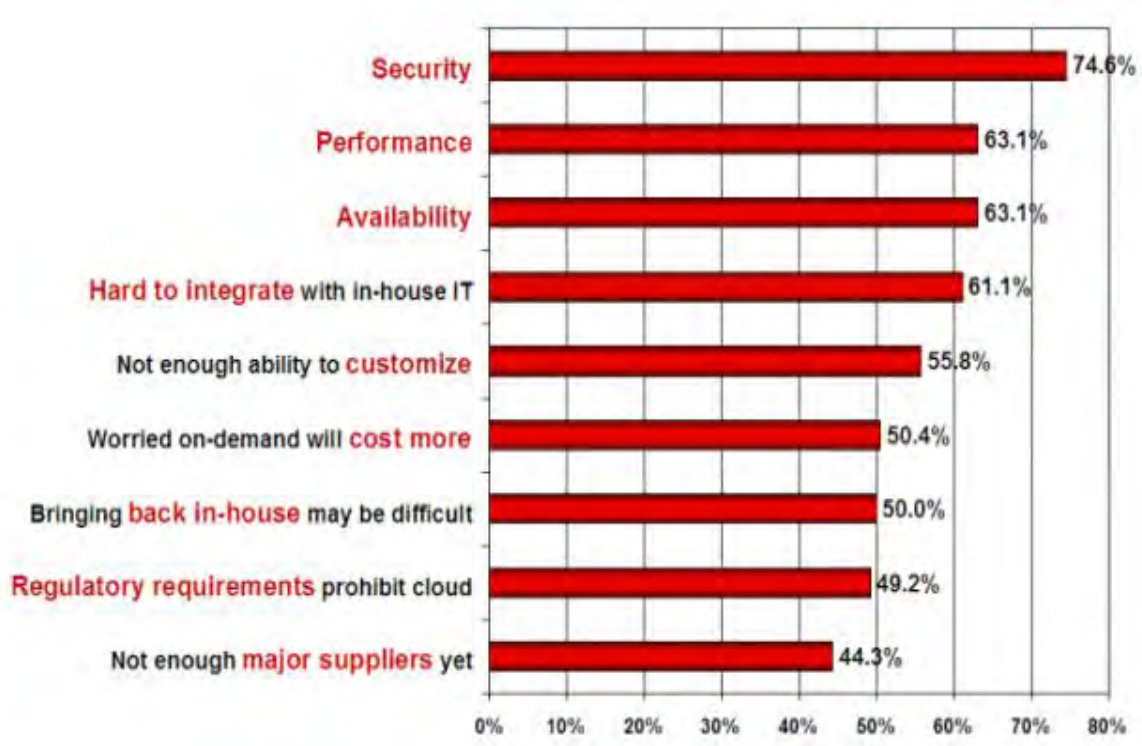


Figure 2.2: Importance of Security in Cloud Computing

Despite the beauty of cloud computing application service, cloud computing is fraught with security risks and basic security issues are brought to the attention of potential cloud service subscribers such as authentication, auditing, confidentiality, integrity, availability and non-repudiation [21].

- Authentication: is a process by which one entity verifies the identity of another entity. This can be a person or program. The authentication process can be done in three ways; something that the user knows such as password or login name, something the user has, such as a PIN and something the user is such as finger print. Another authentication process can be machine-to-machine, which can be client, server and/or mutual authentications. Client authentication involves the server verifying the client‟s identity, server authentication involves the client verifying the server‟s identity and mutual authentication involves the client and server verifying each other‟s identity.

- Auditing: is a process of collecting information about user attempting access to a particular resource, or performs actions. The log in system must be able to record all actions performed on that resource. In case there is any problem, the log file can be checked to trace such a user out.
- Non-repudiation: is the ability to limit parties from refuting that a legitimate transaction took place. Since cloud computing transactions involve money, it is important that the customer commits himself by endorsing his/her signature.

The other issues like confidentiality, integrity and availability are common ones that are referred by data security, which pose major issues for cloud vendors.

There are a number of algorithms and methods implemented on the cloud in order to improve the data security. These are as follows:-

2.4.4.1 AES Algorithm

Advanced Encryption Standard (AES) algorithm is an encryption algorithm to maintain data confidentiality. Both hardware and software implementations are faster still. It is the new encryption standard recommended by NIST to replace *Digital Signature Algorithm* (DES) [35].

According to [36], AES is more secure and efficient compared to DES and *3DES*. Research results in comparison between AES, DES and 3DES as shown in the Table 2.1 [53].

Table 2.1: Comparison between AES, DES and 3DES

Factors	**AES**	**3DES**	**DES**
Key Length	128,192,or 256 bits	(k1,k2 and k3) 168 bits (k1 and k2 is same) 112 bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher

Factors	**AES**	**3DES**	**DES**
Block Size	128,192,or 256 bits	64 bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attack	Vulnerable to differential, Brute Force attacker could be analyzed a plain text using differential cryptanalysis.	Vulnerable to differential and cryptanalysis; weak substitution tables
Security	Considered secured	One only weak which is Exit in DES	Proven inadequate
Possible key	2^{128}, 2^{192} or 2^{256}	2^{112} or 2^{168}	2^{56}
Time required to check all possible at 50 billion keys per second	For a 128-bit key: $5*10^{21}$ years	For a 112-bit key: 800 days	For a 56-bit key: 400 days

Other research result why AES is preferable over the others is stated as follows:

Why AES?

- AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms.
- Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
- This algorithm has speedy key setup time and good key agility.
- It requires less memory for implementation, making it suitable for restricted-space environments.
- The structure has good potential for benefiting from instruction-level parallelism.

- There are no serious weak keys in the AES.
- It supports any blocks size and key sizes that are multiples of 32(greater than 128-bits).
- Statistical analysis of the cipher text has not been possible even after using a huge number of test cases.
- No differential and linear cryptanalysis attacks have been yet proved on AES [43].

A performance comparison among AES, DES and triple DES for different microcontrollers shows that AES has a computational cost of the same order as required for triple DES. Another performance evaluation reveals that AES has an advantage over algorithms *Triple Data Encryption Standard* (3DES), DES and *Ron's Code 2 (*RC2) in terms of execution time with different packet size and throughput for encryption as well as decryption [42]. Also in the case of changing data type such as image instead of text, it has been found that AES has an advantage over RC2, *Rivest Cipher 6 (*RC6) and blowfish in terms of time consumption [43].

2.4.4.2 RSA + SHA (digital signature)

RSA is a public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm [39]. The RSA algorithm is based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in the RSA are based on very large prime numbers [39]. Thus the security of this algorithm is based on its difficulty to factorize the large integers and it can be used for both public key encryption as well as digital signatures [39].

The *Secure Hashing Algorithm* (SHA) is a cryptographic hash function and used in digital certificates as well as in data integrity. SHA is a fingerprint that specifics the data and was developed by NIST as a US Federal information processing standard (FIPS), intended for use with digital signature applications [40].

Data sent to the cloud and stored on the storage server might face data integrity violations. Data integrity ensures through performing digital signature. The digital signature is obtained through a combination of encryption algorithm and hashing algorithm such as RSA + SHA2 [33], since SHA-2 has the least computational cost among the similar algorithms. The NSA designed SHA-2 to overcome theoretical breaks in SHA1. The new design improved security by increasing collision resistance. An attacker requires more time to find any two messages m1 and m2 that hash to that same value „h". Thus, in terms of collision resistance, SHA-2 family is more secure than SHA-1. The RSA digital signature scheme also guarantees the authenticity and integrity of data [44].

2.4.4.3 Access Control

Role–based access control (RBAC) model formulates the user"s access to the system based on the activities that the user has been given in the cloud where the role of a user is assigned based on the least privilege concept, i.e., the role with the least amount of permissions or functionalities that is necessary for the job to be done which has been considered as a viable model for cloud computing environment [34]. RBAC allows users to execute multiple roles at the same time and roles are useful approach to organizations such as cloud, grid and peer to peer environment [46].

According to the research results of Analysis of Different Access Control Mechanism in Cloud, the various access control techniques that are popularly used in cloud environment such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), RBAC, Attribute-Based Access Control (ABAC), Distributed Role-Based Access Control (dRBAC) and Context-Oriented Role Based Access Control (coRBAC) analyzed are as shown in the Table 2.2 [46].

Table 2.2: Comparison of Various Access Control Methods

Access Control	DAC	MAC	RBAC	dRBAC	ABAC	coRBAC
User"s Convenience	High	Varies	High	Medium	High	High
performance	Low	Based on security level	High	Depends on subjects	High	Depends on user
Reusability	Multi	Not mentioned	Multi	Multi	Multi	Multi
Role Assignment	Not Mentioned	Single Node assignment	Multi	Multi	Not mentioned	Multi
Single Point Failure	Authorization failure	Less	Less	High	-	-
Node overhead	Less	Less	Less	High	Varies	-
Authentication failure	Less	Depends on distributed environment	Based on job role assigned	High	Less	Less

RBAC can be used to provide service and assigns roles to each user based on the user identity and its role based on the execution environment in the cloud. RBAC permissions are associated with roles and users are assigned to appropriate roles [46]. System administrators only can be able to create roles and granting permissions to those roles. Without RBAC it is difficult to determine what permission has been assigned to which user [46].

Roles are assigned based on the least privilege for the particular object, so this will minimize the damage of information by intruders. Separation of roles will be maintained so there is no chance of misuse of information because each user is assigned to individual roles [46].

2.4.5 Reference Architecture for the Banking Industry

Reference architectures are an important tool that can help financial institutions modularize and align business and technology assets in a predictable way. There are different

architectures proposed and implemented in terms of different organizations worldwide. Microsoft has proposed reference architecture called the Microsoft Industry Reference Architecture for Banking (MIRA-B) that depicts a banking architecture based-on Microsoft‟s technology platform and services. MIRA-B provides a logical architectural point of view for financial institutions to use for planning purposes [13].

ORACLE also has Reference Architecture for Retail Banking in the banking industry. It is applicable to heterogeneous environments and independent of specific products or versions. The architecture covers enterprise interaction, department business system, operational and core business data, infrastructure, enterprise security, enterprise management and enterprise development. Similarly, the IBM banking framework in the cloud describes architecture, dividing to three layer application, platform and infrastructure within compact and less detailed form [5].

HP also presents an architecture called HP‟s Banking Reference Architecture. The HP Banking Reference Architecture consists of four service layers (Channel Services, Business Services, Platforms, and IT Infrastructure).

But almost all the above reference architectures are based on their own company standard and regulations in favour of their product. As far as their architecture concerns, it can be used as a baseline for designing banking related framework.

NIST Cloud Computing Security Reference Architecture is working on cloud security framework focused on a high level conceptual security framework [3, 17] as shown in Figures 2.3 & 2.4.

