Enhancing User Authentication Framework in Cloud Computing by Using Mobile Phone

"Master Thesis"

By
Ahmad Mohammad Alrefai

Supervisor
Dr. Khaldoun Batiha

This Thesis was submitted in Partial Fulfillment of the Requirements for the Master's Degree in Computer Science

Deanship of Academic Research and Graduate Studies
Philadelphia University

January, 2019

جامعة فيلادلفيا
نموذج التفويض

أنا أحمد محمد حسن الرفاعي ، أفوض جامعة فيلادلفيا بتزويد نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الأشخاص عند طلبها.

التوقيع:
التاريخ:

Philadelphia University
Authorization Form

I, Ahmad Mohammad Hasan Alrefai , authorize Philadelphia University to supply copies of my Thesis to libraries or establishments or individuals upon request.

Signature:
Date:

Enhancing User Authentication Framework in Cloud Computing by Using Mobile Phone

By

Ahmad Mohammad Alrefai

Supervisor

Dr. Khaldoun Batiha

This Thesis was Submitted in Partial Fulfillment of the Requirements for the Master's Degree In Computer Science.

Deanship of academic Research and Graduate Studies

Philadelphia University

January , 2019

Committee Decision

Successfully defended and approved on ----------

Examination Committee	**Signature**
Dr.,……., Chairman Academic Rank: ……	----------
Dr. ……, member. Academic Rank: ……	----------
Dr. ……, member. Academic Rank: ……	----------
Dr. …….. , External Member. Academic Rank: ……	----------

(Name of University)

DEDICATION

I dedicate this work to my parents, beloved family and my friends.

ACKNOWLEDGEMENT

After thanking ALLAH the almighty, and our prophet Mohammad, peace be upon him, I would like to express my great thank to Philadelphia University, and the workers there for their help and cooperation to fulfill this study.

I would like to express my great thanks and appreciation to the supervisor of my study. Dr. Khaldoun Batiha, for his continuous support and encouragement, and for giving me a lot of his time and effort to complete this work.

Also, I would like to thank my parents and family for their continuous help and support that motivate me a lot to achieve this study.

Last, my great thanks for my friends who stood beside me to accomplish this study.

Table Of Contents

Subject	Page
Committee Decision	IV
Dedication	V
Acknowledgement	VI
Table Of Contents	VII
List of Tables	IX
List of Figures	X
List of Abbreviation	XI
Abstract	XII
CHAPTER ONE INRODUCTION	1
1.1 Introduction	2
1.2 Research Context	3
1.3 Problem Statement	3
1.4 Motivation	4
1.5 Research Methodology	4
1.6 Thesis Contribution	6
1.7 Thesis Layout	6
CHAPTER TWO BACKGROUND	7
2.1 Introduction	8
2.2 Cloud Technology	8
2.3 Authentication	10
2.4 Framework	10
2.5 Remote Authentication	11
2.6 Mutual Authentication	11
2.7 QR Code	12
2.8 CAPTCHA	13
2.9 Session Transferring	13
CHAPTER THREE LITRITURE REVIEW	14
3.1 Introduction	15
3.2 The Base of User Authentication Framework in Cloud Computing	15
3.3 Authentication on Mobile Cloud Computing	17
3.4 Mutual Authentication	17
3.5 Remote Authentication	18
3.6 Defense Against DoS Framework	18

3.7 Other Recently Framework	18
3.8 Conclusion	19
CHAPTER FOUR ENHANCED USER AUTHENTICATION FRAMEWORK	20
4.1 Introduction	21
4.2. Enhanced User Authentication Framework	21
4.2.1. Registration Phase	23
4.2.2. Login & Authentication Phase	25
4.2.3. Service Access Authentication Phase (SAAP)	29
4.2.4. Change The Password Activity	32
4.3. The Defense against SYN Flood Attack	32
CHAPTER FIVE EVALUATION AND SECURITY ANALISIS	36
5.1 Introduction	37
5.2 Security Analyses	37
5.2.1. Functionality Requirements	37
5.2.2. Security Requirements	39
5.3. Comparative analyses between different frameworks	41
CHAPTER SIX CONCLUSION AND FUTURE WORK	43
6.1 Conclusion	44
6.2 Future Work	44
REFERENCES	45
الملخص	50

List of Tables

Table Number	Table Title	Page
3.1	**Previous Work Comparison**	19
4.1	**Description of Notation Used in This Thesis**	22
5.1	**Comparative Analyses Based on Functionality Requirement**	41
5.2	**Comparative Analyses Based on Security Requirements**	42

List of Figures

Figure Number	Figure Title	Page
Figure 1.1	Research Methodology	5
Figure 2.1	Cloud Computing Layers	9
Figure 2.2	Cloud Computing Types	9
Figure 2.3	Conceptual Framework Stepwise	10
Figure 2.4	Remote Authentication Vie Fingerprint	11
Figure 2.5	Encoding and Decoding QR Code	12
Figure 2.6	CAPTCHA Example	13
Figure 3.1	Choundhuey et al Authentication Protocol	15
Figure 4.1	Registration Phase Sequence Diagram	24
Figure 4.2	Login & Authentication Phase Terminal Scenario	26
Figure 4.3	Login & Authentication Phase Mobile Scenario	28
Figure 4.4	SAAP Terminal Scenario	30
Figure 4.5	SAAP Mobile Scenario	31
Figure 4.6	Change the Password Flow	32
Figure 4.7	TCP Three Way Handshake Protocol	33
Figure 4.8	SYN Flood Attack	34
Figure 4.9	SAAP Against SYN Flood Attack	34

List Of Abbreviations

Acronym	Meaning
ACK	Acknowledgement
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Humans Apart
DoS	Denial of Service
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
QR Code	Quick Response Code
SAAP	Service Access Authentication Phase
SaaS	Software as a Service
SYN	Synchronize

Enhancing User Authentication Framework in Cloud Computing

Abstract

Cloud computing is a modern technology that refers to handling, configuring and accessing several applications online. Cloud computing provides data storage, infrastructure and application. As well as it is a combination that based on both software and hardware computing resources provided as network services. As new technology there are a lot of threats surrounding cloud computing, such as data integrity, data confidentiality, access control and user authentication that are considered as the most popular security issues in cloud computing.

Recently, There are lot of research works that proposed a user authentication frameworks, in order to defense against several types of attack such as: replay attack, man in the middle attack, denial of service attack, etc. Most of the previous frameworks consist of three main phases which are registration phase, login phase and authentication phase, where most of them use additional activity which is changing the password. Unfortunately the previously proposed frameworks still suffer from many problems such as security weakness in the registration phase, there is no way to deal with internal attack such as SYN flood attack.

In this research work we propose a strong user authentication framework, that overcomes the previous framework shortages. The proposed framework is supported by many security properties such as remote authentication, mutual authentication, session key establishment, etc. In addition to enhanced registration phase, login phase and authentication phases, we added a Service Access Authentication Phase (SAAP), where according to this phase, internal verification will be imposed.

At the end of this research work, we will do a security analysis that justify how the introduced framework defense against several types of attacks, then we present a comparison that shows how is the introduced framework overcomes the mentioned problems in the previous frameworks.

Chapter One:

INTRODUCTION

1.1.Introduction

Cloud computing has many strengths, but it still contains some issues, such as resiliency, performance, interoperability, transition from legacy systems and data migration. Security is considered one of the most issues that was discussed in the last few years (Sharma, S. et al, 2012).

Cloud computing as a modern technology still suffering from many security threats, where the highest impact threat is authentication break through. User authentication is one of the most sensitive security issues in cloud computing environments, because if unauthorized user accesses the cloud server, he/she can cause significant damage to the data and services provided by the server.

To overcome authentication threat, there are a lot of research works that covered the issue of user authentication under the concept framework, which denote to a multi phases approach that used to solved a specific problem (Gao, Y. et al, 2017). The first user authentication framework is proposed by Choudhury (Choudhury, A. J. et al, 2011), where there is a lot of enhancement applied on their approach by (Chen, N., & Jiang, R. 2013), (Jiang, R., 2013), (Chen, N., & Jiang, R., 2014), (Patel, S. C. et al, 2015), (Mun, J. et al, 2016). However their work stayed have some shortages.

In this research work, we analyzed the previous frameworks, in order to fill their shortages. Then we study a modern and robust security concept such as fingerprint, Quick Access Code (QR Code), Completely Automated Public Turing Test to tell Computers and Humans Apart (CAPTCHA) and other technique, to produce a novel framework that authenticates user before access the cloud server by the local system authentication, in addition to use fingerprint as a second security factor under the concept mutual authentication. We have configured the framework to ensure that the cloud is not vulnerable to denial of service (DoS) attack, both external and internal attacks. The framework consists of four main phases, and one activity. which is registration phase, login phase, authentication phase, service access authentication phase

and change the password or fingerprint activity, where each phase will be explain in chapter four.

1.2. Research Context

In this research work, we are moving to improve the security of cloud computing, especially in the area of user authentication. There is a subsequence research work present a strong user authentication framework to defense against several types of user authentication threats in cloud computing.

Their primary goal is to ensure user authentication before accessing the cloud server.
The objective of this research work is to analyze the detected problem in (Choudhury et al, 2011) framework and the subsequence framework that come after them, then we propose a novel framework that overcome the problems of the studied frameworks. In addition, we have given attention to the defense against DoS attacks, because this attack causes a lot of damage on the level of resources and the network, as we aimed to clear each stage in the proposed framework to ensure that this attack will not occur.

1.3.Problem Statement

There are lots of research works that handle user authentication threats in cloud computing area. Where there is a subsequence research work that handle user authentication under the concept framework ((Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016)). They argue that their works are proved to defend against several types of attacks such as Denial of Service (DoS) attacks. Furthermore, they argue that their work prevent any external attack (Attacks before logged to the cloud system) through remote authentication(ensure user authentication before access the server) and mutual authentication (using additional security factor such as smartcard). However, their framework (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016) still suffered from several shortages such as :

1- There is no control over user behavior after logged to the cloud system, where there are many attacks that can occur internally(Attacks after logged to the system) such as internal DoS attack.

2- There is no protection technique includes registration phase, where they assume all of client and server are honest on this phase, which reflects an unrealistic hypothesis.

3- For the registration and login phases, the cloud service provider and cloud user need to have a smartcard reader to prepare and read the released smartcard. So for service provider and the cloud user they are required to have extra device which is smartcard reader, which is unpopular recently (Darwish, M., Ouda, A., & Capretz, L. F. 2015).

1.4.Motivation

Recently, there are many research studies on user authentication framework in cloud computing such as ((Choudhury, A. J. et al 2011), (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016)). But they were discussing how to protect the server from external attack. In addition, they did not take into account the defense against DoS attack in particular case. We can say that DoS is one of the most frequencies attack that may face the cloud systems (Somani, G. et al. 2017), specially it may threat the reliability, availability and performance of cloud computing. Defending cloud systems against the DoS attack is considered as an important research issue, the aim of defense is to avoid the heavy resource usage, which cause financial loss.

1.5.Research Methodology

The research methodology of this work is summarized by the following steps and shown in figure 1.1:

1. Analyzing previous frameworks (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016). specifically analyzing DoS attack in the previous frameworks (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016).

2. Studying different techniques and methods that can be used to optimize the previous frameworks (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016). Such as finger print, CAPTCH recognition and QR code.
3. Proposed enhanced framework including these techniques.
4. Analyzing the proposed framework and proving that it is more secure than other frameworks (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016) by prepare comparison with others frameworks and security analyses.

