



**Arab American University**

**Faculty of Graduate Studies**

**Hybrid Cloud-Based Mobile Payment: Secure &  
Compliance Model**

**By**

**Adel Jamal Abdallah Hassan**

**Supervisor:**

**Dr. Amjad Rattrout**

**This thesis was submitted in partial fulfillment of the  
requirement for the Master's degree in computer  
science**

**Jan / 2019**

**© Arab American University – 2019. All rights reserved.**

# Hybrid Cloud-Based Mobile Payment: Secure & Compliance Model

By

**Adel Jamal Abdallah Hassan**

This thesis was defended successfully on 26/1/2019 and approved by:

Committee members

Signature

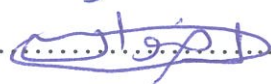
1. Supervisor Name: Dr. Amjad Rattrout

.....  


2. Internal Examiner Name: Dr. Rami Khalil

.....  


3. External Examiner Name: Dr. Radwan Tahboub

.....  


## **Declaration**

I hereby declare that this master thesis has been written only by myself without any assistance of any third party and describes my own work unless otherwise acknowledged in the text of the thesis.

All references, verbatim extracts and information source are quoted and cited properly. Thus, I confirm that no source has been used in this thesis other than those indicated in the thesis itself.

This master thesis has not been accepted in any other previous application, in whole or in part for any degree.

Signature:

Adel Jamal Abdallah Hassan

## **Dedication**

This thesis work dedicates to my wife, who taught me the meaning of patience and endurance.

This work also dedicates to my parents, for continuous love and encouragement.

This work also dedicates to my kids: Nagham, Omar and Judy.

## **Acknowledgments**

I would like first to thank my supervisor Dr. Amjad Rattrout for the instructions and the support that he provides me during thesis research.

Secondly, I would like to thank the AAUP University represented by the College of Information Technology and Engineering for providing opportunities to study and graduate for a Master of Science in Computer Science

Also, I would like to thank my IT team for helping me in the part of coding of this thesis.

Finally, thanks a lot to my wife and my family for supporting me during the period of my study.

## **Abstract**

This thesis presents an innovative research and development work based on mobile cloud computing, security payment and compliance model to provide a new secure payment model using mobile phone system.

This research and development work will affect directly in the direct payment process in the financial services sector and will develop a payment new model in Palestine.

Main issues in mobile banking that this research divided into three main categories , Environment , Security , Compliance. First model is infrastructure model of the platform is designed on the basis of a hybrid model environment (local and cloud), second model is access system model of the platform is designed on the basis of risk-based and adaptive authentication mechanism using biometric techniques (Face Recognition) , third model is compliance model of the platform which designed to match with local regulatory bodies in Palestine (PMA) , and international standard of payment card industries (PCI).

Payment methods in the Palestinian market have different types of payment such as cash payment, or payment by debit cards and credit cards. This research provides a new way to pay using mobile phones to make it easier for people to pay their bills and pay for the goods and services they buy.

We prove on our demonstration that we manage to give better results comparing with related works for each part mentioned in our objectives and goals of this research.

Cloud comparison result based on questionnaire has a result score of 3.8/5 and Security comparison result based on questionnaire has a result score of 4.6/5.

Our research can be considered as foundation key base for any applied research works in the field of payment system.

We manage also, to introduce and build new secure payment system that will be valid to work in market that targeting any financial service organization like banks, payment and fintech companies.

Finally, such these technologies for mobile application and mobile payment are very needed and required for our Palestinian market, since the Israeli occupation divide our land to small pieces of areas that not sufficiently connected to each other's and we cannot control our boards and cannot issue a national currency as in PMA report for financial inclusion [PMA Payment System, 2013]. This thesis will consider the first model to activate mobile payment using mobile banking application to facilitate for Palestinian people to do their financial transaction with very ease of use as a term of usability "customer experience" and more secure environment and considering availability to access their banking system from anywhere and at any time.