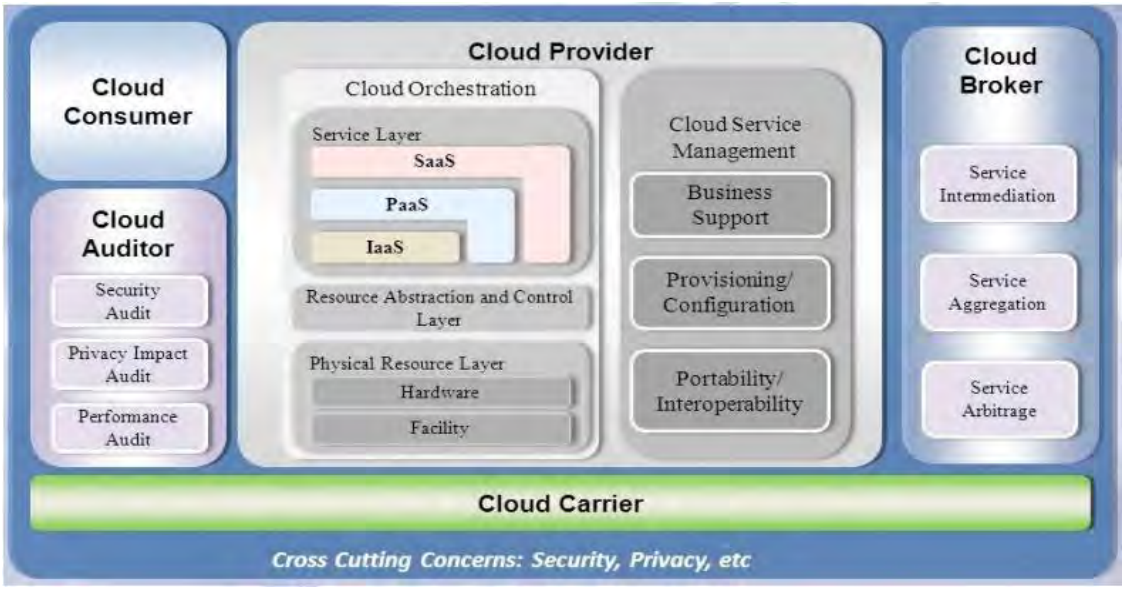


Figure 2.3: NIST Cloud Computing Reference Architecture

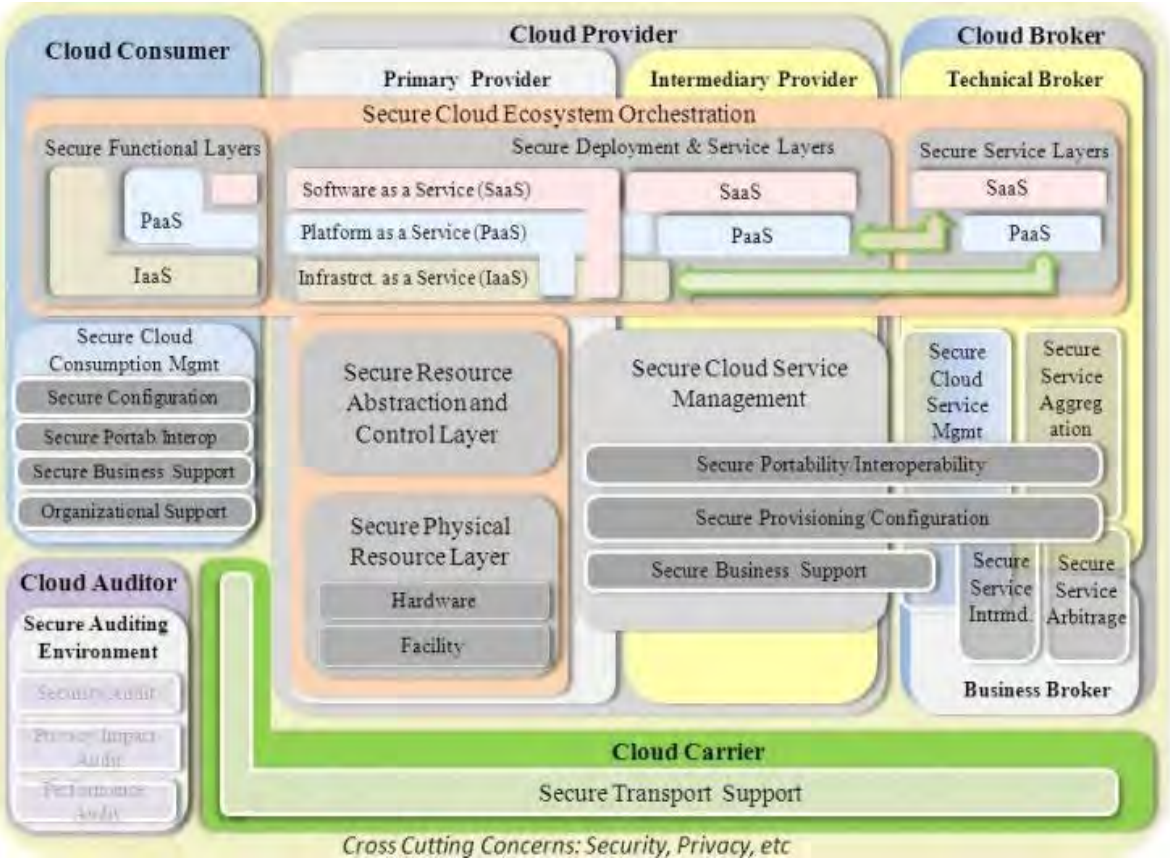


Figure 2.4: NIST Security Reference Architecture Formal Model

2.4.6 Enterprise Security Architecture Framework

There are number of already established Enterprise Security Architectures (EAF) in use today. Some of these frameworks were developed for very specific areas whereas others have broader functionality. Out of those, the Sherwood Applied Business Security Architecture Framework (SABSA) and the Open Group Architecture Framework (TOGAF 9.1) are the frameworks that focus on security.

a. The Sherwood Applied Business Security Architecture Framework

SABSA is a risk-based methodology for delivering security infrastructure solutions that support the firm"s business initiatives to embrace new technological trends and opportunities [41]. SABSA is used successfully by numerous organizations around the world. SABSA is an open-use methodology, not a commercial product. SABSA is a six (Contextual, conceptual, logical, physical, component and services management) by six (asset, motivation, process, people, location, time) matrix layer model for a security architecture that is widely accepted today. This standard is relatively comprehensible in terms of business drivers, but it defines an important framework in terms of security services, logical architecture and security mechanisms, physical architecture and security management, and operational architecture [12].

The SABSA Model follows the work done by Zachman closely, although it has been adapted to security. Each layer represents the view of a different player in the process of specifying, designing, and constructing. The SABSA matrix is outlined in Table 2.3 [42].

Table 2.3: SABSA Matrix

	ASSETS (What)	**MOTIVATION (Why)**	**PROCESS (How)**	**PEOPLE (Who)**	**LOCATION (Where)**	**TIME (When)**
CONTEXTUAL	Business Decisions	Business Risk	Business Process	Business Governance	Business Geography	Business Time Dependence

ARCHITECTURE	**ASSETS** **(What)**	**MOTIVATION** **(Why)**	**PROCESS** **(How)**	**PEOPLE** **(Who)**	**LOCATION** **(Where)**	**TIME** **(When)**
	Taxonomy of Business Assets, ,including Goals& Objectives	Opportunities & Threats inventory	Inventory of Operational Processes	Organizational Structure & the Extended Enterprise	Inventory of Building, Sites, Territories, Jurisdictions, etc	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Role & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objective; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and users; Service Providers & Customers	Security Domain Concepts & Framework	Though-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Polices	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformation; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definition; Inter-domain association & interactions	Start Times, Lifetime & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data inventory	Risk Management Rules & Procedures	Application; Middleware, System; Security Mechanisms	User Interface to ICT System; Access Control System	Host Platforms, Layout & Networks	Timing & Sequencing of Process and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tool & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	ICT Products ,including Data Repositories and Processors	Risk Analysis Tools, Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job description; Roles; Functions; Actions & Access Control Lists	Nodes; Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMEN ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance
	Assurance of Operational Continuity & Excellence	Risk Assessment, Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Application & Services	Account Provisioning; User Support Management	Management of Building, Sites, Platforms & Networks	Management of Calendar And Timetable

b. TOGAF-9 Security Architecture

The Open Group Architecture Framework (TOGAF) is a framework and detailed method and a set of supporting tools for developing enterprise architecture [43]. TOGAF 9 is much different from other architecture frameworks such as Zachman, as it is a lot more process driven and gives a way to essentially codify architectural patterns [43].

TOGAF Security Architecture is a cohesive security design which addresses the requirements and in particular the risks of a particular environment/scenario and specifies what security controls are to be applied where. The design process should be reproducible. This definition is intended to specify only that, architecture is a design, which has a structure and addresses the relationship between the components [43].

The TOGAF 9.1 enterprise architecture framework follows architecture domains differentiated between [44] Business, Data, Application and Technology.

The „data" and „application" architectures are often combined into a single term: Information systems architecture [44]. Data (or information) security architecture focuses on protecting the data. Therefore, these architectures are very single-purpose in nature, in contrary to the extended scope of enterprise security architecture. With the focus on information, common

subjects for data security architecture are encryption and logical access control [44]. Data security diagram for TOGAF is shown in Figure 2.5 [45].

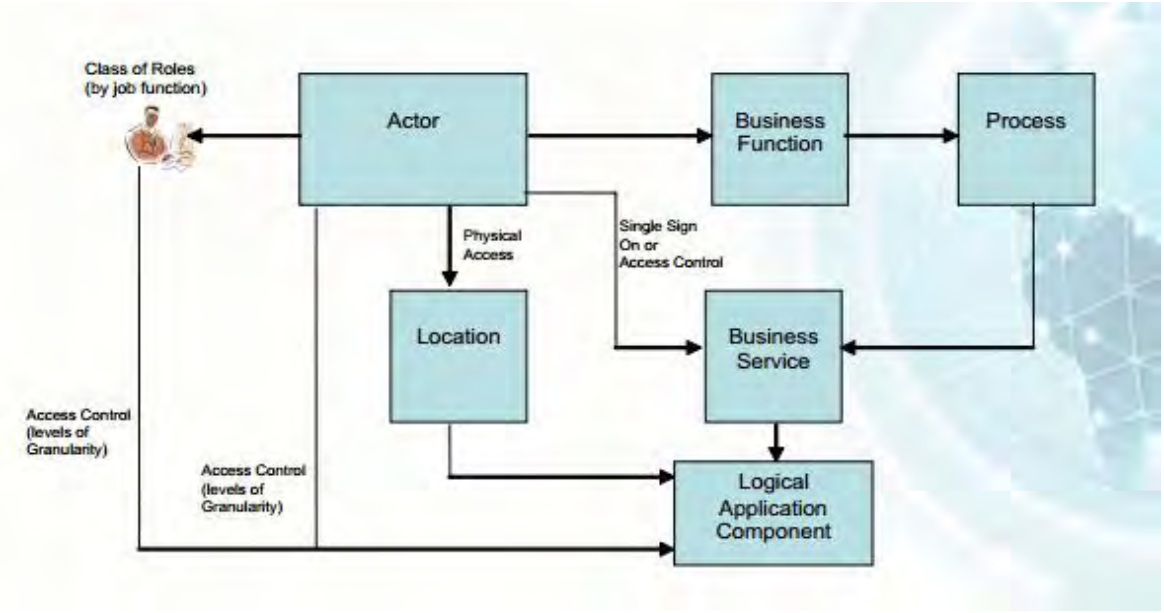


Figure 2.5: Data Security Diagram for TOGAF

Thus, TOGAF9.1 is more related enterprise security architecture to design this research.

2.4.7 Simulation Tools of Cloud Computing and Cryptography

As the adoption and deployment of cloud computing increase, it is critical to evaluate the performance of cloud environments. Modeling and simulation technologies are suitable for evaluating performance and security issues. Cloud simulators are required for cloud system testing to decrease the complexity and separate quality concerns [50]. Several cloud simulators have been specifically developed for performance analysis of cloud computing environments. Some of them are as follows:-

Cloud Simulator (CloudSim): - it is the most popular simulation tool available for cloud computing environment [49]. It is an event driven simulator built upon the core of Grid Simulator [49]. A base programming language for CloudSim is Java, which is one of the famous object oriented programming languages. CloudSim modules are easy to extend as it is based on Java. It is an open source. One unique feature of CloudSim is the federated

policy, which is rarely available in any other simulators [50]. CloudSim contains the following features [49]:

- Support modeling and simulation of large scale computing environment.
- A self contained platform for modeling clouds, service brokers, provisioning and allocation policies.
- Support for simulation of network connections among the simulated system elements.
- Facility for simulation of a federated cloud environment that contains inter-network resources from both private and public domains.
- Availability of a virtualization engine that aids in the creation and management of multiple independent and co-hosted virtual services on a data center node.
- Flexibility to switch between space shared and time shared allocation of processing cores to virtualized services.

CloudAnalyst: - It is a new simulator developed based on CloudSim. CloudAnalyst was basically developed for evaluating the performance of large-scale distributed cloud applications having a high user workload that is geographically distributed over several data centers [50].

Features of CloudAnalyst are the following [49]:

- Easy to use Graphical User Interface (GUI).
- Ability to define a simulation with a high degree of configurability and flexibility.
- Being able to repeat the experiments with slight modifications.
- Generate graphical output in the form of charts and tables.
- Use of consolidated technology and ease of extension.

Smart Cloud Simulator (SmartSim): - It is the only simulator built for mobile cloud computing till to date. It is used for modeling and simulating mobile cloud computing applications in mobile. It uses resource provision, evaluation method for resource utilization in the Smart Mobile Device (SMD) [50].

Ground Simulation Tool (GroudSim): - It is a discrete event simulation tool for cloud and grid computing. It is made specifically for scientific applications in cloud and grid computing. It has Java as an underlying language [51]. It has one unique feature called GroundEntity which has its own error definitions that the user can change at the time of error occurrence [51].

Data Centre Simulation Tool (DCSim): - It is a data center simulation tool for dynamic resource provisioning. It consists of multiple interconnected hosts and each host consists of a scheduler and resource management policy. It simulates data center with a central management system [51]. It also supports Virtual Machine (VM) migration among the hosts and sharing of workload between multiple VMs [49].

MapReduce Cloud Simulation Tool (MR-CloudSim): - It was developed based on CloudSim simulator. The unique feature of MR-CloudSim is its support for simulating MapReduce tasks and thereby supporting BigData processing. CloudSim simulator does not support file processing, cost and time associated with it. In MR-CloudSim, the authors changed some of the core classes in CloudSim to support MapReduce programming model [49].

Based on the information observed on the previous research result, CloudSim is more appropriate for this research.

Cryptool2 is a tool in cryptography for analyzing, learning and implementing algorithms with usual and practical manner. It enables us to create combined encryption algorithms, digital signatures and to analysis and implement the algorithms [38].
Cryptool2 is advantageous due to the following reasons:

- There is a free version on the Internet which is easily accessible by everyone.
- It can be easily installed and it requires no special equipment.
- It provides the user-friendly environment for the users in order that the users can easily use information sources.
- It covers all encryption methods and it is very widespread [38].

Thus, Cryptool2 is convincing to implement combined encryption algorithms.

2.5 Summary

From the review, the major data security concerns are integrity, confidentiality of data and availability of system. When it comes to payment systems, the data needs to be secured in all aspects since it is sensitive to frauds. There are industry standards and practices of payment card system like the well recognized PCI Data security standard for protecting the data.

Cloud computing is a type of Internet-based computing, where different services such as servers, storage and applications are delivered to an organization's computer and devices by the means of Internet and promises several attractive benefits for businesses and end users. Besides that security is questionable for the cloud providers to be trusted for providing their facilities.

Although there are different techniques to secure data on the cloud, such as application of encryption algorithms, robust authentication, access control methods and security policies are some of them. There are also reference architecture implement on the cloud through the various cloud provider companies to be used as reference architecture for the various organizations. Plus to that there are enterprise security architecture frameworks developed so far like SABSA and TOGAF 9.1 which can be adapted to a data security framework.

Cloud computing and cryptography simulation tools are the last review idea like CloudSim, CloudAnalyst, Smartsim, Groundsim, DCsim, MR-CloudSim and Cryptool2. Among those CloudSim is a suitable alternative framework for modeling and simulation of Cloud computing.

Chapter Three: Related Work

This Chapter presents a review of five most related works among cloud data security framework for the banking industry and related security framework. We will try to analyze and identify gaps that exist in previous works. Finally, we summarize the works reviewed.

A cloud security framework for banking industry was proposed in [12]. The research problem is about the security challenge of moving financial, personal data and mission-critical applications by banks to the cloud relation to regulatory policy, compliance and standards.

The work aimed to develop cloud security framework for banking industry and address security needs in terms of integrity, confidentiality and availability of information on cloud by defining security requirements of banking services, identifying the security mechanism and measures through classifying resources.