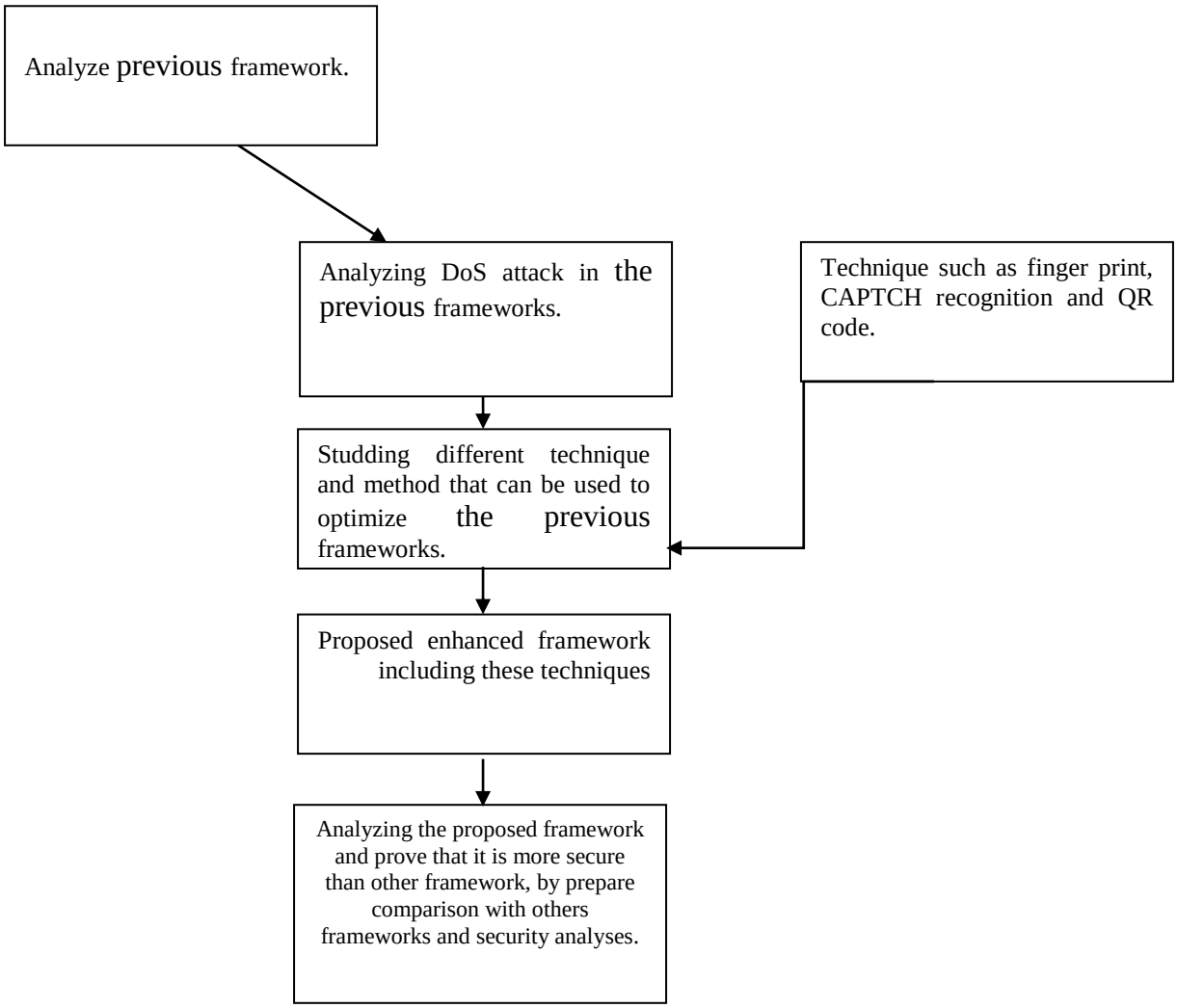

Figure 1.1: Research Methodology

1.6.Thesis Contribution

As denote in the problem statement section, (Chondhury et al, 2011) framework and the subsequence frameworks (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016) have many shortages, in our work we try to overcome these shortages and produce a strong and modern user authentication framework. Where the main factor in the proposed framework is user mobile phone, the proposed frame work guarantee user authentication before access the cloud server, and support many security technologies such as remote authentication, mutual authentication, QR code, CAPTCHA and finger print scanning. The proposed framework consists of four phases and one activity, which is registration phase, login phase, authentication phase, service authentication and change the password or fingerprint activity.

1.7.Thesis Layout

Thesis organized as follow:

Chapter Two Presents a definition of the main concept that used in this work.

Chapter Three Introduces the previous work that handle user authentication threat and DoS attack.

Chapter four Reflects the contribution of this thesis, which is an enhanced user authentication framework based on mobile phone.

Chapter Five Presents thesis evaluation and security analysis.

Chapter six Denotes thesis conclusion, which is a summarization of the main idea in this work, in addition to the future work that may include this work.

Chapter Two:

BACKGROUND

2.1. Introduction

This chapter clarifies the main concept that introduced in this research work, which is around user authentication framework in cloud computing.

2.2. Cloud Technology

Cloud computing denote that, make the services to be such as application that delivered through internet, in addition, cloud provides the required resources to execute, these services such as network infrastructure and system software (Fox. A. et al 2009). Thus, cloud can be characterized as an arrangement of storages, services and interfaces that are given by servers. Cloud computing is currently playing an important position in the field of information technology, where the results of Rackspace survey in 2016 show that (95%) of organizations use cloud computing (Weins, K. 2017).Cloud computing model includes three main layers (figure 2.1), which is software as a service (SaaS) , platform as a service (PaaS) and infrastructure as a services (IaaS) (Zhang, Q. et al 2010). SaaS indicates on demand application providing cross the internet. Examples of SaaS providers include Rackspace.com, Salesforce.com and salesforce.com. PaaS indicates to providing system application or platform, such as software development framework and operating system support. Example of PaaS layer includes Microsoft Windows Azure (www.microsoft.com/azure), Google App Engine (code.google.com/appengine) and Force.com . IaaS indicates to provide hardware and software as resources to deliver services, Example of IaaS layer gogrid.com, aws.amazon.com and flexiscale.com.

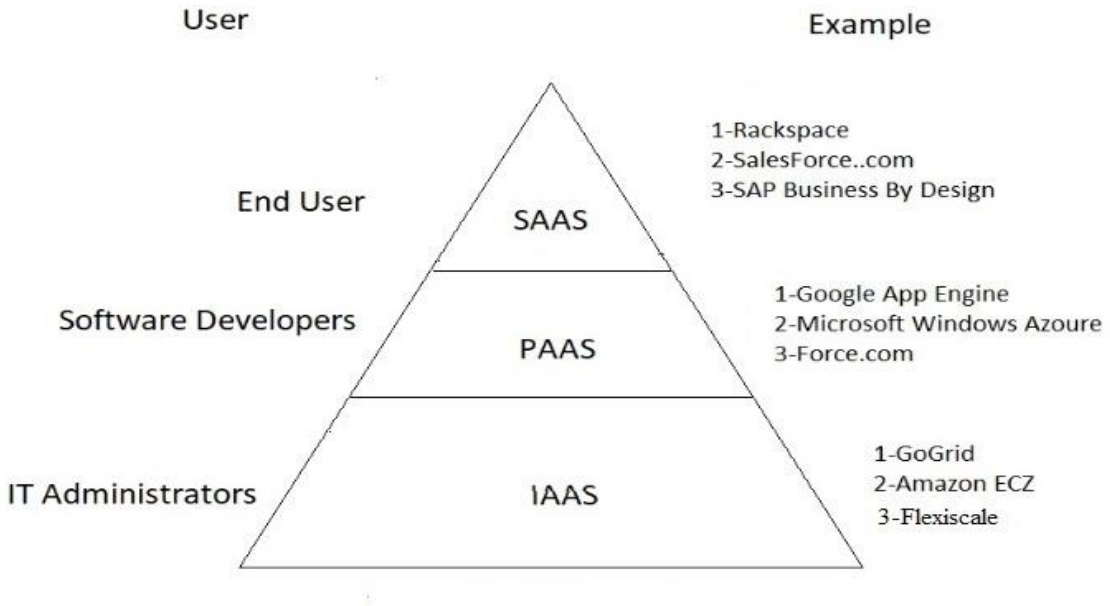

Figure 2.1: Cloud Computing Layers

There are three main types of cloud named as private cloud, public cloud and hybrid cloud (Fox. A. et al 2009) (figure 2.2),where the difference between public and private cloud is shown by services accessibility, network accessibility, security and confidentiality of information, where private cloud requires a lot of user restrictions to use. Hybrid cloud reflects a bridge between private and public cloud.

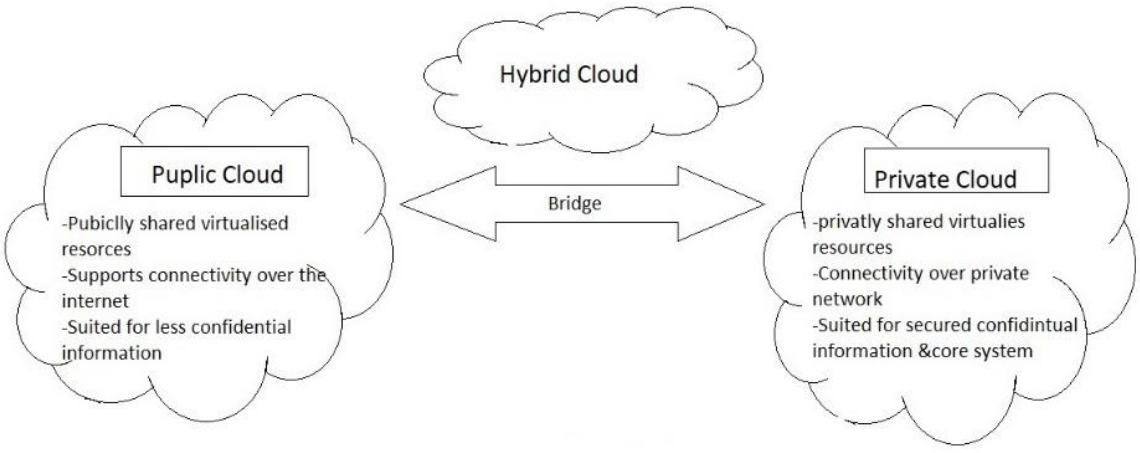

Figure 2.2: Cloud Computing Types

2.3. Authentication

The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

2.4. Framework

Framework denotes that the structure or skeleton that provides a solutions to specific phenomenon problems (Birkmann, J. 2006).There are two types of frameworks (Adom, D. et al. 2018), which are theoretical and conceptual framework. Theoretical framework represents a plan or guide for research based on existing theory, where the main objective of this type of framework is to organize the path of the research. Conceptual framework explains the progress of solving the problems of phenomenon under study problems (figure 2.3), by using several concepts or approaches.