## Table of Contents

Abstract	<b>Error!</b>
<b>Bookmark not defined.</b>	
List of Tables	vii
List of Figures	vii
List Abbreviation	XIII
<b>Chapter 1</b>	
1. Introduction	1
1.1 Overview	1
1.2 Problem Statement	2
1.3 Background & Motivation	2
1.4 Research Contribution	3
1.5 Research Methodology	4
1.6 Thesis Structure	5
<b>Chapter 2</b>	
2. Literature-Review	6
2.1. Overview	5
2.1.1 Mobile-Cloud-Computing-Architectures	7
2.1.2 Benefits of using Mobile-Cloud-Computing	10
2.1.3 Mobile Applications & Mobile Cloud Computing Applications	11
2.1.3.2 Mobile Banking Application	11



2.1.3.3 Mobile Payment Application	13
2.1.4 Mobile with Biometric Recognition	15
2.1.4.1 Face Recognition	17
2.1.4.2 Liveness Detection – Face Recognition	18
2.1.4.3 Face detection	19
2.1.4.4 Face Extraction	19
2.1.4.5 Face Recognition	19
2.1.4.6 Face Recognition Mechanism	20
2.1.4.7 Old Biometric techniques still weak	21
2.1.4.8 Face Recognition Algorithms & SDK	22
2.2 Cloud Computing Technologies	23
2.3 CC & MCC threats and Vulnerabilities	23
2.4 Compliance	24
<b>Chapter 3</b>	
3. System Overview	27
3.1 Current System	27
3.1.1 Issues with the current system design	28
3.2 Proposed System (Mobi-Cash)	28
3.2.1 SMS & OTP Algorithm	32
3.3 Benefits of the proposed system design	34
3.4 Software development on Mobile Applications	34

3.5 Mobile Devices	35
3.5.1 Mobile Devices Operating System	35
3.6 Feasibility Study	36
3.6.1 Technical Feasibility	37
3.6.2 Financial Feasibility	37
3.6.3 Resources and time Feasibility	37
3.6.4 Risk & Legal Feasibilities	37
3.6.5 User & System requirements	37
3.6.6 Functional requirements	38
3.6.7 Non-Functional requirements	38
3.6.8 Domain Requirements	38
3.7 Mitigation methods to tackle most of the Vulnerabilities and threats of cloud & Mobile Cloud computing	39
<b>Chapter 4</b>	
4. System Design and Implementation	45
4.1 Our Public Cloud Layers	46
4.2 Our Private Cloud Layers	52
4.3 Our Mobile Application Layers	55
4.4 Development & Experimental Results	55
<b>Chapter 5</b>	
5. Experimental Results of Implementation	58

5.1 Part # 1: Hybrid cloud model	58
5.2 Part # 2: Security Mobile Payment Comparison	62
5.3 Part # 3: PCI Compliance	68
<b>Chapter 6</b>	
6.1 Conclusions and Future Work	70
6.1 Conclusion	70
6.2 Future Work	73
Bibliography	76
Appendices	87
A. Pseudo Codes	87
B. Mobile and Web Application Interfaces Diagrams	87
C. Mobile & Web Application Images	99
D. Web Application Interface	106
E. Mobile Web Portal Reports	108
F. Experts Opinion for System Structure Mobi-Cash Mobile Banking Questionnaire	109
G. Mobile Banking Questionnaire	109
الملخص	110

## List of Tables

2.1 PCI DSS Requirements	26
4.1 Hardware & Software Specification	57
5.1 Mobile Cloud Computation Security Comparison – Related works	59
5.2 Security Mobile payment Comparison	63
5.3 Security of Mobile cloud computing-related works	65
5.4 PCI DSS Results	68

## List of Figures

2.1 Mobile-Cloud-Computing (MCC) Architecture	7
2.2 Cloud-Computing-Structure Services	7
2.3 MCC Basic Architecture	8
2.4 Cost average transaction of different banking e-channels	10
2.5 Biometric types	15
2.6 Enrollment Process	17
2.7 A generic face recognition system	19
2.8 Samples of Images that shows spoofed images the real images of customer	20
2.9 Image Capture	21
3.1 Software Architecture Diagram	35
3.2 Android OS Kernel	36