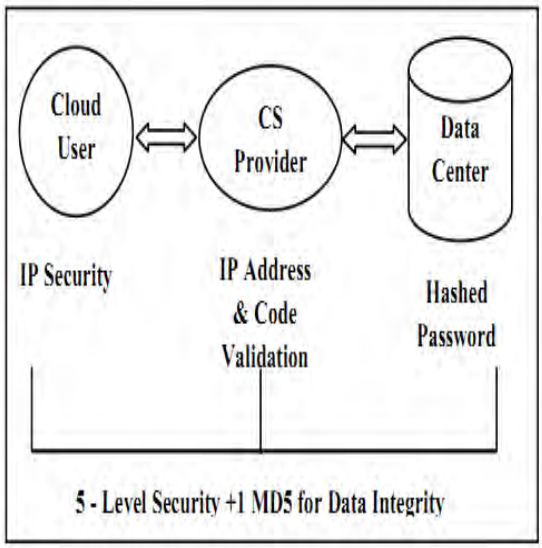
The proposed framework considers all the three cloud service models (SaaS, PaaS, IaaS) and deployment models (Private, Community, Hybrid and Public) of cloud. Sherwood Applied Business Security framework is used as a guide for designing and framework aggregates different templates (Risk Matrix Template, Control Domain Template, Compliance Matrix Template and Security strategy/ major) that help to come up with a solution for measuring risk, compliance and setting suitable security measure. Then it is tested through mapping the proposed security framework to the company security requirement.

Limitation: - the work, identifies security mechanism and measures in relation to regulatory policy, compliance and standards. But since the research is about banking data security, security tools, algorithms under the security strategy should be included. The proposed general framework took the banking data. Neither focuses on payment card data nor on the data on transmission.

The work in [19] proposes a five level security model for cloud computing that introduces strong authentication, confidentiality and integrity mechanisms for storing the data of the client at the data center.

The paper proposes a triple security authentication scheme, with hashed password storage. The IP address is sent with the encrypted identity code to the Cryptographic Service Provider (CSP), the code is decoded and checked at the CSP, stored and passed on to the data centre where code is checked, password is generated and hashed form is stored in the system using a hash function.

The data confidentiality and integrity is provided through Message-Digest Algorithm (MD5) cryptosystem hash technique. In case of change in IP address encountered a notification is sent to the user for the confirmation in change, if assured then the message is preceded to the data center. The proposed 5-level security model for cloud computing that provides authentication, integrity and confidentiality are shown in Figures 3.1 and 3.2.



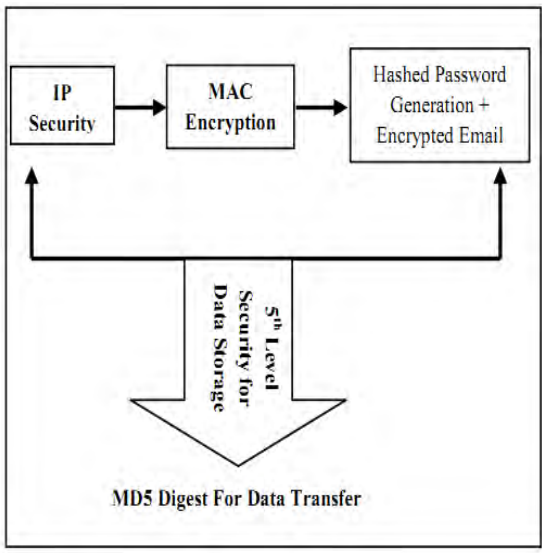


Figure 3.1: Basic Five Level Securities in Cloud *Figure 3.2: Five Level Securities in Cloud*

The authenticity of data center is provided through the encrypted e-mail carrying the password. This is a very strong feature, providing a secure password as once generated and converted cannot be accessed by anyone except the user. The confidentiality and integrity is provided through hash password, MD5 digest.

Limitation: - A 5-Level Security Approach proposed a strong authentication, confidentiality and integrity mechanisms for storing the data in the cloud and describe the technique phase

to achieve the security. The research is limited to data on storage. Encryption techniques are not explicitly stated.

The work in [20] developed a set of guidelines and best practices describing India Reference Architecture Banking Technology (IDRBT) cloud security framework as a practical, simple and easy to use guidebook that will help banks to understand and explore security concerns in the cloud environment. The general security framework is shown in Figure 3.3.

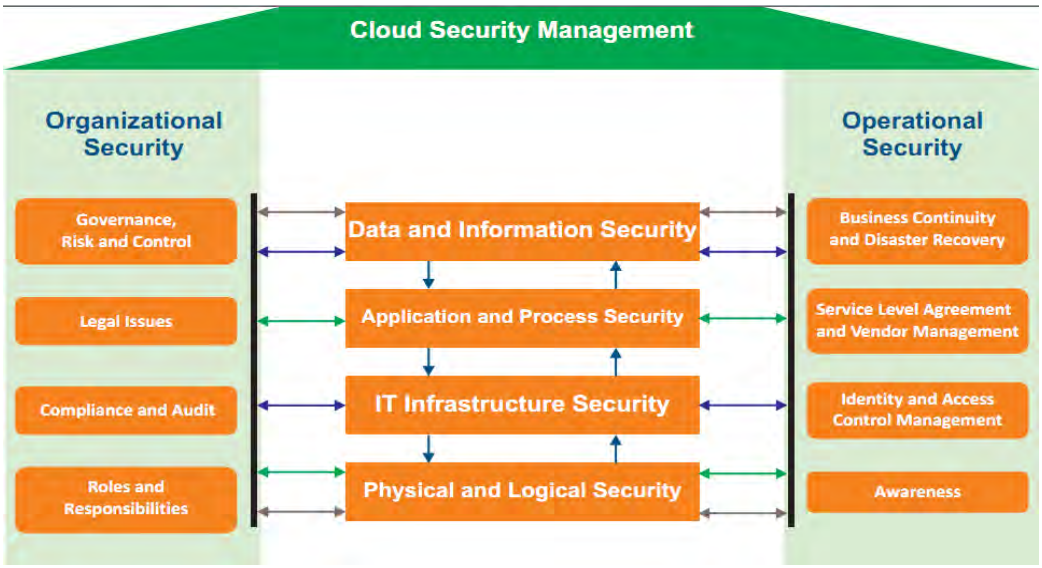


Figure 3.3: IDRBT Cloud Security Frameworks

IDRBT Cloud Security Framework consists of security levels that are categorized into horizontal layers and vertical layers. It describes about each of the security layers.

- Data and Information security provides protection for unstructured and structured data from data privacy, data loss, data disposal, and unauthorized access according to the nature and business value of information.
- Application and Processes security has become a major concern while accessing an application from the cloud. In a multi-tenant cloud environment, this provides security to applications and processes and to their patches and upgrades.
- IT Infrastructure security provides data protection concerns in networks, and virtual environments and it also describes the encryption and monitoring related issues.

- Physical security provides awareness and protection of people, security, and physical resources.
- Logical security techniques are used along with physical security to provide complete security to distributed business critical data and systems.

Limitation: - IDRBT is developed as best practices describing Indian banking sector cloud security framework. The framework focuses neither on a separate layer nor on a specific data life cycle. There are no security techniques selected and attached to the framework layers and banking data source is indistinguishable.

The work in [30] proposes a new security framework between session layer and transport layer such that it is transparent to the application layer and the lower layers. So whenever data is transferred by the client it is first secured by certain authentication protocols and saved at the server end. With this, the data will be stored in a secured way at server end. Those who want to download the data or view it should be connected or have access through the same framework to view the data. This is done in application user level so that the data will be secured and transferred where there is a need to disturb any lower layers of the network. The design of the system is shown in Figure 3.4.

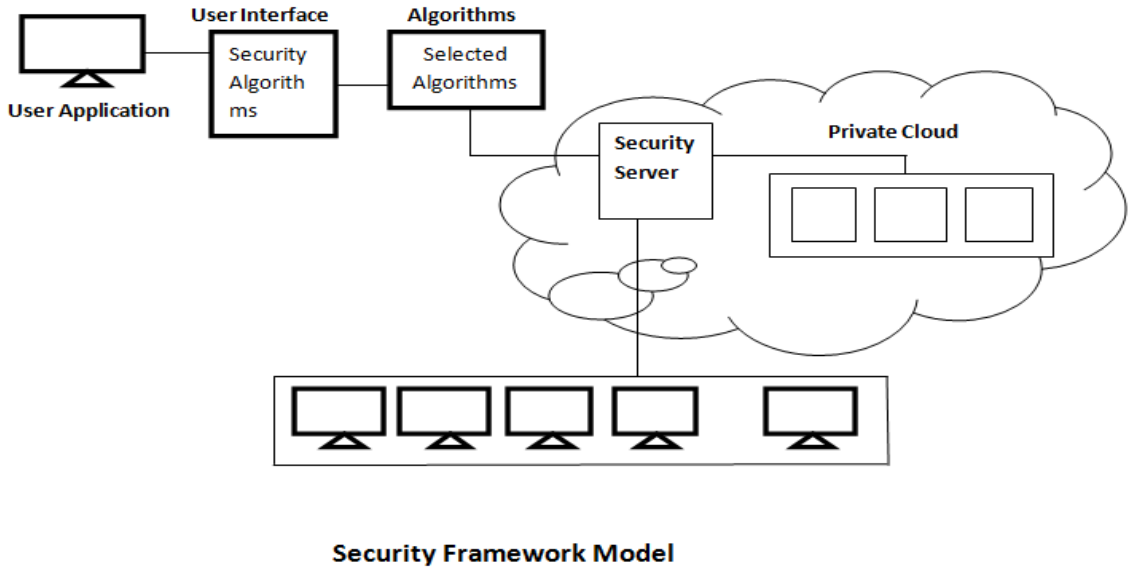


Figure 3.4: System Architecture

When any other user wishes to select any document from the data center, it is required to be connected to the same secure server to get the original document. This helps in security and privacy of the documents. The sender and receiver process are shown in Figures 3.5 & 3.6.

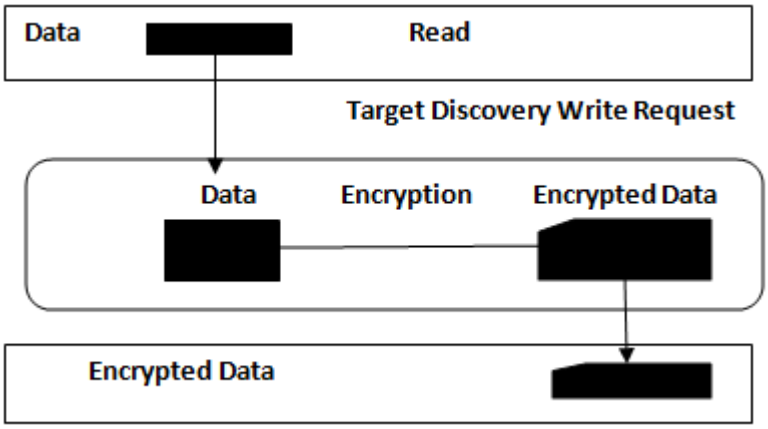


Figure 3.5: Process at Sender

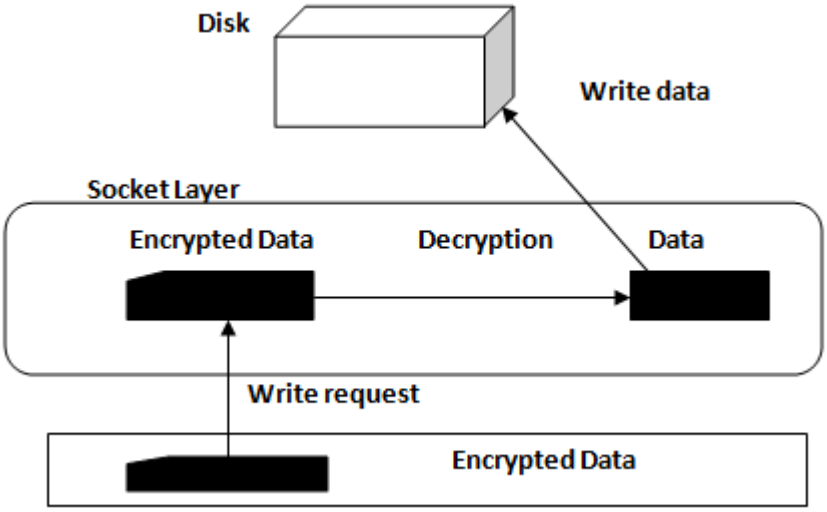


Figure 3.6: Process at Receiver

Limitation: - the security framework model focused on the secured ways of data transmission between a client and data center while the availability of data is limited since it

is required to connect a single secure server to get the data. Security is achieved through a single secure server. It is neither focused on payment card system data.

Since security is one of the main issues in cloud computing, the new data security solution introduced to increase security in the cloud computing [38].

The new security solution provided a strong solution by combining hybrid encryption and digital signature to guarantee data protection and data integrity. The proposed method uses the hybrid encryption algorithm and digital signature scheme. It uses both symmetric key algorithm and asymmetric key algorithm in order to transfer and save the data in the network. The encryption and decryption of the proposed solution are shown in Figures 3.7 & 3.8.