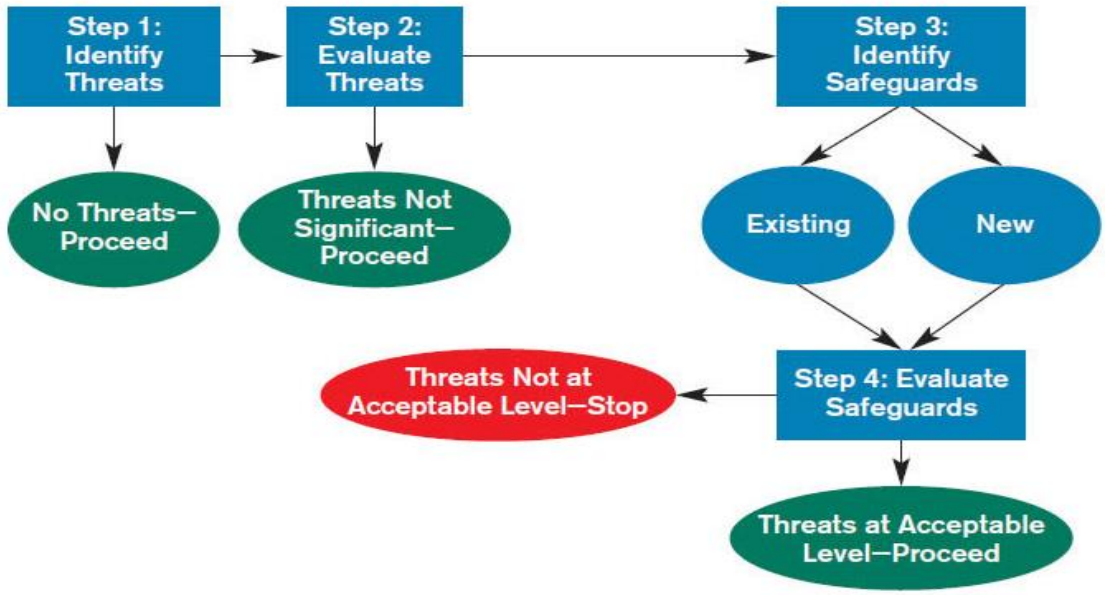

Figure 2.3: Conceptual Framework Stepwise

According to conceptual framework, the process start when there is a threats in a specific phenomenon (step 1 figure 2.3), then the threat will be evaluated and find out the appropriate safeguards to overcome this threats (step 2 and 3 figure 2.3) finally the proposed solution will be evaluated. In this research work we used a conceptual framework in order to immunization the cloud computing environment, were the presented framework included several concepts to enhance user authentication property in cloud computing such as, remote authentication, mutual authentication, Identity management etc.

2.5. Remote Authentication

Remote authentication technique is used to give a specific access to legitimate users through remote access, where authentication grants to users before access the server. The remote authentication scheme is most acceptable, simple and widely adopted mechanism because of its low cost (Doshi, N., & Patel, C. 2018).

Figure 2.4 explains how remote authentication technique accomplished through local authentication via fingerprint (Boyen, X. 2005) (fingerprint as an example).

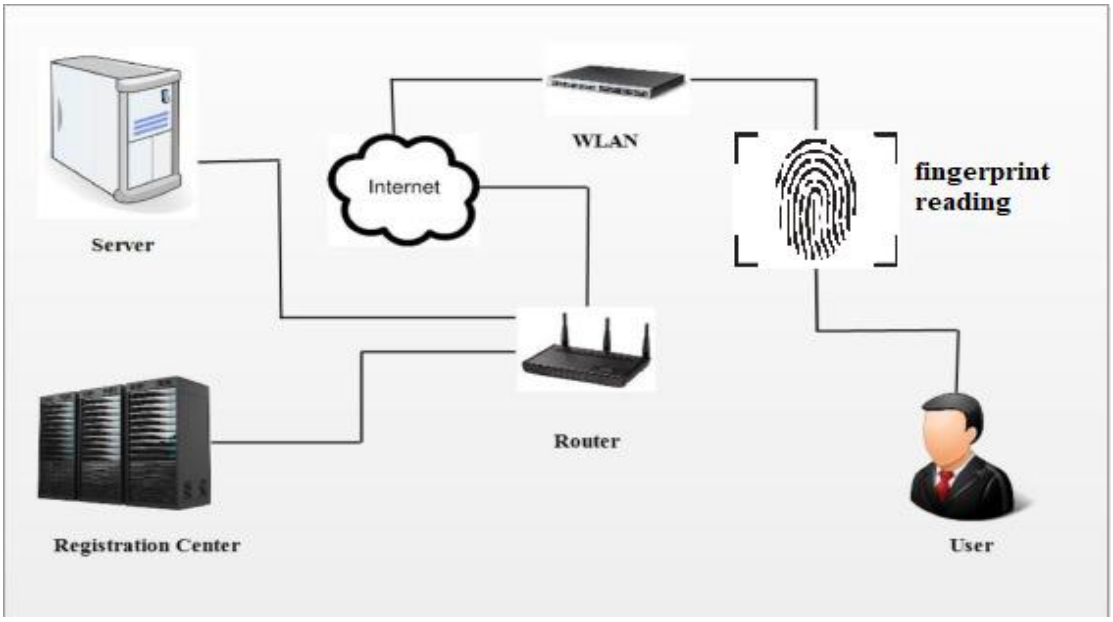

Figure 2.4: Remote Authentication Via Fingerprint

2.6. Mutual Authentication

Also called two way authentication, is a technique in which both sides (user and server) in a specific communication channel authenticate each other, where the user authenticates the server and vice-versa (Chien, H. Y., & Chen, C. H. 2007). In order to enhance the mutual authentication technique, (Yang et al. 2008) propose a new mutual authentication scheme where users authenticate their self through extra authentication factor, such as smartcard, bio factor, specific software, etc. in addition to the password which makes it hard to be hacked.

2.7. QR Code

QR code is a two dimensional barcode, which presented by Japanese company (Denso-Wave) in 1994. The QR code contains encrypted information in both vertical and horizontal dimensions (Liao, K. C., & Lee, W. H. 2010). Figure 2.5 explains how to decoding and encoding QR code via mobile phone.

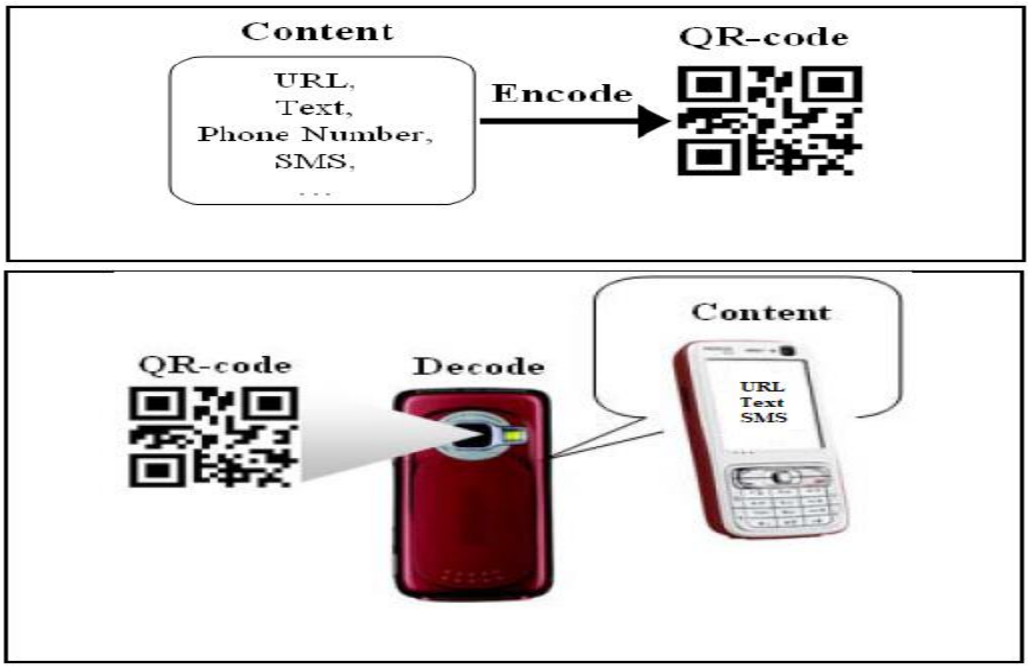

Figure 2.5:Encoding and Decoding QR Code

Recently, QR code is used to link something physical to digital word, not just a physical object, it can be used to transfer data, identifier and session(Vazquez-Briseno, M. et ak 2012) such as web.whatsApp.com.

2.8. CAPTCHA

CAPTCHA is an acronym for Completely Automated Public Turning Test to tell Computers and Humans Apart (Lee, W. B. et al. 2012). It is a protection technique from these malicious applications like Bot. There are many CAPTCHA types such as CAPTCHAs based on text, CAPTCHAs based on image, CAPTCHAs based on audio ect. (Singh, V. P., & Pal, P. 2014). The behavior of CAPTCHA is based on sending a specific image, text, audio, ect. and ask user to recognize and resend it. Figure 2.6 explains an example of image and audio CAPTCHA.

Figure 2.6: CAPTCHA Example

2.9. Session Transferring

There are a lot of Google patents in this topic (McDonough. et al 2010), (Ashley, Paul A. et al 2017), (Zawacki. et al 2017), where there is several models introduced. The most popular model is based on moving the session as a service, through on demand model (McDonough. et al 2010). Where the server manages the transferring path (source and distention of the transferring process).

Chapter Three:

LITERATURE REVIEW

3.1 Introduction

Our research work will be mainly based on sequence of research works (Choudhury, A. J. et al 2011), (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016) that handles user authentication under the concept framework, where the authors present a framework for a strong user authentication protection against several types of attack like DoS attack, Replay attack, Man in the middle attack, Insider attack, etc. In this chapter, we review the most related previous work under the concept framework and discuss their shortages.

3.2. The Base of User Authentication Framework in Cloud Computing

Choundhuey et al (Choudhury, A. J. et al 2011) propose the first user authentication framework, where the framework ensures user authentication before access cloud server, by two-steps verification based on password smartcard and out of bond (i.e. strong two factor) authentication, also they provide identity management, user privacy, session key establish and mutual authentication.

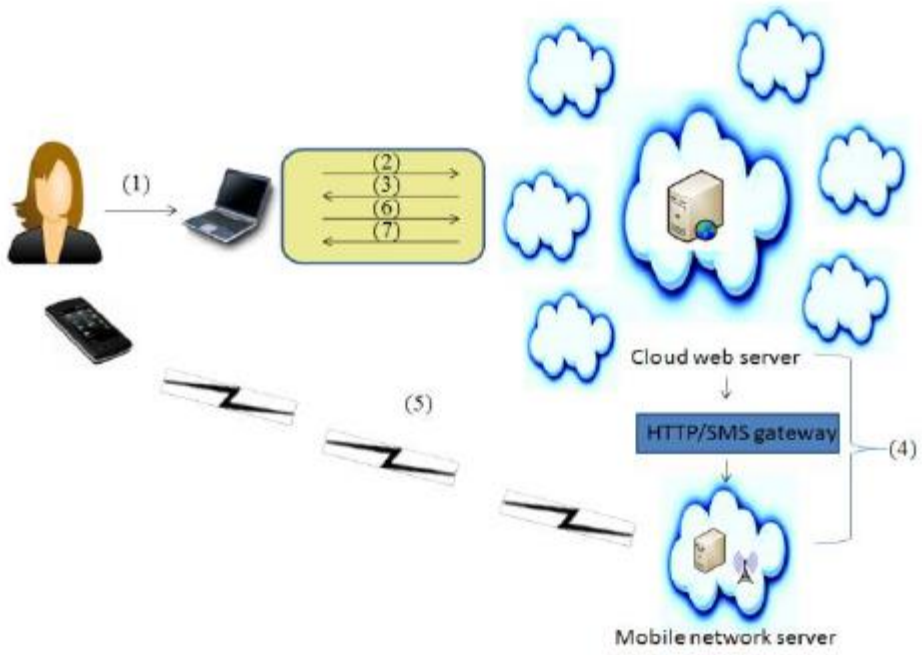

Figure 3.1: Choundhuey et al Authentication Protocol

As shown in the figure 3.1the basic idea of (Choundhuey et al, 2011) framework is as follows.