4.1 our System & Structural Model (Mobi-Cash)	46
4.2 Public Layer Interaction block diagram	49
4.3 Private Layer Interaction block diagram	52
5.1 Private Cloud	60
5.2 Public Cloud	60
5.3 Hybrid Cloud	61
5.4 Hybrid Cloud “Mobi-Cash”	61
5.5 Web Access before attack	68
5.6 Web Access after attack	68

## List of Abbreviations

CC	Cloud-Computing
MCC	Mobile-Cloud-Computing
MC	Mobile-Cloud
SaaS	Software as per a service
PaaS	Platform as per a service
IaaS	Infrastructure as per a service
SOA	Service-oriented architecture
PMA	Palestinian Money Authority
MNO	Mobile Network Operator
PCI	Payment Card Industry
NFC	Near Field Communication
QR	Barcode and quick response code
CPU	Central Processing Unit
2FA	Two Factor Authentication
OTP	One Time Password
API	Application Programming Interface
MAUI	Memory Arithmetic Unit Interface
ATM	Automated-Teller-Machine
PIN	Personal-Identification-Number
FaaS	Framework as a service
3G	Mobile-Third-Generation
GSM	Global System Communication
CDMA	Code Division System
PKI	Public Key Infrastructure
BOP	Bank of Palestine
BART	Bay Area Rapid Transit
P2P	Peer to Peer, Person to Person
MPSP	Mobile Payment Service Provider
HA	High Availability

HPCC	High-Performance Cluster Computing
ISV	Independent Software Vendor
CS	Computer System
IoT	Internet Of Thing
Mobi-Cash	Mobile Cash Application
FMR	False Match of Rate
FPIR	False Positive Identify of Rate
FNIR	False Negative Identify of Rate
FNMR	False Non-Match of Rate
IVR	Interactive Voice Reply System
USSD	Unstructured Supplementary Service Data
SMS	Short Messaging Service
CAPTCHA	Completely Automated Public Turing
STOVE	Strict, Observable, Verifiable Data and Execution Models
SACS	Security Access Control Services
CSA	Cloud Security Alliance
J2ME	Java 2 Platform, Micro Edition
WPKI	Wireless Public Key Infrastructure
PIN	Personal Identification Number
3DES	Data Encryption Standard
OTP	One Time Password
SLA	Service Level Agreement

## **Chapter One**

### **1. Introduction**

This chapter consists of an overview of the research idea, problem statement, background, and motivation. Moreover, it contains the research methodology, research goal, research contribution, and the structure of the thesis.

#### **1.1 Overview:**

Information technology becomes an essential and vital component in any organization that needs to manage and processes their data, especially like banks and financial services sector.

One of these evolving technologies is mobile phones that have invaded our lives in everything's, and it manages to improve the way accordingly how we exchange the information between us and innovate a new method of delivery of services among people.

In parallel, communication technology (Wi-Fi, GSM) has been evolved in such way that enables these mobile devices to communicate in a very modern style and produce a new type of application that allows the people and organization to react with each other's based on nature of services that they are looking for it.

The banking sector is one of the most beneficiaries of this advance in technology, which enabled them to develop the way they deliver services to their customers. The banking services that can be offered to the customer vary according to the nature and function of the service, such as automated teller machine (ATM), telebanking, SMS, internet banking, interactive voice response (IVR), debit cards, credit cards, mobile banking, and mobile payment. These services also called by channels which the way to contact bank customers.

Mobile banking is the newest and advanced channel that enable the customer to access their accounts 24/7 using their mobile devices. Also, mobile banking channel considers less cost and more faster comparing other channels such as ATM and save time and efforts to the customer instead of visiting bank offices and branches (Yong Wang et al., 2015).