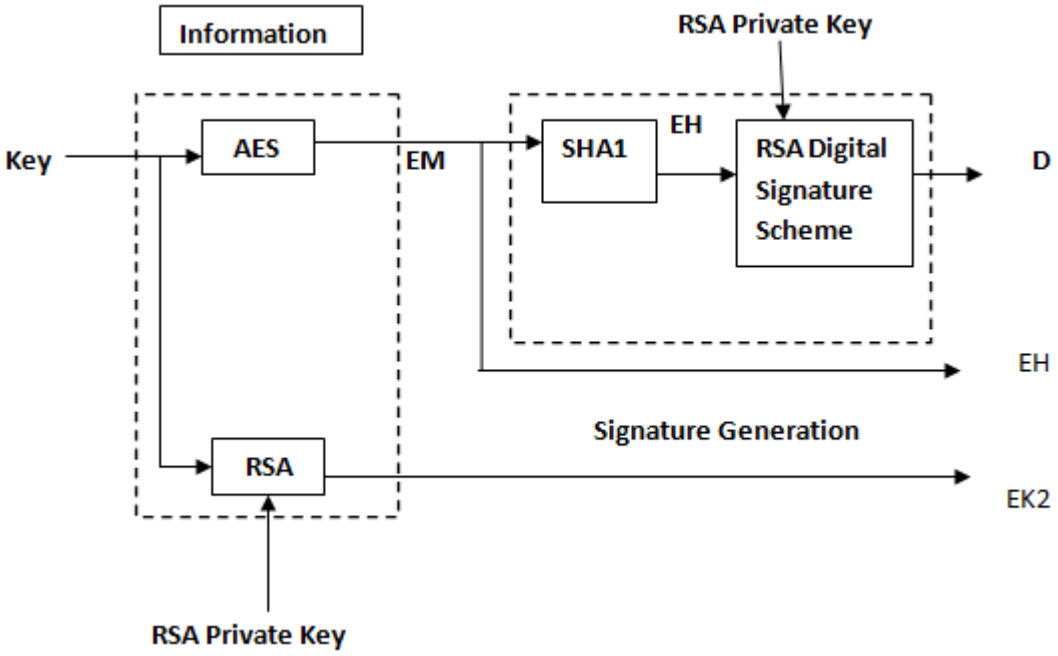
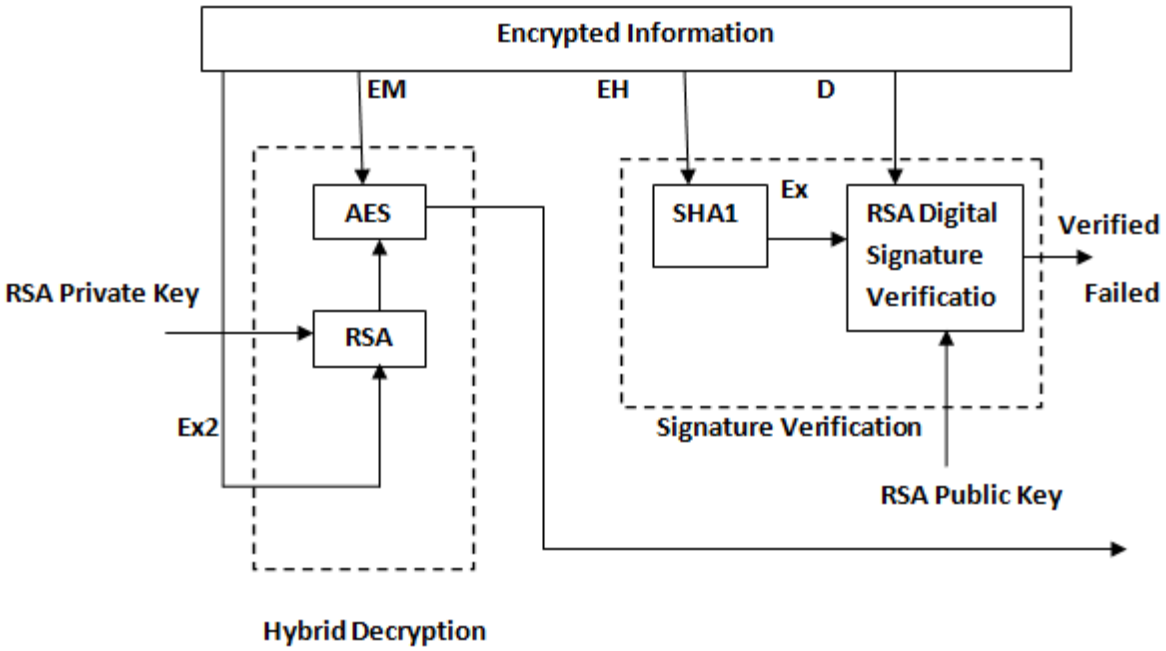


Figure 3.7: Encryption of Proposed Method



K=RSA-Decrypt (Ek2)

M=AES-Decrypt (EM)

EH=SHA-1 (EM)

EH=RSA-verify (D)

Figure 3.8: Decryption of Proposed Method

Cryptools2 is used to create digital signatures, analysis and implement the algorithms.

Limitation: - the proposed solution guarantees data protection and data integrity while using hybrid encryption and digital signature. In the design there is a repetition of RSA algorithm that will take time on the process of encryption and decryption. The evaluation phase requires a sample data passing through the hybrid encryption and applied to the digital signature.

Summary

This Chapter presented related works against the required objective of the thesis. They cover security framework on data transmission and storage in the cloud, security framework for banking industry and data security solution through a hybrid encryption and digital signature in the cloud.

From the review, since data security is about confidentiality, integrity, availability and access control of the data, the related works attempted to ensure those issues through encryptions, hashing algorithms, and integrating security frameworks where stored data and data on transmission are the area of emphasis.

There are also limitations observed so far in the related works that will be addressed by this thesis work through the cloud data security framework for payment card system focused on the stored and data on transmission.

Chapter Four: The Proposed Framework

4.1 Overview

The objective of this Chapter is to have a clear picture of the existing scenario in payment card system process flow focusing on the data security and the proposed solution to secure the data at rest/stored and on transaction/use.

We conducted information gathering through structured questionnaires, structured open interviews and observation. Detailed feedback from the stakeholders is analyzed through issue based analysis technique which is appropriate to the specific case where the information obtained is analyzed under different issues and existing framework of the payment card system reviewed for future suggestions on the proposed cloud data security for the payment card system that will be covered under this Chapter.

4.2 Design Preliminaries

In this research the primary information is obtained through structured questionnaire, structured open interviews and observation. Secondary data source like, books, reports, journal, thesis, conference articles and white paper from the websites of reliable authors and organizations have been used to get information about cloud data security of payment card system.

The existing payment card system is observed with respect to its security and cloud computing practice in the three different banks in Ethiopia namely Nib International Bank, Awash International Bank ,United Bank who were a first clients of PSS where the place questionnaires and interviews were conducted.

a. Questionnaire

In this research there are two structured questionnaires. The first questionnaire is for PSS professionals having five sections including respondent"s detail, ATM, technology and infrastructure, security and cloud computing practice. The second one is for IT professionals within the banks having three sections including respondent"s detail, payment card system data security and cloud computing practice. These questionnaires conducted for

a total of 13 professionals from the PSS and first PSS client banks (Awash, Nib and United international banks). The full questionnaire is attached at Annex B, C.

According to the issue based analysis, the questionnaires analysed based on four topics as discussed below.

- **Introduction about ATM**

According to information replied from the questionnaires, ATM is a machine that lets us control our bank accounts to withdraw, transfer, deposit (not operational in Ethiopia) and other services and make a life of customers easier. The so called payment card systems servers 24/7 creating cashless society and reduce manual work of banks in the opening hours of the day.

- **Technology and infrastructure**

Under technology and infrastructure of payment card system, latest technologies are involved. The database technology in use for payment card data management system is oracle 11g.

The operating system technology in use by the payment card system application and data servers is the Linux operating system which is a secured operating system. The application integrated so far to form the payment card system in the sample banks are the core banking system and payment switch solution.

The communication between the bank, payment switch solution and the different terminals is through the means of VPN, DSL, and other wireless technology.

- **Payment card system data Security**

The payment card system by PSS follows the data security police of PCI DSS. Data security techniques implemented is as shown in Table 4.1.

Table 4.1: PSS Payment Card System Data Security Methods

Security aspects	Data security techniques
Data and information	public key infrastructure, access control and cryptography
Data confidentiality	data encryption, and user id / password
Data integrity	RAID parity, file permissions and user access controls
Data availability	system upgrade, redundancy, failover and RAID high availability clusters
Security aspects	Data security techniques
Application and process	Cryptography, access control and session lock

Despite all the above techniques to secure the payment card system service, there is an unsecured way of data communication between terminals and payment applications.

- **Cloud computing practice**

The experience of cloud computing in a case of Ethiopian banks is uncommon. According to the information gathered, Enat international bank adopts their swift operation to the cloud. There are also a few signs on agent banking and swift operation in similar sectors.

According to the questionnaire response, Enat international bank is using a public cloud named swift light 2 that provides application as a service, platform as a service and infrastructure as a service. The security of light 2 is through the SSL certificate, username/ password and token. Based on the new cloud service that the bank started to receive security, availability, reliability, respond time for incoming and outgoing swift messages problem is improved. There is no worry about down the gateway, no need of the updated version and message transferring speed problem.

According to the questionnaire response, almost all IT professionals and operational are willing to move to the cloud and they are aware of its benefits like flexibility, disaster recovery, automatic software update, security and work from anywhere despite the negotiation with NBE (National Bank of Ethiopia) procedures and approval.

Conducting the questionnaires, we realized that there is an unsecured way of data transmission between the ATM terminals, payment card system and core banking system even though there are some securing techniques used in the payment card system. There are also internal frauds seen in the area.

According to the questionnaire, PSS payment card system activity flow is shown in Figure 4.1.

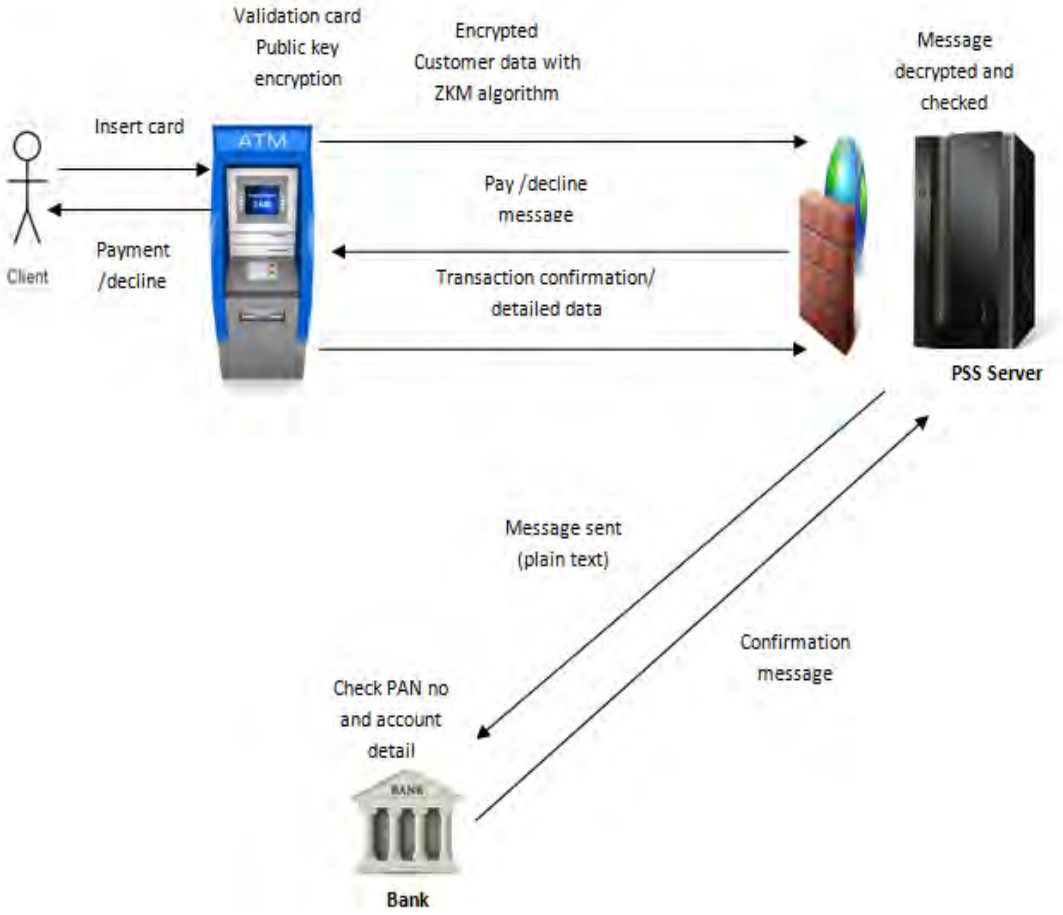


Figure 4.1: PSS Payment Card System Activity Flow

b. Interview

In this research there is structured opened interview prepared for bank IT managers, bank IT staffs and PSS professionals. The interview holds three sections under each professional position. For IT managers, there are policy, managerial questions and general questions and for IT, PSS professionals, security and technology questions.

The interview conducted for a total of 8 professionals from the PSS, first PSS client banks (Awash, Nib and United international banks) and Enat international bank. The full interview is attached at Annex A.

The interview analyzed though the issue based analysis technique. The interview findings are organized based on the research focus areas for different professionals under policy, managerial, general, security and technological areas.

According to the interview analysis, there are 19 banks in Ethiopia and among them six of them are under PSS service. There are security policies, standards and guidelines for banking industry, which is more or less similar to each other. There are also similar policies with the third party handling the payment card system called PSS.

Concerning security, there is an unsecured way of data transmission and unlimited access control on library files since it has some access control mechanism enforced so far like session lock, remote access, wireless access, concurrent session control, separation of duties and different privilege.

The exposure of cloud computing seems on-one in Ethiopia but according to the information captured so far, there are banks in Ethiopia that uses the public cloud services like swift by Enat international bank and there are also interests in the area especially to implement agent banking projects in the cloud.

Concerning cost related to the payment card system project, interview results stated that it is in millions excluding the regular payment. For instance, Nib International Bank has invested approximately 165 million ETB to implement the payment card system project. The full interview is attached at Annex A.

Conducting the interview, similarly we realized that there is an unsecured way of data transmission and access control problems in library files related to the payment card system. Implementing a payment card service is a huge investment as a project and there is also an annual cost after implementation despite the network, operational and security problem facing by the clients. In addition to that internal frauds due to different reasons are being one of the threats.

In addition to the questionnaire and interview, an observation contributes on data collection and analysis. Payment card system process flow is analyzed through the process and verified by the concerned body. Figure 4.2 shows the existing payment card system flow.