1. The user logged in by insert smart card and enter user Identification (ID) and password(PW). The local system checks user legitimacy based on smartcard, ID and PW.
2. When the user is verified in local system, login request released to the cloud server.
3. According to receiving the login request, authentication data will be released by cloud server based on the specific user.
4. The cloud server sends to mobile network the onetime key, through HTTP/SMS gateway.
5.Via SMS the mobile network will send the onetime key to the user.
6. The user trusts and authenticates the server and sends conformation message according to smartcard, ID and onetime key.
7. The server authenticates user based on data sent by the user in step 6.

There are a lot of research works that came after Choundhuey et al work, aimed to analyze and prove Chondhury framework, Rui Jiang in (Jiang, R. 2013) claimed that Chondhury framework suffers from weakness in facing some of attacks, such as the OOB (Out Of Bond) attack, the masquerading attack and the password change flaw, where this weakness appears after analyzing Chondhury framework. So they proposed an advance user authentication framework based on remote authentication schemes and apply two factor authentication technology in order to overcome above security shortages.

Chen and Jiang (2013), analyzed Chondhury framework and claimed that there were some weaknesses in it .So, they made some improvements on them by taking in account cryptographic standard in order to enhance the communication security between user and cloud server. Chen and Jiang also present an extended security analysis.

Chen and Jiang(2014), enhanced Chondhury framework and proved formally the mutual authentication of their protocol by using of space model theory and the authentication test tools, in addition to that they made performance simulation to prove their works.

Mun, Kim and Won (2016), claimed that Chondhury framework and the research works come after still suffer from weaknesses in defense against some of attacks such as server impersonation attack, outsider attack, off-line password guessing attack and smart card stolen attack, in addition to that there were no mechanism to detect the password correctly . So, they built a secure and robust framework by using remote user authentication scheme.

3.3 Authentication on Mobile Cloud Computing

Hasan, M., Riaz. et al (2017) propose a multi technique model to ensure user authentication, while he is moving between cloud and mobile cloud computing. Where they use several authentication approaches such as device based approach, image and biometric based, token based approach and text based approach. Where the proposed model chooses the best approach to use according to user device capabilities. Hasan, M. et al, (Birkmann, J. 2006) does not introduce the stage of user registration, where there is no verification on the registered users.

Tsai, J. L., & Lo, N. W.(2015) proposed a privacy aware authentication scheme that ensures user authentication through distributed mobile cloud system. The proposed scheme built under the dynamic nonce generation and bilinearpairing cryptosystem protocols. They argue that their scheme allow user to access several mobile cloud services from several cloud providers by using one private key, by using robust smart card generator. The proposed scheme supports key exchange, mutual authentication, user intractability and user anonymity.

3.4 Mutual Authentication

\Huszti, A and Ol´ah, N. (2016) present an authentication scheme that based on two-security factors, which are password and smartcard. They seek through using mutual authentication to protect the cloud server from the insider attack. Merkle tree used to hash user password when it was shared.

Nayak, S. K. et al (2012) propose mutual authentication framework, based on user ID, password and user E-mail. The framework consists of three phases which are initialization phase, registration phase and authentication phase. Through the authentication phase, user sends his password and ID to the server, then the server will send a token to the used E-mail, and ask user to enter the value of the token, in addition they introduce the flexibility of change the password activity and the session agreement between user and server.

3.5 Remote Authentication

Roy, S. et al (2014) build a mobile cloud computing framework based on lightweight remote authentication scheme. They used several techniques to ensure user authentication such as bitwise XOR, cryptographic hash and fuzzy extractor functions. User authentication grunted remotely before access the cloud server through authenticates the user on the level of network operator, then the request will be sent through the internet to the cloud service provider. They take in their account the resource constrained on user mobile deviceand design the framework to be such that a lightweight scheme.

3.6 Defense Against DoS Framework

Darwish, M. et al, (2015) propose an adaption framework to defense against DoS attack. The proposed framework consists of three phases, which are registration phase, adaptive DoS defender protocol and authentication phase. Where they argue that using a complex model or scheme could exhaust the cloud's resources and can cause a weakness in defense against a DOS attack. They used cost-based model approach to calculate each arrived request values then detect the malicious requests.

3.7 Other Recently Framework

Chang, V. et al. (2016) propose an adaption framework to defense against Viruses and Trojans threat, in addition to deal with SQL injection through intrusion prevention system. They use a multi layered framework that consists of three layers, which are identity management layer, firewall layer and encryption.

Al-Attab, B. S., & Fadewar, H. S. (2016) proposed an authentication framework that can handle several types of attacks such as denial of service (DOS), password guessing, replay , man-in-the -middle ,insider and so on. They argue that their framework built under coherent techniques such as hash function, USB token and Diffie-Hellman. The proposed framework consists of three phases, which are registration phase, login phase and authentication phase and two activity which are USB token backup and change of password.

Kai, F. et al, (2018) propose a mutual authentication scheme based on smartcard and hash function. The scheme analyze Singhal et al.'s Scheme (2015) and prove that their work vulnerable to offline password guessing attack and lost smartcard attack, so Kai, F. et al proposed an enhanced scheme to overcome this threats. The Scheme consist of three phases which are registration phase, login phase and mutual authentication phase.

3.8 Conclusion

There is a sequence of research work that handle user authentication threat under the concept framework. In this chapter, we introduce and analyze the previous research work contribution, and the incorrectness that their work suffered from it (Table 3.1).

Table 3.1 : Previous Work Comparison

Research work	Criteria		
	Used bio factor	Registration phase refinement	Internal attack detection
(Choundhuey et al 2011)	X	X	X
(Jiang, R. 2013)	X	✓	X
(Chen, N., & Jiang, R. 2014)	X	✓	X
(Mun, J. et al 2016)	X	X	✓
(Kim and Won 2016)	X	✓	X
(Andrea and Norbert 2016)	X	✓	✓
(Hasan, M. et al, 2017)	✓	X	✓
(Roy, S. et al, 2017)	✓	✓	X
(Darwish, M. et al, 2015)	X	✓	✓
(Kai, F. et al, 2018)	X	✓	X
Our Framework	✓	✓	✓

Chapter Four

ENHANCED USER AUTHENTICATION FRAMEWORK

4.1. Introduction

In this research work we built a strong user authentication framework to defend against several types of attacks, in particular the defense against DoS attack. The framework is built based on remote authentication technique, where user must identify himself before access the cloud server. In addition to use two factors to authenticate users which are user password and user fingerprint.

4.2. Enhanced User Authentication Framework

The presented framework is built on the base of subsequence researches (Choudhury, A. J. et al 2011), (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016), that handle the threat of user authentication property in cloud environment. The framework consists of four main phases and one activity, which are: (the notations used in this research work are mentioned below in (Table 4.1)

TABLE 4.1 : DESCRIPTION OF NOTATIONS USED IN THIS THESIS

Notation	Description
A	Denote a specific user
a	Denote user basic information
b	Denote Server authentication information
C	Denote CAPTCHA text
FP	Denote finger print
h(.)	Denote to hash function
ID	Denote user identity
k	Denote onetime shared key between user and server
LA	Denote to local authentication process
M	Denote mobile phone
PW	Denote user password
Q	Denote QR code
R(FP)	Denote Read fingerprint
S	Denote cloud server
SA	Denote to server authentication process
SE	Denote a specific session
Si	Denote Service identifier
T	Denote terminal (desktop, laptop)
t	Denote time stamp

4.2.1. Registration Phase

In the registration phase, user needs to register at the server by providing appropriate identification data such as ID,PW and FP. The server process user's data and store it, then send them to local system (Mobile phone). Where the registration phase occurs though two steps, the first step will be accomplished on user terminal (Desktop, Laptop) to insert user basic information such as first name, last name, E-mail ..etc. and CAPTCHA recognition, then second step will be accomplished on user mobile phone, where through mobile phone, user will insert his fingerprint, password and ID, where the session will be transferred from user terminal to the mobile phone. Server provides the terminal by QR code where the terminal asks user to read QR code through his mobile to move the session to his mobile phone.

The presumptions on this phase is:

A: The user has a mobile phone that supports fingerprint reading.

B: This phase required two devices to be submitted, which are mobile phone and terminal, so user must have them.

The procedure of this phase is as follows (Figure 4.1) :

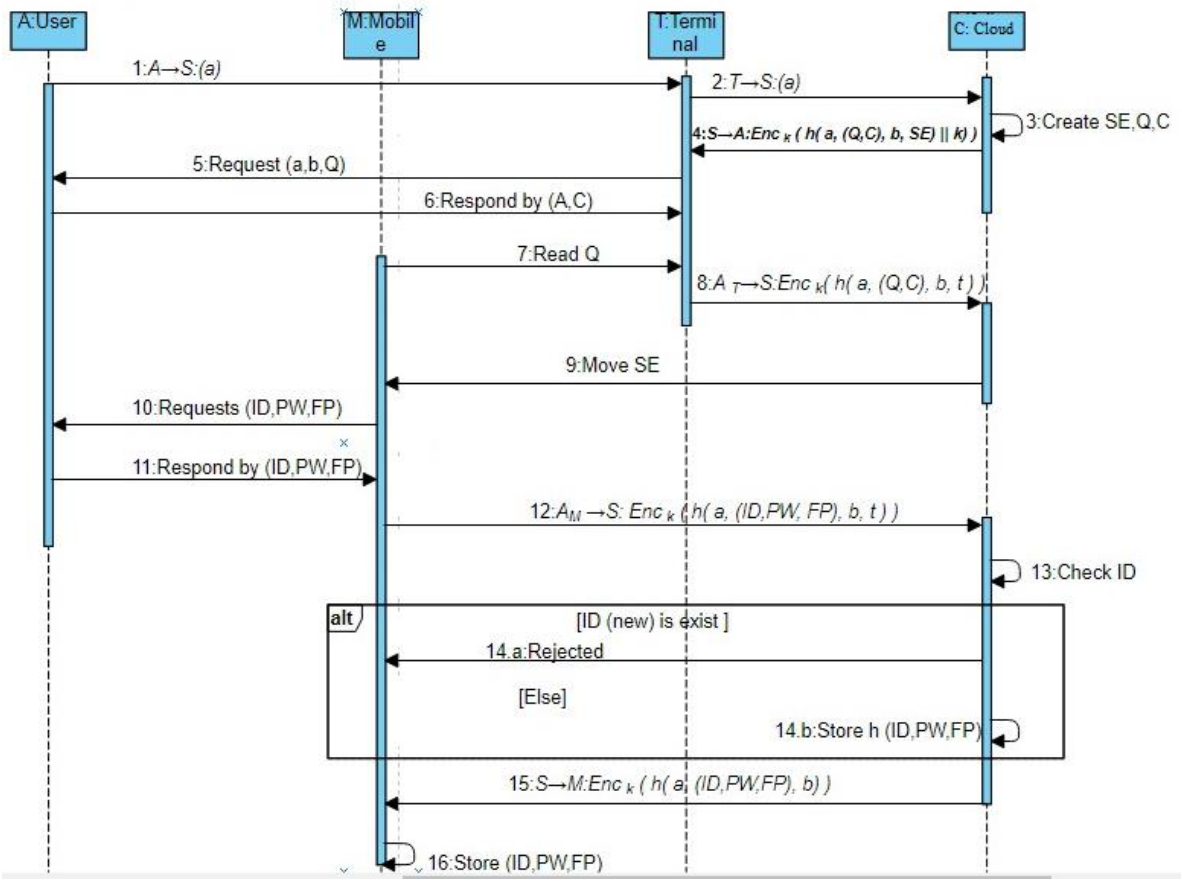

Figure 4.1 : Registration Phase Sequence Diagram

1- User sends registration request through his terminal (Desktop/Laptop) with his basic information *a*.

A→S: h(a)

2- The terminal sends the request to cloud server.

T→S: h (a)

3- Server received the request and generates onetime shared key *k*, and created *SE*,*Q*, *C* for user *A*.

4- The server sends *SE* and *h((Q,C, b) || k)* to terminal and requests *C* and *Q* from user *A*:

S→A: Enc $_k$ (h(a, (Q,C), b, SE) || k))

5- Through terminal, user asked to insert *a*,*C* and read *Q*.

6- User inserts *a* and *C*.

7- When the user inserts *a* and *C*, he/she uses his/her mobile phone to read *Q*.

8- Terminal compute $h(b, C, Q)$ and send them to server:

$A_T \rightarrow S: Enc_k (h(a, (Q,C), b, t))$

9- Server stores *a, b* and moves *SE* from terminal to mobile phone with *k*.

10- Mobile requests *(ID,PW,FP)* from user.

11- User inserts *ID,PW* and *FP*.

12- Mobile sends *h(ID,PW,FP)* to the server:

$A_M \rightarrow S: Enc_k (h(a, (ID,PW, FP), b, t))$

13- Server checks whither ID_{new} not exist in the ID table.

14 a- if ID_{new} exists in the *ID* table, the *ID* will reject.

14 b- if ID_{new} not exists in the ID table, the server saves h(ID,PW,FP).

15- Server save *ID,PW,FP* in the identity table and sends *h(ID,PW,FP)* to mobile phone:

$S \rightarrow M: Enc_k (h(a, (ID,PW,FP), b))$

16- Mobile saves *h(ID,PW,FP)* locally for local authentication.

4.2.2. Login & Authentication Phase

This phase is invoked when user wants to login into the cloud, where the users are verified before access to the cloud. Login phase accomplished through two scenarios, where the first scenario presents the behavior of user, mobile, terminal and the server, when the user accesses the cloud through terminal. The second scenario presents the behavior of user, mobile and the server when the user accesses the cloud through his mobile, for each login session the server generate random number that denote to session key, where the key will be changed after session expired.

There are two authentication steps included in this phase, the first one is local authentication, according to registration phase user *ID, PW* and *FP* will be stored at two places, which are the server and user mobile phone. When the user asks to login to cloud, he must firstly prove his identity locally before sending the request to the cloud server, where the user inserts his identity data (*ID, PW and FP*) and mobile phone will compare them with the stored data. The second one is server authentication, where then the local authentication is finished, the login request will arrive to the server and the server will authenticate user through his *ID, PW and FP*.

As a presumption on this phase:

A: User has a mobile phone that supports fingerprint reading.

B: Cloud server have a specific context aware technique to find out which device is used (mobile or terminal) to logged in to cloud system.

A- Login Through Terminal

When the user sends a login request to the server through terminal, he must use his mobile phone to authenticate himself, through inserting his fingerprint on mobile phone. So the session will be transferred to the mobile phone to allow user to read his finger print, we used a *QR* code as a precondition to transfer the session.

The basic flow of this scenario is as follow (figure 4.2).

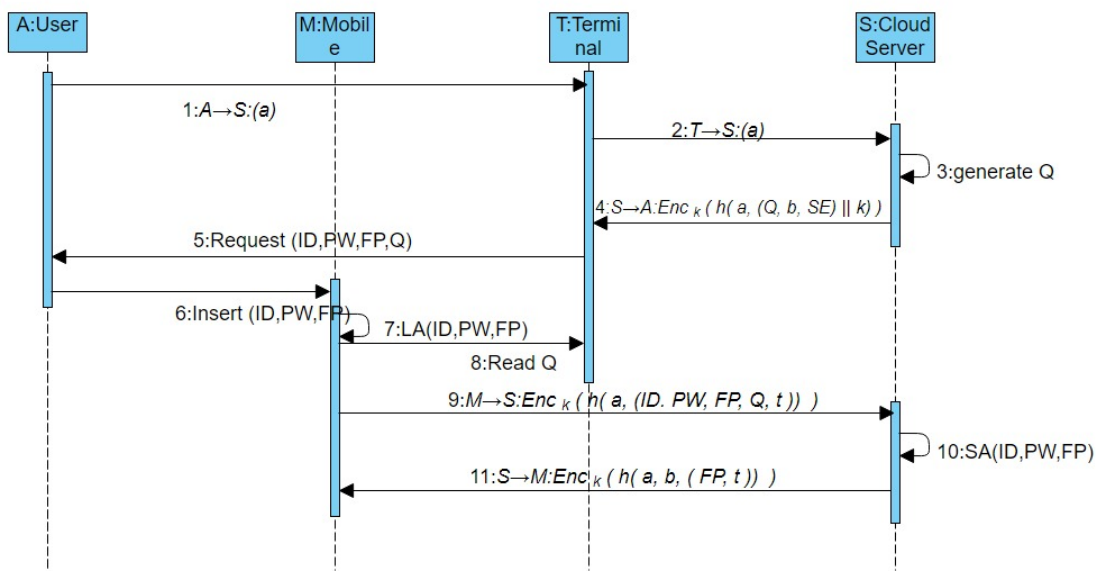

Figure 4.2 : Login & Authentication Phase Terminal Scenario Sequence Diagram

1- User sends login request through his/her terminal(Desktop/Laptop) with his/her basic information *a* :

$A \rightarrow S : h(a)$

2- The terminal sends the request to cloud server:

$T \rightarrow S: h(a)$

3- Server received the request and generate Q and *k* as a fresh onetime shared key.

4- The server sends SE and h(Q) to terminal.

$S \rightarrow A: Enc_k (h(a, (Q, b, SE) \| k))$

5- Through terminal, compute $Enc_k (h(a, (Q, b, SE))$ and asked user *A* to insert his ID,PW,FP and read Q using mobile phone camera.

6- User inserts ID,PW and FP on mobile phone.

7- Local authentication performed based on user data that stored on mobile.

8- Through mobile phone Q will be scanned from terminal.

9- Mobile sends h(ID,PW,FP,Q) to the server:

$M \rightarrow S: Enc_k (h(a, (ID. PW, FP, Q, t)))$

10- Server authenticates user.

11- Server responds by sending *SE* that have user profile.

$S \rightarrow M: Enc_k (h(a, b, (FP, t)))$

B- Login Through Mobile Phone

The basic flow of this scenario is as follow (figure 4.3).

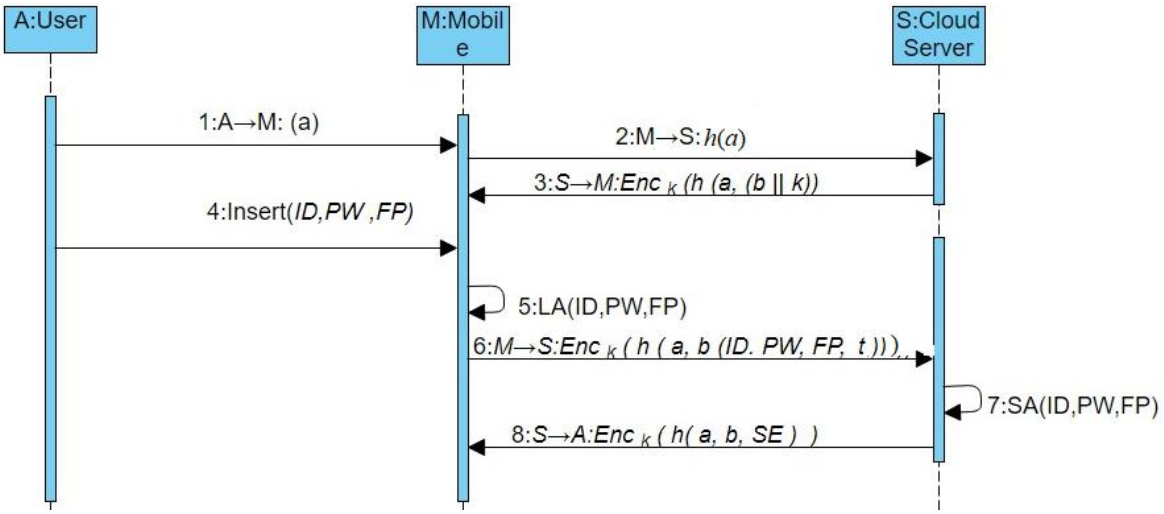

Figure 4.3 : Login & Authentication Phase Mobile Scenario Sequence Diagram

1- User sends login request through his Mobile with his basic information *a* :

A→M: a

2- Trough mobile the request will be sent to the server *M* :

M→S :h (a)

3- Server responds by generating a fresh onetime shared key with server authentication information *b*, and send it to user *M:*

S→M: Enc k (h (a, (b || k))

4- User inserts *ID,PW and FP* on mobile phone.

5- Local authentication performed based on user data that stored on mobile.

6- Mobile sends h(a, b, ID,PW,FP,Q, t) to the server:

M→S: Enc k (h (a, b (ID. PW, FP, t)))

7- Server authenticates user.

8- Server responds by sending *SE* that have user profile:

S→A: Enc k (h(a, b, SE))

4.2.3. Service Access Authentication Phase (SAAP)

In this phase, and for each user request, he must prove himself via insert his fingerprint. Where, by this verification the server will be protected from any internal attack such as SYN Flood attack. SAAP phase accomplished through two scenarios, where the first scenario presents the behavior of user, mobile, terminal and the server when the user accesses the cloud through terminal. The second scenario presents the behavior of user, mobile and the server when the user accesses the cloud through his mobile.

As presumptions on this phase:

A: User has a mobile phone that supports fingerprint reading.
B: Cloud server have a specific context aware technique to find out which device is used (mobile or terminal) to request a service from the cloud system.

A- SAAP Through Terminal

When the user requests a specific service from the server through terminal, he must use his mobile phone to authenticate himself, through inserting his fingerprint on mobile phone. So the session will be transferred to the mobile phone to allow user to read his fingerprint, we used a QR code as a precondition to transfer the session.

The basic flow of this scenario is as follow (figure 4.4).