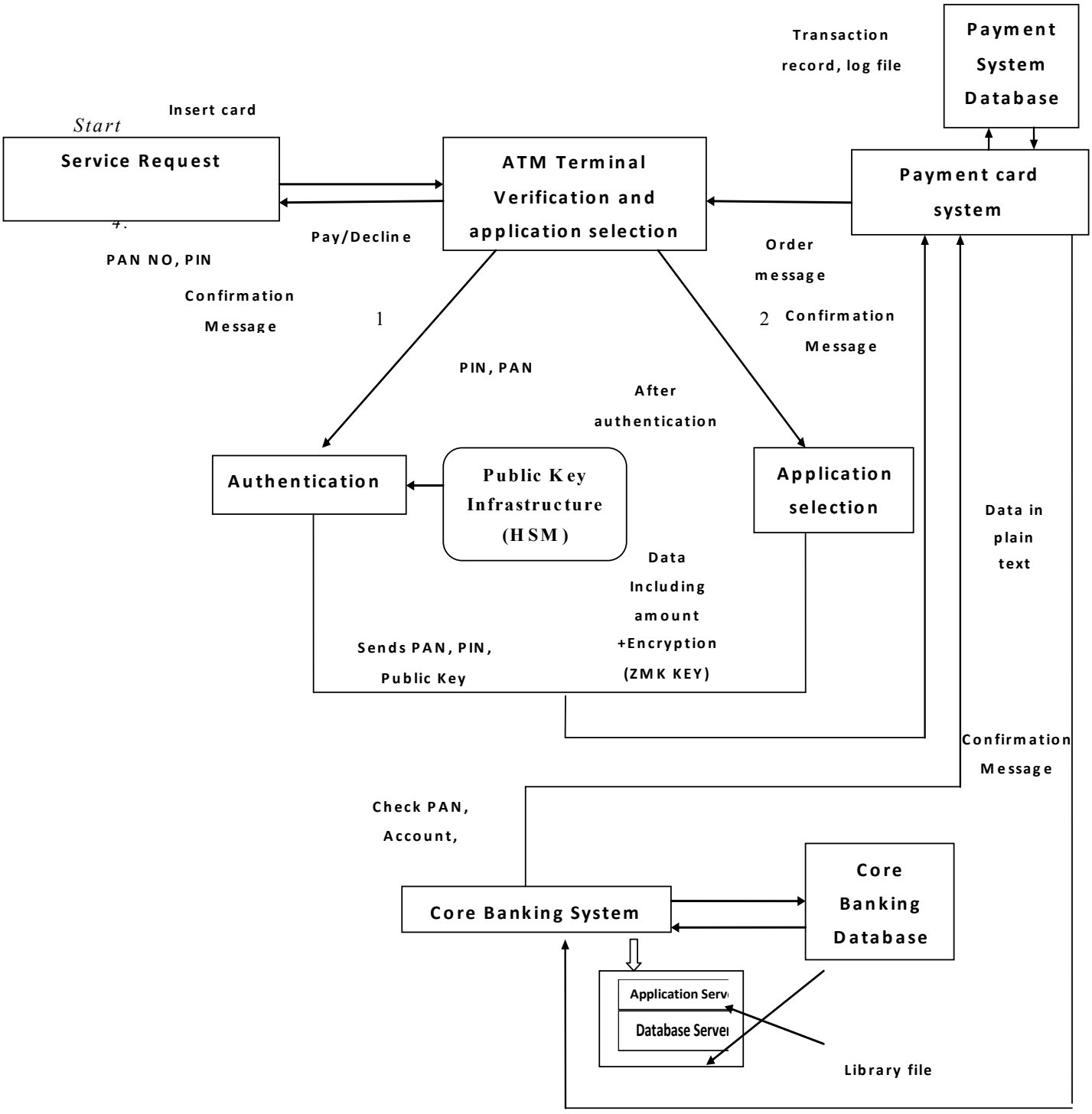


Figure 4.2: Existing Payment Card System

As shown in Figure 4.6, unsecured way of message exchange between the core banking and payment card system and unlimited access control rights on library files is observed. Public key infrastructure and ZMK encryption are the ways of protecting transferring data between

ATM terminals to the payment card system. Therefore, the proposed framework introduces a new security component containing combined encryption algorithm.

The proposed framework implements hybrid cloud deployment model to increase the security of financial data transaction within the control of the data owners and the framework structure follows the data security framework of TOGAF 9.1 to optimize the risk of transactional and stored data where the TOGAF 9.1 addresses similar scenarios. CIA – Confidentiality, Integrity and Availability of a data ensures through the combination of encryption algorithm AES and RSA plus SHA-2 hashing algorithm, role-based access control (RBAC) and backups.

The stored data and in transit is the main concerns that will be secured under the proposed framework. Data in storage includes payment card system database and core banking database having customer, account information, payment card information and transaction history.

Although encryption of stored data is mainly the focus for security since it is more likely that a hacker will target systems with data on local drives or storage networks, encrypting data in transit is also important to avoid potential interception by unauthorized persons. Data in transit includes data that travels across the Internet, from tier to tier within an application like transaction data between ATM terminals, payment card system and core banking system.

4.3 Components of the Proposed Framework

The proposed cloud data security framework for a payment card system is divided into three different modules as shown on Figure 4.2 where each module contains five or more components.

4.3.1 ATM Terminal Module

The ATM terminal module contains components called service request, card issue, ATM terminal application, authentication, application selection and secured data transmission interface.

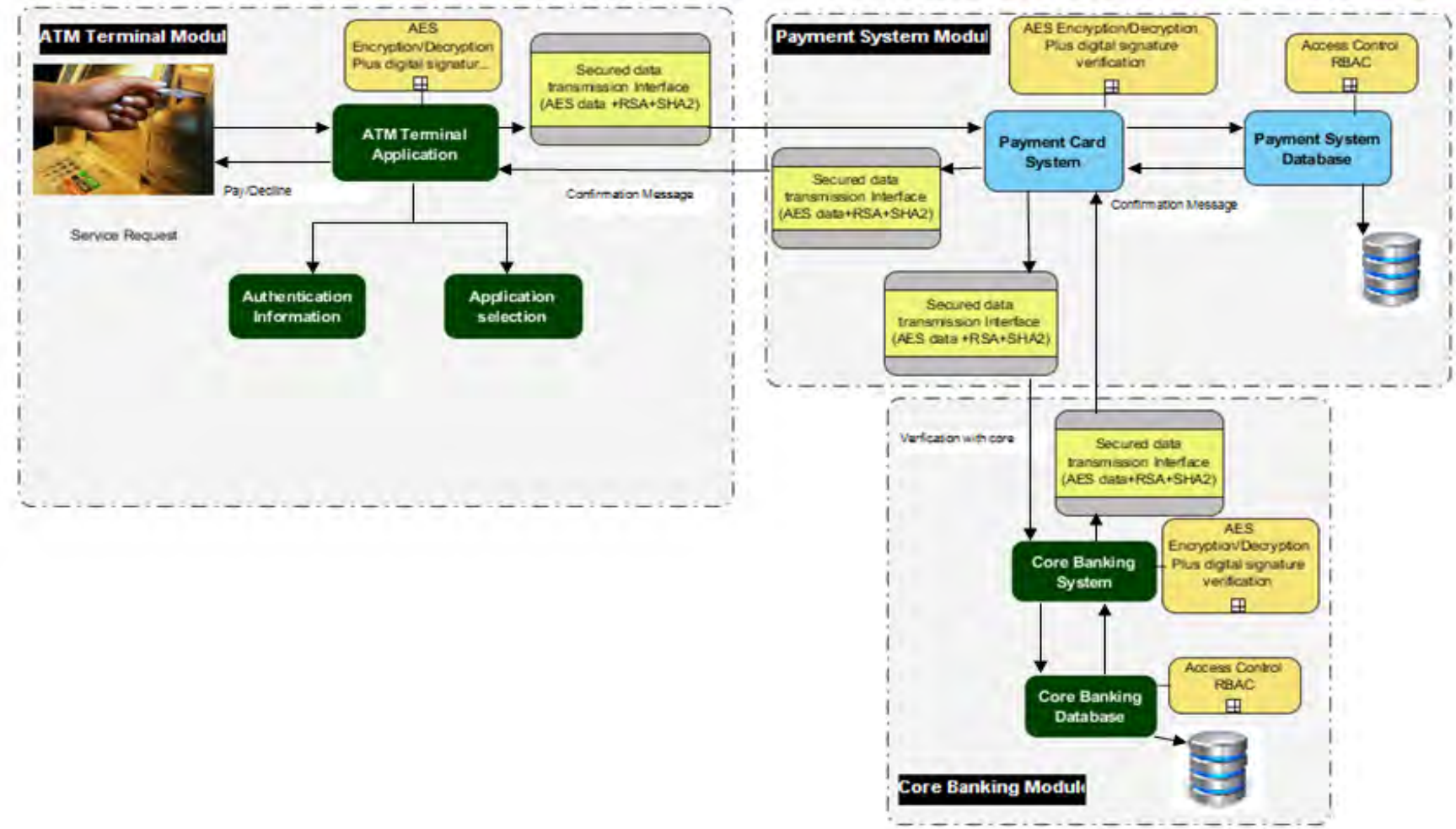


Figure 4.3: Proposed Cloud Data Security Framework for a Payment Card System

Service request represents the client request both to issue cards and order payment through manually and ATM terminals respectively. Card issue is the process performed between the bank and the customer. The customer requests a payment card service in order to access her/his account. According to the formal procedure a card is prepared and issued to the customer. Payment card details like PAN No and PIN are created on payment card system and attached to the specific account in the core banking system to allow the service.

ATM terminal is the device used as a terminal to transact card payment. An application is installed on these terminals to send information about card owner and application selection information to the payment card system and receive a final message for payment execution. There is a sub process called AES algorithm encryption applied to the terminal application data to ensure the data confidentiality.

Authentication and application selection are the two tasks of terminal application. Authentication is all about authenticating the right privileged payment card customer of the bank. With the above framework, it is a place where client identification of an ATM users will be identified using PAN No, and PIN through the communication between the terminal, core banking and payment card system. Application selection is about the specific transaction type that the user will select and related details.

Secured data transmission interface is a security component responsible for interfacing a data transmission between the non-cloud application and cloud based application. It contains combined encryption algorithms named AES, RSA and SHA2. AES algorithm is selected for this specific case based on the fact that this algorithm is more secured and preferable due to the different research result stated in Section 2.4.4.1. It is used to ensure the confidentiality of data within the application and on the data transmission between the applications.

RSA encryption is used to ensure data integrity in the cloud data security framework at a time of data transmission. Transmit data from non-cloud application to cloud application in an encrypted and signed way. RSA encryption is selected due to the fact that RSA algorithm is more suitable to insure data integrity according to research result covered under Section 2.4.4.2.

The SHA-2 hashing algorithm is a cryptographic hash function applied in digital signature as well as in data integrity. SHA-2 combined with RSA encryption applied to the data for transmission to conserve the data integrity between the applications. Algorithm 4.1 shows the pseudo code of data flow in ATM terminal module of our proposed framework.

```
<User swipes the ATM card>
Do you want to proceed (yes/no)?
<User pushes yes button>
Enter PIN No.:
Choose transaction: Deposit or Withdrawal or Balance
Inquiry:
<User selects the button for deposit>
Enter amount:
Do you want to issue a ticket (yes/no)?
<User pushes yes button>
AES encryption is applied to the input data
Encrypted data + RSA+SHA2
Encrypted and signed data send to PS
```

PS: Payment System

Algorithm 4.1: Pseudo-code of ATM Terminal Module

4.3.2 Payment System Module

The payment system module contains payment card system, payment system database and secured data transmission interface.

The payment card system is one of the cloud components where payment is processed and forwarded to the final terminals to be paid or transaction declined after the confirmation processes with the core banking system. It is a place where PAN No, PIN, account no and similar details are validated and processed for payment. AES encryption/ decryption is applied to the payment card system data to ensure the data confidentiality.

In the payment card service process, data is stored on two sides. The first one is on the payment card system database which is in the cloud having card detail, transaction information and history log files. The database is an Oracle database which has a transparent data encryption algorithm applied to protect stored data.

In the proposed framework access control is a sub process on the payment system database. It enforces access control measures for systems, programs, processes, and data. Role-based access control model has been incorporated in the proposed framework since RBAC is a viable model for cloud computing environment, according to the previous research result reviewed under Section 2.4.4.3.

Secured data transmission interface is another component in this module. The data from payment system passes through the secured data transmission interface. AES algorithm is applied to data confidentiality and RSA plus SHA2 at time of data transmission to ensure data integrity. Algorithm 4.2 shows the pseudo code of data flow in payment system module of our proposed framework.

```
Data decrypted and verified in PS
Data send to PS database
If (PAN, PIN and Account No) exist in PS database
      {
      Encrypt the data with AES
      Encrypted data + RSA+SHA2
      Encrypted and signed data send to CS
      }
Else
      {
      AES encryption is applied to the replied message
      Encrypted message + RSA+SHA2
      Encrypted and signed message send to AT
      Message decrypted and verified in AT
      Application reply based on the rejection message
```

```
            Payment declined
            }
```

AT: ATM Terminal CS: Core banking System PS: Payment System

Algorithm 4.2: Pseudo-code of Payment System Module

4.3.3 Core Banking Module

The Core banking module contains core banking system, core banking system database and secured data transmission interface.

Core banking is a banking service provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices. It is often associated with retail banking and many banks treat the retail customers as their core banking customers.

The banks make these services available across multiple channels like ATM, POS, Internet banking and mobile banking in addition to branches.

Core banking system is an application where all core banking functionalities come true. Related to the payment card transaction, it is a place where an account and customer verification is performed. AES encryption/ decryption are applied to the core banking system data to ensure the data confidentiality similar to the previous two modules.

The second database in the payment service process is core banking system database next to the payment system database where full customer and account information is stored. The core banking system uses mostly an Oracle database whereby data encryption protects the stored data. Role-based access control model is incorporated on the component.