1- From terminal user requests a service from the cloud server:
$A \rightarrow S: h(a)$
2- Server responds by generating Q and a fresh onetime shared key k, and sends it to user A:
$S \rightarrow A: Enc_k (h (a, (b, Q) \| k)))$
3- Through mobile user needs to read Q from terminal.
4- Via mobile Q will be read.
5- Mobile sends $h(FP,Q)$ to the server:
$M \rightarrow S: Enc_k (h (a, (b, Q, FP)))$

6- Server checks *Q,FP* and responds by the service with its *Si (service identifier)*:

$S \rightarrow T: Enc_k (h (a, (b, Si, SE)))$

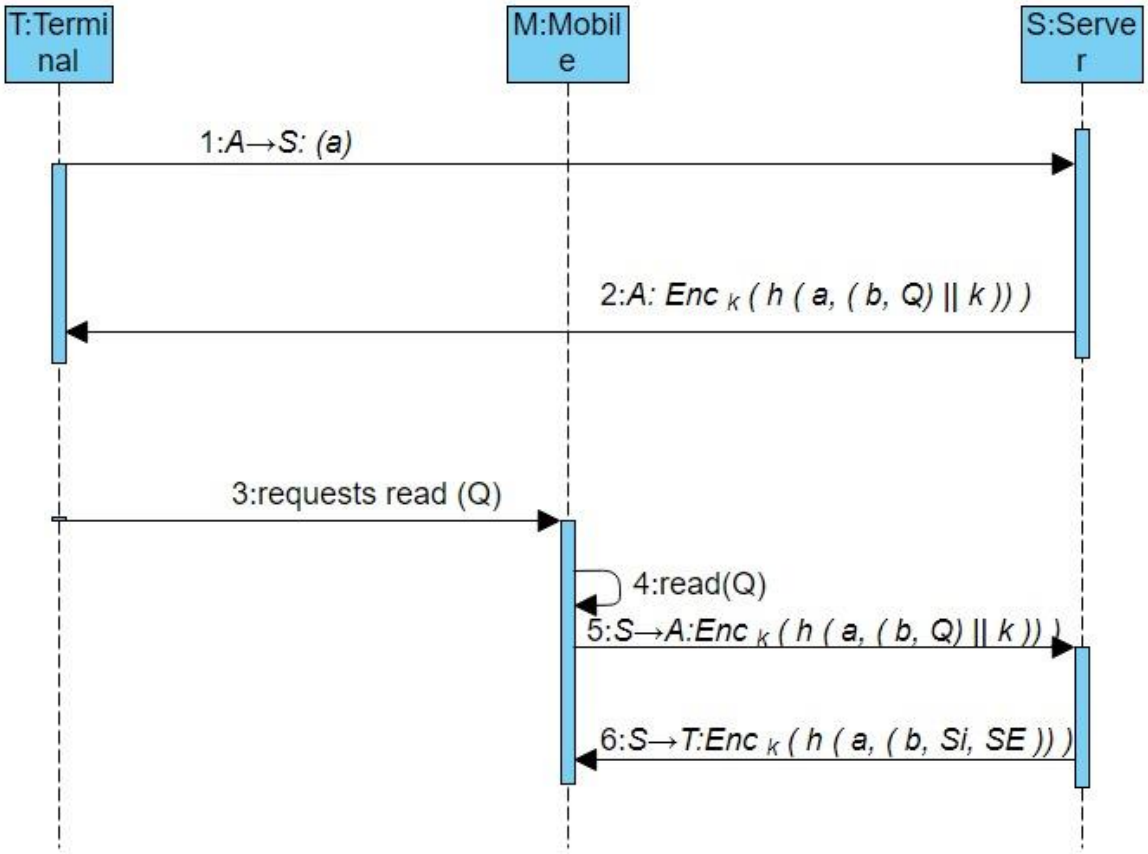

Figure 4.4 : SAAP Terminal Scenario

B- SAAP Through Mobile Phone

The basic flow of this scenario is as follow (figure 4.5).

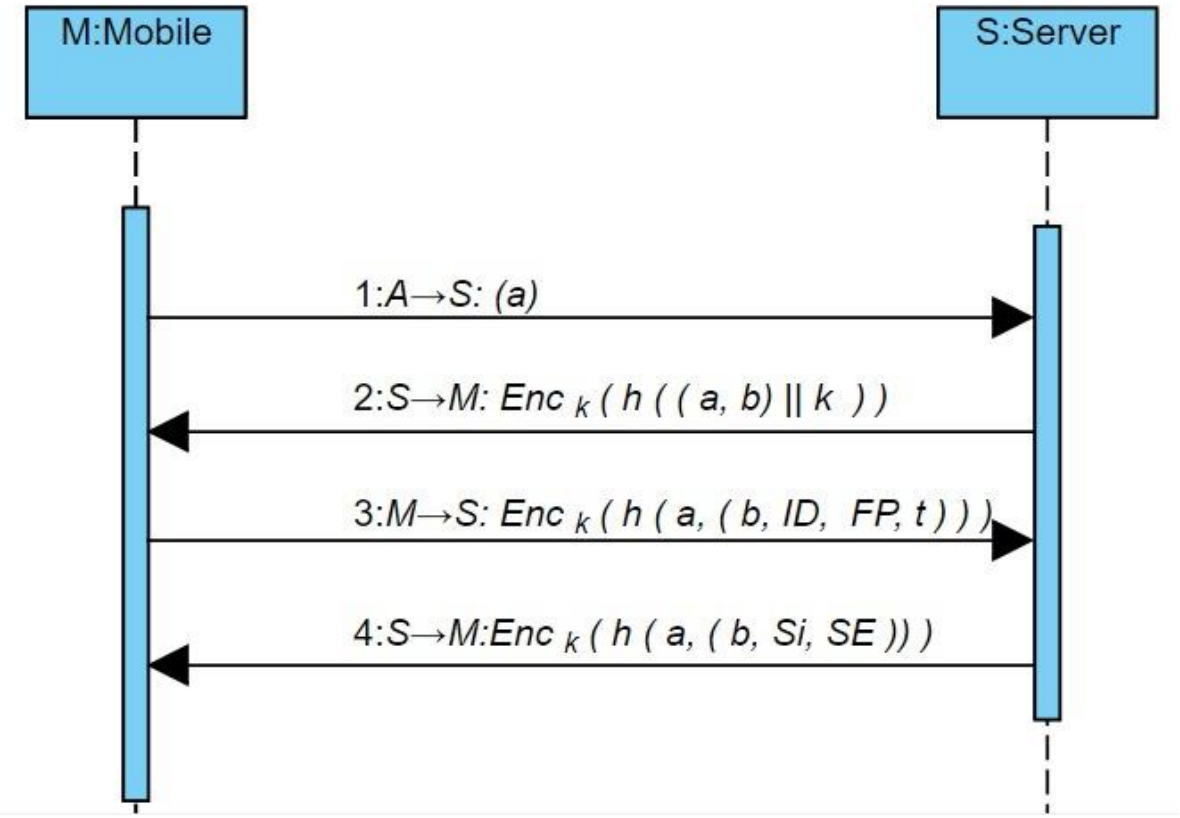

Figure 4.5 : SAAP Mobile Scenario

1- From mobile, user requests a service from the cloud server:

$A \rightarrow S: h(a)$

2- Server responds by generating a fresh onetime shared key *k*, and requests FP from mobile*:*

$S \rightarrow M: Enc_k (h ((a, b) || k))$

3- Mobile sends *h(FP,ID)* to the server:

$M \rightarrow S: Enc_k (h (a, (b, ID, FP, t)))$

4- Server checks ID,FP and responds by the service with its *Si (service identifier)*:

$S \rightarrow M: Enc_k (h (a, (b, Si, SE)))$

4.2.4. Change The Password Activity

The presented framework, considered a flexible framework, where user can on any time change his password.

The presumption of this activity is:
A: User can change his password through mobile phone only.
B: User is already logged in to cloud system.

The basic flow of this activity is shown in figure (4.6):

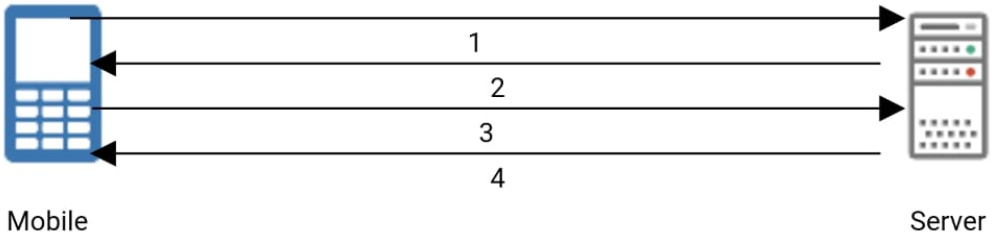

Figure 4.6: Change the Password Flow

1- User insert his/her *ID*, *PW* and *FP* in order to change his password.
2- The server check the correctness of *ID*, *PW* and *FP* then ask user to insert PW_{new}.
3- User sends PW_{new} to the server.
4- The server saved PW_{new} and sends it to the mobile phone for local authentication purpose.

4.3. The Defense against SYN Flood Attack

SYN Flood attack is a type of internal Denial of Services (DoS) attack. The attacker exploits the usage of TCP protocol, where according of TCP, there are three ways

handshake protocol as shown in figure (4.7), when the server releases an SYN-ACK to the user, the server is waiting an ACK from the user, where if the request is sent vie attacker he will not send ACK to the server and the request will be under the state of open connection request (Halagan, T. et al 2015).

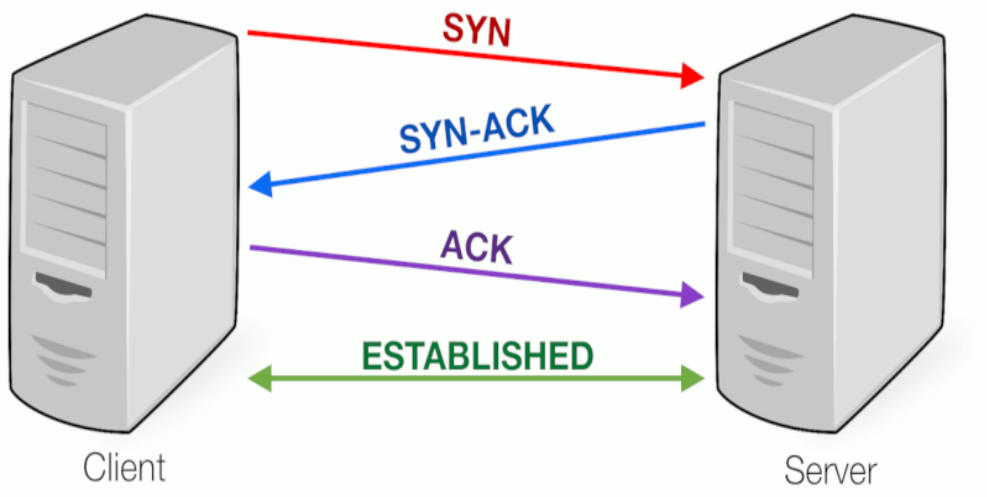

Figure 4.7: TCP Three Way Handshake Protocol

The presence of SYN flood attack (figure 4.8), when the attacker sends a large number of concurrent requests; without sending ACK to the server the buffer will be flooded by unreal request. So, if there is an honest user send a request to server he/she will find the server flooded (Hussain, K. et al 2016).

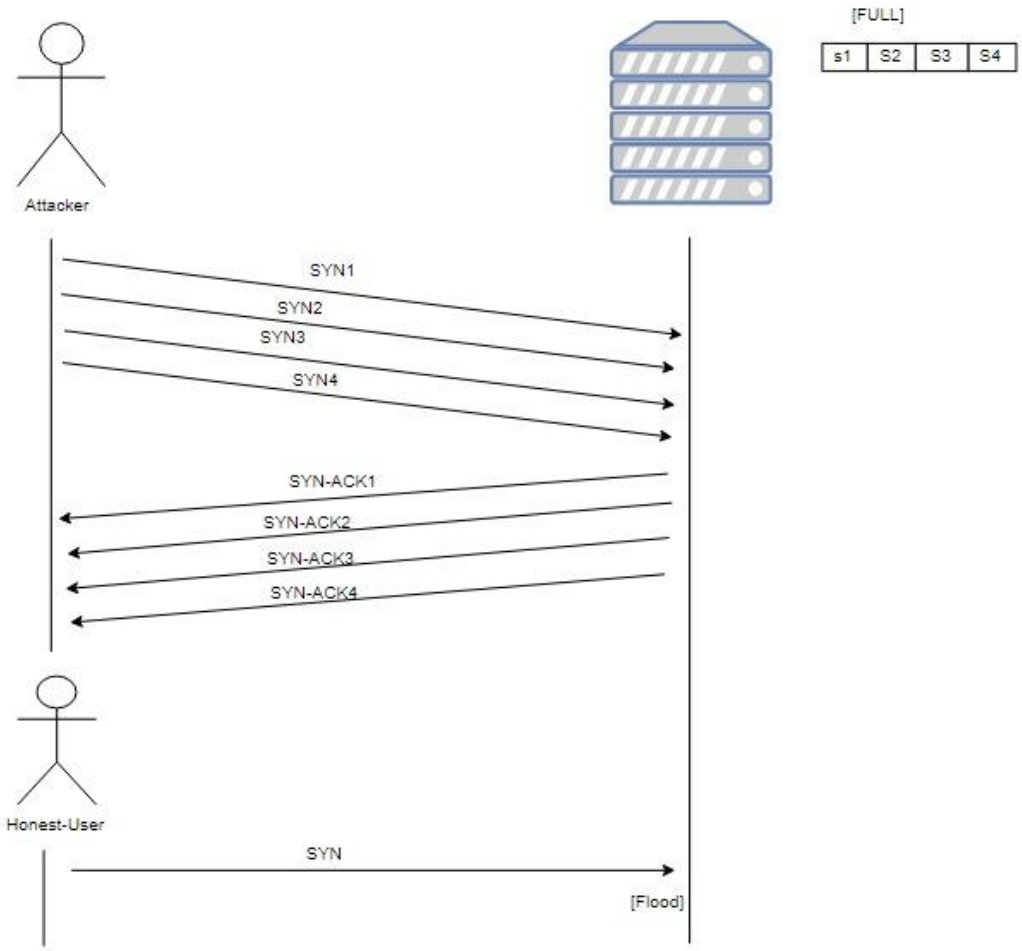

Figure 4.8: SYN Flood Attack

According to the presented framework, there is no way to be attacked by SYN Flood attack, where depending on SAAP (figure 4.9) the request will not be accepted or inserted in to the buffer until user sends his fingerprint with each request. Then the attacker cannot send any malicious request, because he cannot generate a fingerprint with each request depend on (Krämer, L et al. 2015).

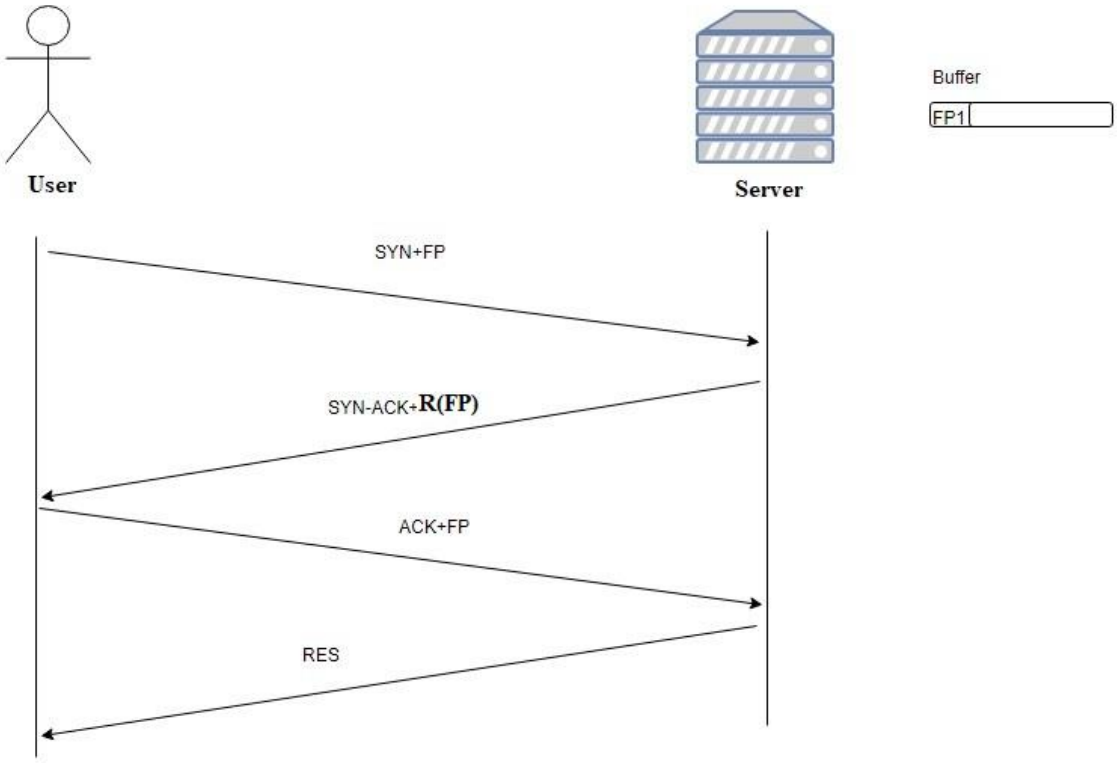

Figure 4.9: SAAP Against SYN Flood Attack

Firstly, user requests a specific service from the cloud server, where he must insert his fingerprint with each request. The server responds by inserting the requested ID and user fingerprint in the buffer and send SYN_ACK + R(FP), then user sends ACK and waiting for server responding.

Chapter Five:

EVALUATION AND SECURITY ANALYSIS

5.1 Introduction

In this chapter, we present an evaluation for the presented framework. According to (Hasan, M., Riaz. et al 2017), there is no clear stander or technique to test the authentication property under the concept framework. So, we used the evaluation technique that used in (Al-Attab, B. S., & Fadewar, H. S. 2016), where they used a security analyses that conclude in two step, the first one is functionality requirements which clear and justify the main function or property that used to defense against several types of attacks. The second one is security requirements which is justify who the framework defense against several types of attacks. Then a comparison table will show that, how the presented framework is more robust and efficient.

5.2 Security Analyses

In this section, the analyses will be divided into functionality requirements and security requirements.

5.2.1. Functionality Requirements

F1: Mutual Authentication

Is a technique in which both sides (user and server) in a specific communication channel authenticate each other, where the user authenticates the server and vice-versa. In the presented framework, the user verifies him/herself through two step, which are the local authentication and server authentication. The server authenticates itself to user by using server authentication information (*b)*.

In all phases, the user and the server authenticate each other by checking the equality of the user fingerprint *FP* and the server authentication information *b* at each side.

F2: Identity Management

When the user inserts his ID on the registration phase step 11, the server will check whether the ID $_{new}$ is unique (registration phase step 13) through ID management table, where the table contains all registered IDs.

F3: User Privacy

According to this work, each message transmitted under cryptographic mechanism, that by encrypting the messages between parties by onetime shared key for each opened session, where it is hard to be decoded. Hence, the scheme provides user privacy.

F4: Session Key Agreement

For each session, the server generates a fresh onetime shared key *k* between the user and the server. This key is concatenated with a specific session token established to prevent reuse that key. Therefore, in each login session, there is a session token generation. The generated token is established between the user and the server after the authentication process is finished. When the session is expired the token will not be repeated.

F5: Password Change

The presented framework includes password change activity, where on demand user can change his/her password as shown in chapter four section 4.2.4.

F6: Portability

This research work presents an authentication framework that able to be applied on cloud computing and mobile cloud computing everywhere any time.

F7: Authenticate the User at Registration phase

In the previous subsequence research works (Choudhury, A. J. et al 2011), (Chen, N., & Jiang, R. 2013), (Jiang, R. 2013), (Chen, N., & Jiang, R. 2014), (Patel, S. C. et al 2015), (Mun, J. et al 2016), the authors do not care about the registration phase, where they assumed that all the users and service providers are honest in the registration phase. So they did not take any security measures at the user registration phase. In this work, we provide several techniques to immunize the registration phase, such as CAPTCHA, onetime shared key establishment, session token, hashing, and QR code.

5.2.2. Security Requirements

R1: Replay attack

Replay attack occurs when the attacker eavesdrops on two-points of communication in order to repeat the request when the session is ended. The presented framework has a session key establishment where the session key is random and will never repeated, In addition to use of a time stamp.

R2: Password Guessing Attack

The framework stores the password in encrypted form in addition to use one way hash function (h(.)).The framework relies on two factors to determine user authentication, which are password and fingerprint. If the password has been disclosed, the fingerprint prevents intruder to access the server.

R3: External DoS

The framework guaranteed user authentication before access the cloud server in the login phase (chapter four, section 4.2.2, (A) step 7), thus there is no way to damage the server by external DOS.

R4: Internal DoS

After authentication phase, the Service Access Authentication Phase (SAAP) is started, in this phase the server asked user to prove himself/herself by sending his fingerprint with each request, he/she sends it to the server. Thus there is no way to send malicious requests to the server.

R5: Man in the Middle Attack

If the attacker have the message that sent from the user and the server or vice versa, his\her malicious attempt is not successful, where the attacker cannot modify the messages since it was encrypted in addition to used a time stamp and fingerprint mechanisms.

R6: Insider Attack

Insider attack is considered as one of the most dangerous threat to any inter-networking system. In this research work we prevent insider attack through SAAP, where user must identify his/her self by using fingerprint.

R7: Stolen Verifier Attack and Data Modification Attack

In this research work, we used the mobile phone to verify user authentication. where if the mobile phone is stolen, it is impossible for him/her to use it for accessing the cloud server, because he/she needs the fingerprint to access the service.

R8: Impersonation Attack

The presented framework does not transmits user ID and PW in the plaintext form, Instead, user ID and PW will be hashed and encrypted before they were transmitted. Also the framework using onetime sheared key, the key delivered to user through secret channel.

R9: Phishing Attack

The presented framework, include Mutual authentication between the user and the server (chapter five section 5.2.1), only authenticated server can send *b* and QR which consider the server identifier, that will be verified by the user.

R10: Server Masquerade Attack

In order to masquerade attack, the attacker forge his/her identity to get access to the cloud server, or to get greater privileges than they are authorized for. The attacker need to stole other user identity to performed masquerade attack, according to the presented framework there is no way to stole user identity, where the user used two security factors which are the password and fingerprint to verify himself/herself to the server, this made his/her identity very hard to be stolen.

5.3. Comparative analyses between different frameworks

In the following tables (Table 5.1 and Table 5.2) the comparative analyses of this research work with previous frameworks is given which indicate the contribution and enhancement of this work.