Secured data transmission interface is another component similar to the payment system module. The data from core banking system passes through the secured data transmission interface. Algorithm 4.3 shows the pseudo code of data flow in core banking module of our proposed framework.

```
Data decrypted and verified in CS
Data send to CS database
If (Account No +account balance) exist in CS
database
     {
     Encrypt the confirmation message with AES
     Encrypted message + RSA+SHA2
     Encrypted and signed message send to PS
     Message decrypted and verified in PS
     Message checked
     AES encryption is applied to the replied
     message
     Encrypted message + RSA+SHA2
     Encrypted and signed message send to AT
     Message decrypted and verified in AT
     Application reply based on the confirmation
     message
     Payment successful
     }

Else

     {
     AES encryption is applied to the replied
     message
     Encrypted message + RSA+SHA2
     Encrypted and signed message send to PS
     Message decrypted and verified in PS
     Message checked
     AES encryption is applied to the replied
```

```
                Message
                Encrypted message + RSA+SHA2
                Encrypted and signed message send to AT
                Message decrypted and verified in AT
                Application reply based on the rejection
                message
                Payment declined
                }
```

AT: ATM Terminal CS: Core banking System PS: Payment System

Algorithm 4.3: Pseudo-code of Core Banking Module

Algorithm 4.4 shows the pseudo code of single data flow from a client terminal to the payment card application in the proposed framework.

```
Input PAN No
AES encryption applied to Input data
Encrypted data +RSA_SHA2
Encrypted and signed data sent to PS
Verification on data
Data decrypted
Compare PAN No in PS database
If (PAN No) exist
     AES encryption applied to PAN No + data
     Encrypted data +RSA+SHA2
     Encrypted and signed data sent to CS
     Verification on data
     Data decrypted
```

```
Compare Account No, balance detail in CS
database
If (account no and balance) exist
     AES encryption applied to message
     Encrypted message +RSA_SHA2
     Encrypted and signed message sent to PS
     Message checked
     AES encryption is applied to the replied
     message
     Encrypted message + RSA+SHA2
     Encrypted and signed message send to AT
     Message decrypted and verified in AT
     Application reply based on the confirmation
     message
     Payment successful

Else

     AES encryption is applied to the replied
     message
     Encrypted message + RSA+SHA2
     Encrypted and signed message send to PS
     Message decrypted and verified in PS
     Message checked
     AES encryption is applied to the replied
     message
     Encrypted message + RSA+SHA2
     Encrypted and signed message send to AT
     Message decrypted and verified in AT
```

```
                Application reply based on the rejection
                message
                Payment declined
    Else
          AES encryption is applied to the replied message
          Encrypted message + RSA+SHA2
          Encrypted and signed message send to AT
          Message decrypted and verified in AT
          Application reply based on the rejection message
          Payment declined
```

AT: ATM Terminal CS: Core banking System PS: Payment System

Algorithm 4.4: Pseudo-code of Single Data Flow

4.4 Summary

In this Chapter, we described the empirical findings, design consideration in effect and the proposed cloud data security framework for payment card system with its components. Questionnaire, interview and observations are conducted for data collection and analysis. Analysis reflected that there is an unsecured data transmission between the ATM terminals, payment card system and core banking system, unlimited access control right and internal fraud.

Thus the security solution is recommended by the proposed cloud data security framework for the payment card system. The proposed framework has three modules: ATM terminal, Payment system and Core banking having components group together. Secured data transmission interface is the new security component in the proposed framework. It is composed of three different algorithm named AES, RSA encryption algorithm and SHA-2 hashing algorithm for secured data transmission between the cloud and non-cloud applications. The access control method named role–based access control is another component of the proposed framework. All the components in the proposed framework are

direct participants in the securing process, i.e., the output of one component will be the input of the next component. In the next chapter, we will describe the prototype detail of the proposed security component.

Chapter Five: Prototype and Results

5.1 Overview

The proposed framework is designed based on the data security framework of TOGAF 9.1. It ensures data confidentiality, integrity and availability. The development environment, programming language and simulation tool that is used for prototyping of the proposed framework is described in this Chapter. Prototype for the security component of the framework is discussed with support of screenshots based on the corresponding results. The prototype has two parts. The first one is simulating the combined encryption algorithm that will be applied to the data at the time of transfer and the second one is applying the combined encryption algorithm on a data transfer from client to cloud storage through the simulation tools.

5.2 Development and Simulation tools

CloudSim and Cryptool2 are the main tools used in this research. We have discussed about CloudSim in Chapter Two under Section 2.4.7. It is a new generalized and extensible simulation toolkit that enables seamless modeling, simulation, and experimentation of emerging Cloud computing systems and application, infrastructures and management services [47, 48]. CloudSim is actually a Library for Cloud Simulation written in Java Language that can be added to our source files. Since it is Java, the CloudSim uses fully-featured Java IDE named Eclipse.

Cryptool2 is the tool for analyzing, learning and implementing algorithms with usual and practical manner. We have discussed more in Chapter Two under Section 2.4.7. CloudSim is used for simulating cloud environment and Cryptool2 used to implement combined encryption algorithms.

5.3 Prototype Implementation

The prototype implementation is divided into two parts as discussed below.

5.3.1 Combined Encryption

Cryptool2 is used to simulate the combined encryption shown on the proposed framework. It is cryptographic tool used to analyze and implement encryptions and hashing algorithms. Single input data is encrypted through the simulation.

The security component named secured data transmission interface which is composed of encryption algorithms protects the input data throughout the data flow. Here is the simulated result of the combined encryption within a security component as shown in Figure 5.1

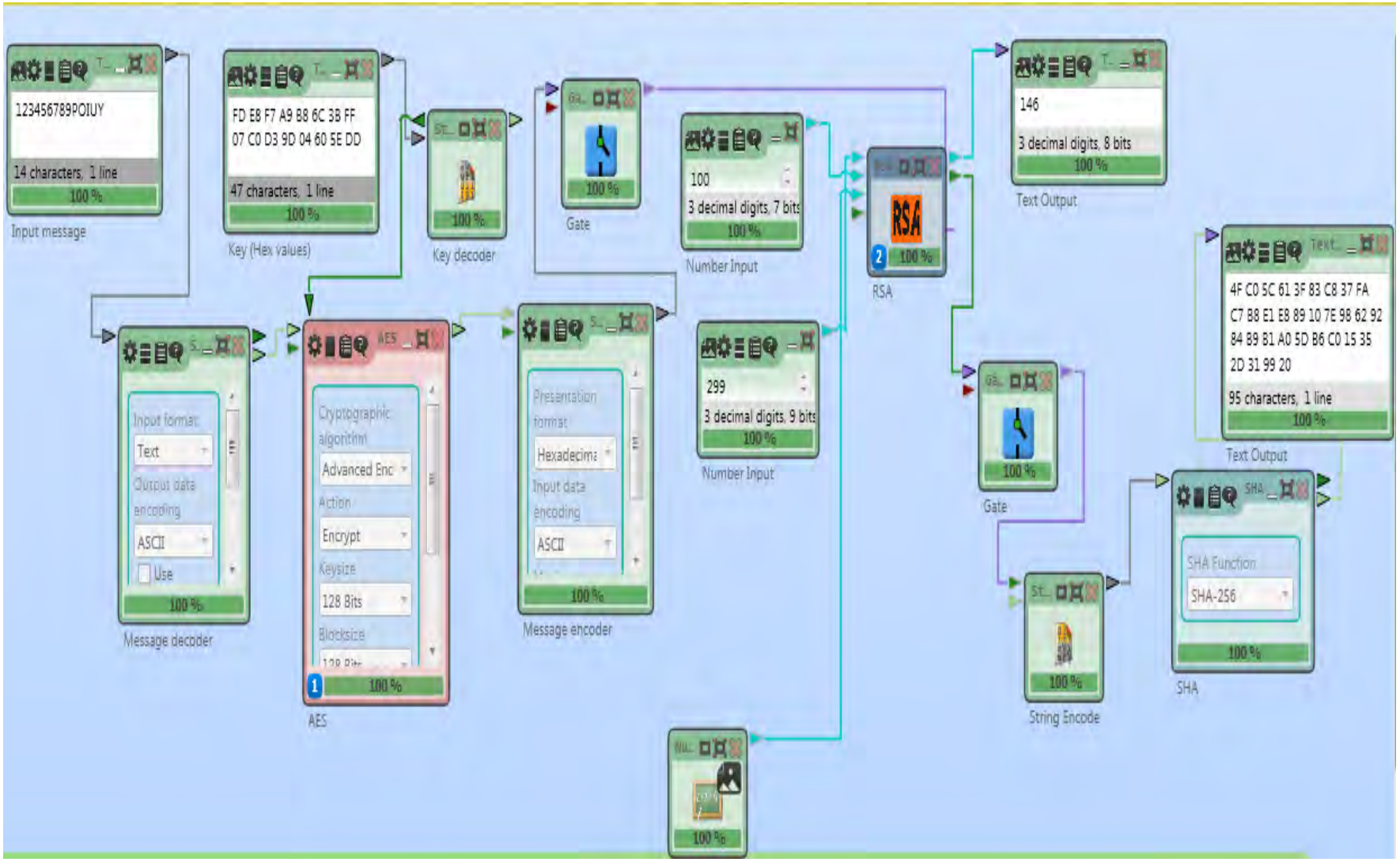


Figure 5.1: Simulation Output of AES, RSA and SHA2 on Crypto Tool2

5.3.2 Combined Encryption on Data Transfer to the Cloud

CloudSim is a toolkit (library) for simulation of cloud computing scenarios. There are three steps required in order to apply the combined encryption on the data transfer to the cloud.

Modeling on the cloud is the first step to simulate in CloudSim. Modeling is about designing and creating data centers, hosts, virtual machines, a broker and cloudlets. The proposed data security framework for the payment card system model on the cloud is shown in Figure 5.2.

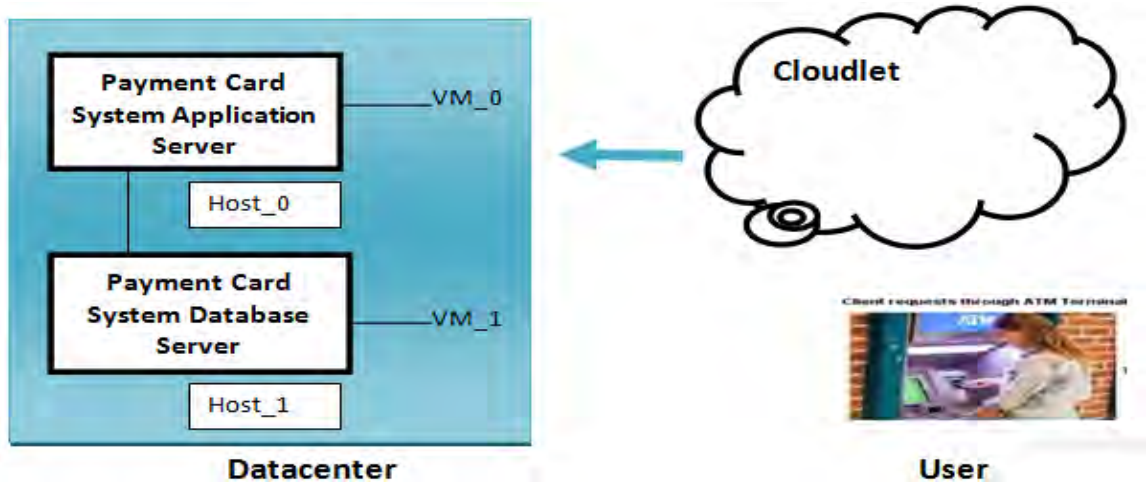


Figure 5.2: Cloud Model of the Proposed Framework

In the CloudSim the model is modeled on the environment as shown in Figure 5.3.

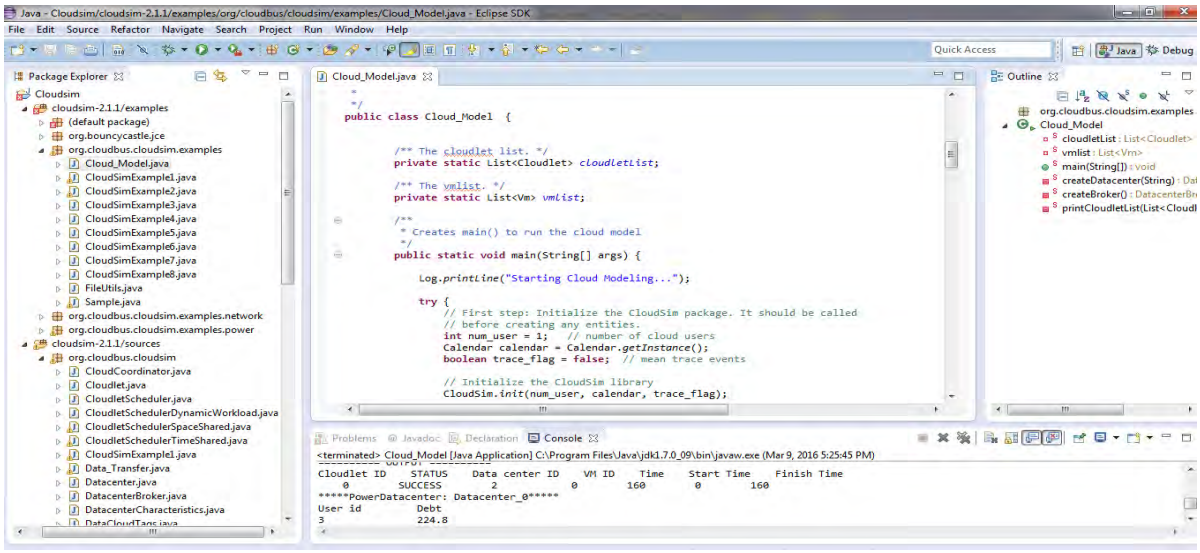


Figure 5.3: Working Environment of CloudSim Simulation Tool

The simulation result is shown in Figure 5.4.

```
Starting Cloud Modeling...
Initialising...
Starting CloudSim version 2.0
Datacenter_0 is starting...
Broker is starting...
Entities started.
0.0: Broker: Cloud Resource List received with 1 resource(s)
0.0: Broker: Trying to Create VM #0 in Datacenter_0
0.0: Broker: Trying to Create VM #1 in Datacenter_0
0.0: Broker: VM #0 has been created in Datacenter #2, Host #0
0.0: Broker: VM #1 has been created in Datacenter #2, Host #1
0.0: Broker: Sending cloudlet 0 to VM #0
160.0: Broker: Cloudlet 0 received
160.0: Broker: All Cloudlets executed. Finishing...
160.0: Broker: Destroying VM #0
160.0: Broker: Destroying VM #1
Broker is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for
shutting down.
Datacenter_0 is shutting down...
Broker is shutting down...
Simulation completed.
Simulation completed.

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID    Time    Start
Time    Finish Time
    0              SUCCESS        2            0             160
0          160
*****PowerDatacenter: Datacenter_0*****
User id          Debt
3              224.8
**********************************
Cloud Model finished!
```

Figure 5.4: Simulation Output of the Proposed Framework Cloud Model

Figure 5.4 shows that **Host #0** and **Host #1** are created on a **Datacenter_0**.A **cloudlet 0** is created to send a request to **VM #0**.