- Functionality Requirements

Table 5.1: Comparative Analyses Based on Functionality Requirement

Functionality Requirements	**Previous Framework**					**Our Frame-work**
	(Choudhury, A. J. et al 2011)	**(Nayak, S. K. et al 2012)**	**(Al-Attab, B. S., & Fadewar, H. S. 2016)**	**(fan, K. et al, 2018)**	**(Raina, P., & Patel, B. 2017)**	
F1	✓	✓	✓	x	✓	✓
F2	✓	✓	✓	x	x	✓
F3	✓	x	✓	x	✓	✓
F4	✓	✓	✓	x	x	✓
F5	✓	✓	✓	x	x	✓
F6	x	x	x	✓	✓	✓
F7	x	x	x	x	x	✓

- Security Requirements

Table 5.2: Comparative Analyses Based on Security Requirements

Security Requirements	Previous Framework					Our Frame-work
	(Choudhury, A. J. et al 2011)	(Nayak, S. K. et al 2012)	(Al-Attab, B. S., & Fadewar, H. S. 2016)	(fan, K. et al, 2018)	(Raina, P., & Patel, B. 2017)	
R1	✓	✓	✓	✓	x	✓
R2	✓	x	✓	✓	✓	✓
R3	x	x	✓	x	x	✓
R4	x	x	x	x	x	✓
R5	✓	✓	✓	✓	✓	✓
R6	✓	x	✓	x	✓	✓
R7	✓	x	✓	✓	x	✓
R8	✓	x	x	✓	x	✓
R9	✓	x	x	x	✓	✓
R10	x	x	x	✓	x	✓

Chapter Six:

CONCLUSION AND FUTUER WORK

6.1 Conclusion

In this work we present an enhanced framework to overcome the threat that may face the authentication property in cloud computing. The presented framework analyzed the most previous work shortages and resolved them. Where the framework construct under the concept of remote authentication, mutual authentication, identity management etc. The framework defense against several types of attacks such as Replay attack, Impersonation attack, Phishing attack, Denial of Service attack and others which were mentioned on chapter five. The presented framework consist of four main phases which are registration phase, login phase, authentication phase and service access authentication phase (SAAP). We reinforced the registration phase to be more robust by using CAPTCHA recognition and session key agreement through QR code. The login and authentication phase accomplish through two level of authentication which are local authentication and server authentication to guarantee only legitimate user can access the cloud server. In addition we provide the framework by SAAP to detect and defense against internal attack such as SYN flood attack.

To evaluate the presented framework, we firstly prepare a security analyses that justify each property and defense technique in the framework, then we compare the presented framework with most recently produced framework. The result show that the presented framework exceed all the comparative research.

6.2 Future Work

In the future work, we plan to provide an instance of the presented framework, in order to be able to implement. So then we can test the efficiency of the presented framework.

REFERENCES

References:

- **Adom, D., Hussein, E. K., & Agyem, J. A. (2018).** Theoretical and Conceptual Framework: Mandatory Ingredients Of A Quality Research. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH*, *7*(1), PP:2-4 .

- **Al-Attab, B. S., & Fadewar, H. S. (2016, December).** Authentication scheme for insecure networks in cloud computing. In *Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), 2016 International Conference on* (pp. 158-163).

- **Ashley, Paul A., Christopher Y. Choi, and Simon W. Gee(Aug. 2017).** "Sharing web application sessions across multiple devices." U.S. Patent No. 9,729,642. 8.

- **Birkmann, J. (2006).** Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions. *Measuring vulnerability to natural hazards: Towards disaster resilient societies*, *1*, 9, pp 3-7.

- **Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., & Smith, A. (2005, May).** Secure remote authentication using biometric data. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 147-163).

- **Chang, V., Kuo, Y. H., & Ramachandran, M. (2016).** Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*,pp 24-32.

- **Chen, N., & Jiang, R. (2013).** Analysis and improvement of user authentication framework for cloud computing. In *Advanced Materials Research*,756, pp. 3482-3486.

- **Chen, N., & Jiang, R. (2014).** Security analysis and improvement of user authentication framework for cloud computing. *Journal of Networks*, *9*(1),pp2-5.

- **Chien, H. Y., & Chen, C. H. (2007).** Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces*, *29*(2), pp 254-259.

- **Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011, December)**. A strong user authentication framework for cloud computing. In Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific (pp. 110-115).

- **Darwish, M., Ouda, A., & Capretz, L. F. (2015).** A cloud-based secure authentication (CSA) protocol suite for defense against Denial of Service (DoS) attacks. *Journal of information security and applications*, *20*,pp 3-7.

- **Doshi, N., & Patel, C. (2018, September).** A Novel Approach for Biometric Based Remote User Authentication Scheme using Smart Card. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 2093-2097).

- **Fan, K., Deng, H., Li, H., & Yang, Y. (2018**). Privacy Protection Smartcard Authentication Scheme in Cloud Computing. *Chinese Journal of Electronics*, *27*(1),pp 2-5.

- **Fox. A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., ... & Stoica, I. (2009).** Above the clouds: A berkeley view of cloud computing. *Rep. UCB/EECS*, *28*(13),pp 2-3.

- **Gao, Y., Fischer, R., Seibt, S., Parekh, M., & Li, J. (2017).** Integrated Security Framework., *INFORMATIK,28(1),pp 4-9*.

- **Halagan, T., Kováčik, T., Trúchly, P., & Binder, A. (2015).** Syn flood attack detection and type distinguishing mechanism based on Counting Bloom Filter. In *Information and Communication Technology*,12(1) pp. 30-39.

- **Hasan, M., Riaz, M. H., & Rahman, M. A. (2017).** Authentication Techniques in Cloud and Mobile Cloud Computing. *International Journal of Computer Science and Network Security*, *17*(11),pp 28-32.

- **Hussain, K., Hussain, S. J., Dillshad, V., Nafees, M., & Azeem, M. A. (2016).** An Adaptive SYN Flooding attack Mitigation in DDOS Environment. *International Journal of Computer Science and Network Security (IJCSNS)*, *16*(7), pp5-8.

- **Huszti, A and Ol´ah, N. (2016).** A Simple Authentication Scheme for Clouds, The 2nd IEEE Workshop on Security and Privacy in the Cloud, pp 1-4

- **Jiang, R. (2013).** ADVANCED SECURE USER AUTHENTICATION FRAMEWORK FOR CLOUD COMPUTING. *International Journal on Smart Sensing & Intelligent Systems*, *6*(4),pp 2-7.

- **Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., & Rossow, C. (2015, November).** Amppot: Monitoring and defending against amplification ddos attacks. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 615-636).

- **Lee, W. B., Fan, C. W., Ho, K., & Dow, C. R. (2012, November).** A CAPTCHA with Tips Related to Alphabets Upper or Lower Case. In *Broadband, Wireless Computing, Communication and Applications (BWCCA),* (pp. 458-461).

- **Liao, K. C., & Lee, W. H. (2010).** A novel user authentication scheme based on QR-code. *Journal of networks*, *5*(8), pp 2-5.

- **McDonough, John C., and Hadley Rupert Stern(Aug. 2016).** "Communication session transfer between devices" U.S. Patent No. 9,413,758. 9.

- **Mun, J., Kim, J., & Won, D. (2016).** An Improvement of User Authentication Framework for Cloud Computing. *JCP*, *11*(6), pp 3-7

- Munyaka, D., Noviansyah, B., Goel, V., Yenchik, A., & Durham, S. (2012). Cloud Computing Security. *Telecommunications Management*,7(2), pp 1-3

- **Nayak, S. K., Mohapatra, S., & Majhi, B. (2012).** An improved mutual authentication framework for cloud computing. *International Journal of Computer Applications*, *52*(5), pp 2-4.

- Patel, S. C., Singh, R. S., & Jaiswal, S. (2015, February). Secure and privacy enhanced authentication framework for cloud computing. In *Electronics and Communication Systems (ICECS)*,pp. 1-3.

- **Raina, P., & Patel, B. (2017).** Authentication Scheme in Cloud Computing Environment. International Journal of Advanced Research in Computer Science, 8(3),pp2-5.

- Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumar, N., & Vasilakos, A. V. (2017). On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services. *18*(*5)*,pp 2-4.

- **Singh, V. P., & Pal, P. (2014).** Survey of different types of CAPTCHA. *International Journal of Computer Science and Information Technologies*, *5*(2), pp 1-2.

- **Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017).** DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, *107*, pp 5-12.

- **Tsai, J. L., & Lo, N. W. (2015).** A privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE systems journal*, *9*(3), pp 2-4.

- **Vazquez-Briseno, M., Hirata, F. I., de Dios Sanchez-Lopez, J., Jimenez-Garcia, E., Navarro-Cota, C., & Nieto-Hipolito, J. I. (2012).** Using RFID/NFC and QR-code in mobile phones to link the physical and the digital world. In *Interactive Multimedia*. InTech,pp 5-9.

- **Weins, K. (2017).** Cloud computing trends: State of the cloud survey [Online], Available:http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloudsurvey

- Yang, G., Wong, D. S., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of computer and system sciences*, *74*(7), pp 3-9.

- **Zawacki, Jennifer Greenwood, et al(Jan. 2017).** "Seamless application session reconstruction between devices." U.S. Patent No. 9,537,957. 3.

- **Zhang, Q., Cheng, L., & Boutaba, R. (2010).** Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), pp 2-7.

تحسين إطار عمل موثوقية المستخدم في الحوسبة السحابية بأستخدام الهاتف المتنقل

الملخص

الحوسبة السحابية هي تقنية حديثة تستخدم للتعامل مع العديد من التطبيقات وتكوينها والوصول إليها عبر الإنترنت. ويوفر تخزين البيانات والبنية التحتية والتطبيقات. بالإضافة إلى أنه عبارة عن مجموعة تعتمد على موارد الحوسبة البرمجية والمادية المتوفرة كخدمات الشبكة. تعاني مثل هذه التكنولوجيا الجديدة الكثير من التهديدات المحيطة بالحوسبة السحابية ، مثل تكامل البيانات وسرية البيانات والتحكم في الوصول ومصادقة المستخدم التي تعتبر أكثر المشكلات الأمنية شيوعًا في الحوسبة السحابية.

في الآونة الأخيرة ، هناك الكثير من الأعمال البحثية التي اقترحت أطر توثيق المستخدم ، من أجل الدفاع ضد عدة أنواع من الهجمات مثل هجوم إعادة الهجوم ، والرجل الأوسط في الهجوم ، والحرمان من الخدمة ، وغيرها. إن معظم الأطر السابقة تتكون من ثلاث مراحل رئيسية هي مرحلة التسجيل ومرحلة تسجيل الدخول ومرحلة المصادقة ، والكثير منهم أضاف نشاط إضافي لتغيير كلمة المرور. لكن، لا تزال أطر العمل المقترحة سابقاً تعاني من العديد من المشاكل مثل الضعف الأمني في مرحلة التسجيل ، ولا توجد طريقة للتعامل مع الهجوم الداخلي مثل هجوم فيضان SYN.

في هذا البحث ، نقدم إطارًا قويًا للمصادقة على المستخدم ، يتغلب على النقص السابق في إطار العمل. ويدعم الإطار المحسن العديد من خصائص الأمان مثل المصادقة عن بُعد والتوثيق المتبادل وإنشاء مفتاح تشفير لحلقة الاتصال وغيرها. بالإضافة إلى مرحلة التسجيل المحسنة ومرحلة تسجيل الدخول ومراحل التوثيق ، أضفنا مرحلة مصادقة الوصول إلى الخدمة (SAAP) ، حيث سيتم في هذه المرحلة فرض التحقق الداخلي.

في نهاية هذا العمل البحثي ، قمنا بتحليل أمني يبرر كيفية اقتراح الدفاع الإطاري ضد عدة أنواع من الهجمات ، ثم نقدم مقارنة يبين كيفية تجاوز الإطار المحسن الاطر السابقة.

تحسين إطار عمل موثوقية المستخدم في الحوسبة السحابية بأستخدام الهاتف المتنقل

إعداد

أحمد محمد الرفاعي

المشرف

الدكتور خلدون بطيحه

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في علم الحاسوب

عمادة البحث العلمي والدراسات العليا

جامعة فيلادلفيا

كانون الثاني ، 2019