The second step is data transfer from the terminal to the cloud based payment application through the combined encryptions in the CloudSim. The simulation shows the first three steps in data flow and send the encrypted data to the cloud.

1. A terminal accepts the customer input data, e.g., PAN No.
2. The input data is encrypted with AES.
3. The encrypted data plus RSA +SHA2 (encrypted data are signed) and then send the final signed data to the cloud based payment application hard disk storage.

The simulation result is shown in Figure 5.5.

```
Starting Cloud Modeling...
Initialising...
Enter a PAN No
1234567891kjiou2
* * *
data encrpted
á?5Áê®"?R¡B´___~
* * *
encrpted data signed

 „þÅÑE
▯¦O €HÞq'Tiz? €%▯Gm▯AËéBØi▯m*£hâ‡▯™5fgneÃÝ ▯,mÌò½x¥%{8íBY ▯▯▯U.¨üÁ3Óyga¨Ž >⁰åføÚb▯˜´h‟«ŠB?ÌmÄë`}tQì,s–ƒ
* * *
Starting CloudSim version 2.0
Datacenter_0 is starting...
Broker is starting...
Entities started.
0.0: Broker: Cloud Resource List received with 1 resource(s)
0.0: Broker: Trying to Create VM #0 in Datacenter_0
0.0: Broker: Trying to Create VM #1 in Datacenter_0
0.0: Broker: VM #0 has been created in Datacenter #2, Host #0
0.0: Broker: VM #1 has been created in Datacenter #2, Host #1
0.0: Broker: Sending cloudlet 1 to VM #0
160.0: Broker: Cloudlet 1 received
160.0: Broker: All Cloudlets executed. Finishing...
160.0: Broker: Destroying VM #0
```

```
160.0: Broker: Destroying VM #1
Broker is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for
shutting down.
Datacenter_0 is shutting down...
Broker is shutting down...
Simulation completed.
Simulation completed.
* * *
Used disk space on hd1=300.0
* * *
Number of file stored on hd1=1
* * *
Current disk space on hd1=724.0
* * *
Time to transfer the file=38.96484375
* * *
Seek time=0.29296875

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID    Time    Start
Time    Finish Time
    1        SUCCESS        2            0        160        0
160
*****PowerDatacenter: Datacenter_0*****
User id          Debt
3          224.8
**********************************
Cloud Model finished!
```

Figure 5.5: Simulation Output of ATM Terminal Module

Figure 5.5 shows a customer PAN No. encrypted with AES encryption algorithm, encrypted data digital signed and send to the cloud application. **Number of file stored on hd1=1** and **Used disk space on hd1=300.0** KB.

The third step is verifying and decrypting the data transferred from the terminal to the cloud based payment application storage. The simulation shows the following two steps in data flow.

1. Verifying the data
2. Decrypting the encrypted input

The simulation result is shown in Figure 5.6.

```
Starting Cloud Modeling...
Initialising...
Enter a PAN No
1234567891kjiou2
* * *
data encrpted
á?5Áê®"?R¡B´___~
* * *
encrpted data signed
 „þÅÑE
▯¦O €HÞq'Tiz? €%▯Gm▯AËéB▯i▯m*£hâ‡▯™5fgneÃÝ ▯,mÌò½x¥%{8íBY ▯▯▯U.¨üÁ3Óyga¨Ž >®åf▯Úb▯˜´h"«ŠB?ÌmÄë`}tQì,s–ƒj(®▯Õ
* * *


----------------------------------------
==Digital signed verification==
Verify: True
Decrypt: 1234567891kjiou2
Starting CloudSim version 2.0
Datacenter_0 is starting...
Broker is starting...
Entities started.
0.0: Broker: Cloud Resource List received with 1 resource(s)
0.0: Broker: Trying to Create VM #0 in Datacenter_0
0.0: Broker: Trying to Create VM #1 in Datacenter_0
0.0: Broker: VM #0 has been created in Datacenter #2, Host #0
0.0: Broker: VM #1 has been created in Datacenter #2, Host #1
0.0: Broker: Sending cloudlet 1 to VM #0
160.0: Broker: Cloudlet 1 received
160.0: Broker: All Cloudlets executed. Finishing...
160.0: Broker: Destroying VM #0
160.0: Broker: Destroying VM #1
Broker is shutting down...
```

```
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for
shutting down.
Datacenter_0 is shutting down...
Broker is shutting down...
Simulation completed.
Simulation completed.
* * *
Used disk space on hd1=300.0
* * *
Number of file stored on hd1=1
* * *
Current disk space on hd1=724.0
* * *
Time to transfer the file=38.96484375
* * *
Seek time=0.29296875

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID    Time
Start Time    Finish Time
    1        SUCCESS        2            0        160        0
160
*****PowerDatacenter: Datacenter_0*****
User id          Debt
3          224.8
**********************************
Cloud Model finished!
```

Figure 5.6: Simulation Output of Payment System Module

Figure 5.6 shows an encrypted and signed data sent to the cloud application is verified and decrypted in the cloud side and result same value with the original input.

5.4 Summary

In this Chapter, we illustrated the prototype simulation result of the proposed cloud data security framework for a payment card system security component. We used two simulation tools called Cryptool2 and CloudSim to implement one of the security components where data confidentiality and integrity are ensured. Cryptool2 is used to implement the combined encryption algorithms and the CloudSim simulated the model of payment card system in the

cloud and data transfer through the application of the combined encryption solution. The simulation result shows the security component in the proposed framework provides a secured data transfer between non cloud and cloud applications.

Chapter Six: Conclusion and Future Work

6.1 Conclusion

The general objective of this research is to develop cloud data security framework for the payment card system. In order to achieve this objective information gathering and analysis of the existing system, and assessment of recent work on an area of data security, payment card system, issues of cloud computing, data security solutions in the cloud, reference architecture for banking industries, enterprise security architecture framework and cloud data security frameworks for a payment card system and related issues were assessed.

Based on these assessments to address the research problems we designed cloud data security framework for payment card system of Ethiopia. Our framework addresses the previous framework gap by incorporating the encryption algorithms and access control methods in detail in a payment process. The framework considers the best practices in handling payment like PCI DSS global data security standard, framework for card payment schemes-standards, Open Group Architecture Framework TOGAF 9.1 data security framework and cloud data security solutions.

The cloud data security framework for payment card system incorporates the payment application, banking application with respect to their databases, terminal application with stored and data on transmission through security component having encryption algorithms (AES, RSA), hashing algorithms (SHA2), Role-based access control on the databases, and implemented on the simulation tool named Cryptool2 and on the CloudSim a simulation of cloud computing infrastructures and services.

With the application of the proposed framework of the payment card system, the payment card system data security framework is secured compared to the existing framework and it is a good practice in the area of card payment data security framework on the cloud.

6.2 Future Work

There are still several issues regarding the payment card data security on the cloud computing environment that warrant further research. Card validation process, customer identification process to check the credential of the customer, any related data security on

transmission can be seen in the future and integrated in the above framework for a better output.

The following are future works.

- ✓ Testing with different security threats at the time of data transfer and on the stored data for a better approval on the strength and performance of the combined encryption on the security component.
- ✓ Measuring the performance of the combined encryption solution through various parameters such as speed and memory required.
- ✓ Data transfer speed enhancements.

Last but not least, the research should also take into consideration the fact that the cloud is still being developed and continuously changing. Thus the risks identified within this study may need to be updated accordingly.

References

[1] Denning and Dorothy E., “Cryptography and Data Security,” Addison-Wesley Publishing Company, ISBN 0-201-10150-5, 1982.

[2] Summers, G., “Data and Databases,” in Koehne, H Developing Databases with Access: Nelson Australia Pty Limited, 2004.

[3] Open Data Center Alliance Inc., “Open Data Center Alliance: Data Security Framework Rev 1.0,” 2013.

[4] Kaur, Ramandeep and Pushpendra Kumar Pateriya, "A Study on Security Requirements in Different Cloud Frameworks,” International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol-3, Issue1, March 2013.

[5] Maheshwari, Rohit and Sunil Pathak, "A Proposed Secure Framework for Safe Data Transmission in Private Cloud," International Journal of Recent Technology and Engineering 1.1, pp.78-82, 2012.

[6] Ana Bucur, “Banking 2.0: Developing Reference Architecture for Financial Services in the cloud,” Bucharest, Romania, 2011.

[7] Sajid, Mohammad and Zahid Raza, "Cloud Computing: Issues & Challenges," International Conference on Cloud, Big Data and Trust, New Delhi, India, Nov 13-15, 2013.

[8] Forbes Inc., “Some Banks are Heading to the Cloud,” http://www.forbes.com/sites/tomgroenfeldt/2014/06/26/some-banks-are-heading-to-the-cloud-more-are-planning-to/, Last Accessed on 26 June 2014.

[9] Patil, D. H., Rakesh R. Bhavsar, and Akshay S. Thorve, "Data Security over Cloud,” International Journal of Computer Applications, 2012.

[10] Business Insider, “Global Payment Card System Fraud Costs,” In BI Intelligence, 2015.

[11] Aderaw Semma, “Defending the Virtual Infrastructure of Cloud Computing from Denial of Service Attack,” Unpublished Master‟s Thesis, Addis Ababa University,

School of Graduate Studies, College of Natural Sciences, Department of Computer Science, Addis Ababa, Ethiopia, February 2014.

[12] Meskerem Alemu, “Cloud Computing Security Framework for Banking Industry,” Unpublished Master‟s Thesis, HiLCoE School of Computer Science and Technology, Addis Ababa, Ethiopia, August 2013.

[13] Microsoft Corporation, “Microsoft Industry Reference Architecture for Banking (MIRA-B),” May 2012.

[14] Larry Ryan, “HP Enterprise Cloud Services Bank on the Power of Cloud-Based Services,” Hewlett-Packard Development Company, L.P 2011-2012.

[15] IBM Corporation, “IBM Cloud Computing Architecture Some Selected Aspects,” North Castle, New York, United States, 2010.

[16] Ahmed E. Youssef and Manal Alageel, “A Framework for Secure Cloud Computing, field of Information Systems,” International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012.

[17] National Institute of Standards and Technology, NIST Cloud Computing Standards Roadmap Working Group, “NIST Cloud Computing Standards Roadmap,” NIST Special Publication 500-291, Version 2, U. S. Department of Commerce, July 2013.

[18] Bashar, Abul., "Modeling and Simulation Frameworks for Cloud Computing Environment: A Critical Evaluation, "Al-Khobar, Saudi Arabia, 2014.

[19] Bina Kotiyal, Priti Saxena, R. H. Goudar and Rashmi M. Jogdand, "A 5-Level Security Approach for Data Storage in Cloud, "International Journal of Computer Applications, 2012.

[20] Institute for Development and Research in Banking Technology, “Cloud Security Framework for Indian Banking Sector,” India, August 2013.

[21] Safiriyu Eludiora, Olatunde Abiona, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, and Lawrence Kehinde Eludiora, "A user Identity Management Protocol for Cloud Computing Paradigm," 2011.

[22] Maddineni, Venkata Sravan Kumar, and Shivashanker Ragi, "Security Techniques for Protecting Data in Cloud Computing," 2011.

[23] Camenisch, Jan L., Jean-Marc Piveteau, and Markus A. Stadler, "Security in Electronic Payment Systems," In: Proceedings of the ESO RISKS 94, 1994.

[24] Morse, Edward A. and Vasant Raval, "PCI DSS: Payment Card System Industry Data Security Standards in Context," Computer Law & Security Review 24.6: 540-554, 2008.

[25] Council, P. C. I., "PCI DSS Requirements and Security Assessment Procedures, Version 2.0.," 2010.

[26] Amziani, Mourad, Tarek Melliti, and Samir Tata, "A generic Framework for Service-based Business Process Elasticity in the Cloud," Business Process Management, Springer Berlin Heidelberg, 194-199, 2012.

[27] Pandith, Masrat Yousuf, "Data Security and Privacy Concerns in Cloud Computing," Internet of Things and Cloud Computing 2.2: 6, 2014.

[28] Andrei, Traian and Raj Jain, "Cloud Computing Challenges and Related Security Issues," A Survey Paper. DOI= http://www. cse. wustl. edu/~ jain/cse571-09/ftp/cloud. Pdf, 2009, Last Accessed on 14 May,2009 .

[29] European Central Bank, “Oversight Framework for Card Payment Schemes-Standards,” January, 2008.

[30] Maheshwari, Rohit and Sunil Pathak, "A Proposed Secure Framework for Safe Data Transmission in Private Cloud," International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, 2012.

[31] Matthew Haughn and Stan Gibilisco, “Confidentiality, Integrity, and Availability (CIA triad),”http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA, Last accessed on November, 2014.

[32] SO Kuyoro, "Cloud Computing Security Issues and Challenges," International Journal of Computer Networks 3.5, 2011.

[33] Lenka, Sudhansu Ranjan and Biswaranjan Nayak, "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm," International Journal of Computer Science Trends and Technology (IJCST)–Volume 2, 2014.

[34] V. Goyal, O. Pandey, A. Sahai and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89-98, 2006.

[35] Kawser Wazed Nafi1, Tonny Shekha Kar, Sayed Anisul Hoque and Dr. M. M. A Hashem, "A newer User Authentication, File Encryption and Distributed Server based Cloud Computing Security Architecture," 2013.

[36] Mahajan, Prerna and Abhishek Sachdeva, "A study of Encryption Algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology 13.15, 2013.

[37] Sachdev, Abha and Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm," International Journal of Computer Applications 67.9: 19-23, 2013.

[38] Shiralizadeh, Aysan, Abdulreza Hatamlou and Mohammad Masdari, "Presenting a New Data Security Solution in Cloud Computing," 2015.

[39] Singh, Sombir, Sunil K. Maakar and Dr Sudesh Kumar, "A Performance Analysis of DES and RSA Cryptography," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN: 2278-6856, 2013.

[40] Piyush Gupta and Sandeep Kumar, "A Comparative Analysis of SHA and MD5 Algorithm," International Journal of Computer Science and Information Technologies, Vol. 5 (3), 4492-4495, 2014.

[41] Sherwood John, Clark Andrew and Lynas David, “Systems and Business Security Architecture,” SABSA Limited, 17 September 2003.”

[42] John Sherwood, Andrew Clark, and David Lynas, “Enterprise Security Architecture,” SABSA, White paper, SABSA Limited, 1995-2009

[43] Ertaul, L., A. Movasseghi and S. Kumar, "Enterprise Security Planning with TOGAF-

9," Math & Computer Science, CSU East Bay, Hayward, CA, USA

[44] Rob van Os, “Comparing Security Architectures, Defining and Testing a Model for Evaluating and Categorizing Security,” 03 May 2014.

[45] The Open Group, “TOGAF Standard Courseware V9 Edition,” January 2009.

[46] Punithasurya, K. and S. Jeba Priya, "Analysis of Different Access Control Mechanism in Cloud," International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS 4.2, 2012.

[47] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, Cesar A. F. De Rose and Rajkumar Buyya, "CloudSim: a Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms," 2011.

[48] Rodrigo N. Calheiros, Rajiv Ranjan, César A. F. De Rose and Rajkumar Buyya, "Cloudsim: A novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services," 2009.

[49] Suryateja and Pericherla S., "A Comparative Analysis of Cloud Simulators,” International Journal of Modern Education and Computer Science (IJMECS) 8.4: 64, 2016.

[50] Malhotra, Rahul and Prince Jain, "Study and Comparison of Various Cloud Simulators Available in the Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering 3.9 :347-350, 2013.

[51] Kaur, Ramandeep and Navtej Singh Ghumman, "A Survey and Comparison of Various Cloud Simulators Available for Cloud Environment," International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015

[52] S.Rajesh, S.Swapna and P.Shylender Reddy, “Data as a Service (Daas) in Cloud Computing [Data-As-A-Service in the Age of Data],” Double Blind Peer Reviewed International Research Journal , USA, Volume 12 Issue 11 Version 1.0,2012.

[53] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, “New Comparative Study Between DES, 3DES and AES within Nine Factors,” Journal of Computing, Volume 2, Issue 3, ISSN 2151-9617, March, 2010.

Annex A: Interview Questions

Interview designed for Banks and Premier Switch Solution S.C. to gather information on the process of payment card system related to data security issues and cloud computing experiences.

Introductory question

- What is your name; would you please tell me your education level and work experience?
- What is your position in the organization?

Part 1:- For IT Managers

Policy question

- Is there any security policy, standard and guidelines that exist for the banking industry? If so, could you please tell me some of the guideline areas?
- Is there any security policy in your bank to secure its asset, application and data? If so, could you please mention some of them?
- Do you think a third party provider (PSS) held the same policies and standards with the banks?
- What is your opinion on policies and rules that should be added to secure the banking data more?

Managerial question

- Could you please tell the different services of the banking industry?
- Could you please tell me how much expense do you spent on the payment card system project and annual payment on rough estimation?
- What will be your opinion on the existing payment card system availability, quality of service, throughput and security?
- Do you believe that there is a proper protection of data and information for payment card data on the existing scenario?

- Could you please tell me your opinion on moving payment card system to the cloud computing platform?
- Do you think that the security of data will be affected when a payment card system move to the cloud computing platform?

General question

- Could you please tell me how many banks are in Ethiopia?
- Could you please tell how many of them are providing payment card service to their customers and how many of them are under the service of a third party?

Part 2:- For IT professionals and Premier Switch Solution (PSS) professionals

Security question

- Could you please tell me how many banks joined PSS?
- Do you believe that there is a proper protection of data and information for payment card system on current condition? If not, what are the security holes if it is not confidential?
- Is there any robust authentication technique for the payment card system? If so, could you please explain the authentication parameters? If not, why?
- Is there any access control mechanism enforced so far like session lock, remote access, wireless access, access control for mobile, concurrent session control, separation of duties and different privilege?
- Could you please tell me the encryption algorithm being used in the payment card system through the exchange of data b/n application if it is not confidential?

Technology questions

- Could you please tell me if you have any exposure on cloud computing? If so, can please tell me your experience?
- Did your organization adopt any kind of cloud technology? If so, would you tell us about the service?
- Is there any governmental problem that you know to adopt cloud in Ethiopia?

- Could you please tell me your opinion on adopting payment card system on the cloud?

  Assuming that we are about to adapt the payment card system to the cloud,
- What should be the cloud deployment model for payment card system from the security point of view?
- What kind of cloud services out of the three (SaaS, PaaS, IaaS) should be adopted for the payment card system?
- Could you please tell me your thoughts about cloud data security?
- Could you tell me about your expectation on data security aspects that should be addressed on cloud computing?

Annex B: Questionnaire for PSS Professionals

1. Respondent's Details

1.1. Education level

☐ BSc ☐ MSc ☐ PhD

1.2. Employment Position: _____

1.3. Work Experience: _____

☐ 1-2 years

☐ 3-4 years

☐ More than 4 years

2. ATM

2.1. Introduce what an ATM is and its main purpose?

_____

_____

_____

2.2. What is the unique nature of payment card transactions?

_____

_____

_____

3. Technology and infrastructure

3.1. What is database technology currently using for payment card system data management system?

☐ jBase ☐ oracle 11 g ☐ SQL Server

If it is out of the above, please specify_____

3.2. What is the OS technology currently using by payment card application and data servers?

☐ Linux ☐ Windows ☐ Netware

If it is out of the above, please specify_____

3.3. What are the different applications integrated to perform payment card operation? Select the applications from the list.

☐ Core banking system

☐ Payment switch solution

☐ ATM terminal application

If there is any other, please specify_____

3.4. How can core banking system, ATM terminals and payment switch solution communicate?

☐ DSL

☐ EPON

☐ GPON

☐ Wireless connection

☐ VPN

If there is any other, please specify_____

4. Security

4.1. Is there any data security policy enforced so far? If not, why?

☐ Yes ☐ No

_____

_____

4.2. What are the techniques to secure **data and information** in payment card system current environment?

☐ Encryption algorithm

If there is any other, please specify_____

4.3. What are the ways of ensuring availability of payment card system data?

☐ Solving software conflicts

☐ System upgrade

☐ Allocate adequate bandwidth

☐ Preventing bottlenecks

☐ Disaster recovery

☐ Redundancy, failover, RAID even high-availability clusters

If there is any other, please specify_____

4.4. How does the payment card system guarantee data confidentiality?

☐ Data encryption

☐ User IDs and passwords

☐ Two-factor authentication

☐ Biometric verification

☐ Security tokens

☐ Soft tokens

If there is any other, please specify_____

4.5. What are the ways that the payment card system used to ensure stored data integrity?

☐ Mirroring

☐ RAID Parity

☐ Check summing

☐ File permissions

☐ User access controls

☐ Version control

If there is any other, please specify_____

4.6. What are the techniques to secure **application and process** in the payment card system current environment?

☐ Cryptography

☐ Session lock

☐ Access control

If there is any other, please specify_____

4.7. Is there a way to secure **IT infrastructure** in the payment card system current practice?

☐ Yes ☐ No

4.8. Assess the list of security parameters according to the existing payment card system functionality.

	V.high	high	medium	low	V. low
Availability	☐	☐	☐	☐	☐
Through-put	☐	☐	☐	☐	☐
Quality of service	☐	☐	☐	☐	☐
Robust authentication	☐	☐	☐	☐	☐

4.9. What are the authentication parameters to identify a single customer?

- ☐ Customer ID
- ☐ Account No.
- ☐ PIN
- ☐ PAN Number

Please specify if there is any other parameter, _____

4.10. Is there any access control techniques implemented so far? If so, which of them are implemented from the list? If not why?

- ☐ Separation of Duties
- ☐ Least Privilege
- ☐ Unsuccessful Login Attempts
- ☐ System Use Notification
- ☐ Concurrent Session Control
- ☐ Session Lock
- ☐ Identification/ Authentication
- ☐ Remote Access
- ☐ Wireless Access
- ☐ Access Control for Mobile Device

Please specify if there are any access control techniques, _____

_____

_____

4.11. Is there any log file holding the transaction history on your side?

☐ Yes ☐ No

4.12. Is there any audit, operational?

☐ Yes ☐ No

4.13. Is there any risk assessment done so far?

☐ Yes ☐ No

4.14. Is there a security hole in the existing payment card system? If so, what are the security holes in the payment card system?

☐ Yes ☐ No

_____

_____

_____

_____

4.15. Is there any fraud attempt for the last three years on the payment card system practice? If there is, what are fraud attempt scenarios?

☐ Yes ☐ No

_____

_____

_____

_____

_____

4.16. If your answer is yes for the question 4.15, what are the solutions given to the fraud attempts and what would you recommend for securing it more?

_____

_____

_____

_____

4.1.7. If possible, sketch the process of a single payment execution in the payment card system?

5. Cloud computing practice

5.1. Do you know about cloud computing technology?

☐ Yes ☐ No

5.2. Does your company have a plan to host its services in the cloud?

☐ Yes ☐ No

5.3. If your answer is yes for the question 5.2, what is your opinion if the payment card system adopts to move to the cloud? If no, why not?

_____

_____

_____

_____

Annex C: Questionnaire for IT Professionals

1. Respondent's Details

1.1. Education level

☐ BSc ☐ MSc ☐ PhD

1.2. Employment Position: _____

1.3. Work Experience: _____

☐ 1-2 years

☐ 3-4 years

☐ More than 4 years

2. Payment card system data security

2.1. Is there any payment card system facility in your bank?

☐ Yes ☐ No

If the answer for the question 2.1 is yes, proceed to the next question. If not, go to part 3.

2.1.1. what type of data exist on the bank side?

☐ History file

☐ Log file

☐ Transaction data

If there is any other, please specify_____

2.1.2. What is the means of communication in a WAN technology between the bank and the payment switch solution to perform the payment card system operation?

☐ DSL

☐ EPON

☐ GPON

☐ Wireless connection

☐ VPN

If there is any other, please specify_____

2.1.3. Is there any data security policy in the bank side? If not, why?

☐ Yes ☐ No

_____

_____

_____

2.1.4. Is there any security hole in payment card system? If so, please state the major holes.

☐ Yes ☐ No

_____

_____

_____

2.1.5. Assess the list of security parameters according to the existing payment card system functionality.

	V.high	high	medium	low	V. low
Availability	☐	☐	☐	☐	☐
Through-put	☐	☐	☐	☐	☐
Quality of service	☐	☐	☐	☐	☐
Robust authentication	☐	☐	☐	☐	☐

3. Cloud computing practice

3.1. Is there any banking module in a cloud environment in your bank?

☐ Yes ☐ No

If the answer for the question 3.1 is yes,

3.1.1. What is the name of the application?

☐ Retail ☐ Credit ☐ IBD ☐ Swift

☐ Payment card ☐ Mobile banking

If there is any other, please specify_____

3.1.2. What kind of cloud service is that the bank using out of the different cloud computing services? Select the specific service from the list.

- ☐ Software as a Service (SaaS)
- ☐ Platform as a Service (PaaS)
- ☐ Infrastructure as a Service (IaaS)

3.1.3. What about the deployment mode? Select the specific mode from the list.

- ☐ Public cloud
- ☐ Private cloud
- ☐ Hybrid cloud
- ☐ Community cloud

3.1.4. What are the security techniques that the cloud providers are currently using for the specified banking module?

- ☐ Access policies
- ☐ Access control techniques
- ☐ Cryptography
- ☐ Data lockdown
- ☐ Data categorization and the use of data labels
- ☐ Encryption

If there is any other, please specify_____

3.1.5. Do you think there is some security hole in their service? If so, please state the major holes.

_____

_____

_____

3.1.6. If there is a security hole, what would you recommend to be more secure?

_____

_____

_____

3.1.7. What are the benefits that the bank incurs due to the existing cloud service?

- ☐ Backup
- ☐ Big data analytics
- ☐ Disaster recovery
- ☐ File storage
- ☐ Infrastructure as a service (IaaS)
- ☐ Platform as a service (PaaS)
- ☐ Software as a service (SaaS)
- ☐ Test and development

If there is any other, please specify_____

Declaration

I, the undersigned, declare that this thesis is my original work and has not been presented for a degree in any other university, and that all source of materials used for the thesis have been duly acknowledged.

Declared by:

Name: Edil Endalew

Signature: _____

Date: _____

Confirmed by advisor:

Name: _____

Signature: _____

Date: _____