## **1.2 Problem Statement:**

Main issues in mobile banking are

- Environment
- Security
- Compliance

Most of banks have many issues related to how to provide services to their clients under the conditions of the Israeli occupation to its territory, which leads to the difficulty of geographical communication between its cities and villages. This prompted the banks to adopt new mechanisms that are not dependent on the client's visit to the bank to conduct its banking operations such as account inquiry, money withdrawal, transfer between accounts and bill payment.

Furthermore, the banking risk assessment shows that one of the most important threats facing banks is the lack of the necessary infrastructure for information technology due to Israeli occupation activities, such as not allowing devices to enter the country to build computer data centers such as security and encryption devices.

In addition to the aggression by the Israeli occupation forces on the facilities and institutions of the country at any time. On the other hand, security issues must be handled when dealing with customers' information in these adverse circumstances to protect from international threats facing the IT environment about physical security, communication, and data security issues.

## **1.3 Background & Motivation**

Most banks have different channels to offer their services to customers. Starting from service delivery through the telephone to service delivery through the internet. From another hand, the revolution walks side by side in mobile devices and wireless services that push the banking sector looking for new way to attract their customers using innovation methods using internet services such as internet banking and mobile banking. Mobile banking (M-banking) term used by (Tiwari and Buse, 2007) has been

born, which is describe how the customer can reach bank services using their mobile devices. Mobile banking services enable customers to use their phones to check balances, transactions, get account information, do transfer funds, locate branches or ATMs, and pay their bills (E Turban, D King, J Lee, 2008) taking in consideration that these services can be done using different types of communication channels like SMS, GPRS, and 3G.

Banks consider mobile banking as one way to reduce costs such as building and IT costs. The fewer customers are visiting the bank, the less demand there is to open new branches and offices. On the other hand, statistical report view, there are 5 billion mobile users worldwide, but mobile banking users do not exceed 200 million (Waranpong Boonsiritomachai, 2017)

In spite of attractive using mobile banking features and the opposite side, there is less adoption of using it locally and globally. In addition to the occupation of Israeli to our land and their consequences to the Palestinian economy, this is being the reason why pushing me to introduce a model to tackle all these issues and move forward to adopt mobile banking model in all our financial services organizations.

#### **1. 4 Research Contribution:**

1. Design & build a new innovative adaptive system model of mobile banking application that uses hybrid cloud environment.
2. Develop mechanism and procedures mapping security with mobile banking system to secure payment process and each component in system architecture.
3. Achieve compliance model following of PMA and PCI instructions.
4. In addition to following benefits add to payment system:
  - Reduces the time and the effort of the traditional banking operations.
  - Reliable authentication
  - High availability

- Minimize the latency
- Greater efficiency
- User friendly
- Fraud Detection Mechanism
- Risk Decisioning

The ultimate goal of this thesis to introduce a model to use mobile banking application to serve bank customers depend on the hybrid environment “ On-premise & cloud” from infrastructure side to cover all weakness and shortages in each environment in aside. Moreover, the new model will design and build a new software mobile application that deals with all security concerns that are facing mobile, cloud and communication parts of the model. On the other hand, the new model will address the regulatory issues to build a compliance model from both sides locally by following PMA instructions and globally by following international standards like PCI standards.

### **1.5 Research Methodology:**

In this research, we will basically follow the steps below to achieve the goals and objectives of the thesis.

1. Study and analysis of cloud computing and how we can use these technologies in our market to come over the challenges of Infrastructure availability and expandability aspects.
2. Study and analysis of MCC models and build the new system design to solve all limitations and challenges (Amjad Rattrot, 2013), the articles describe in problem definition.
3. Exploring and review Mobile payment technologies existence and choose one method to be used in the thesis that fit with the sole of research scope.
4. Study and analysis of the PMA & PCI regulations for financial services.
5. Study and analysis all threats and vulnerabilities on cloud and mobile cloud computing facing mobile payment system.

6. Build mobile banking application that uses both private and public cloud.
7. Identify all techniques to reserve the safest and secure use of mobile payment system.
8. Develop mechanism and procedures mapping security with mobile banking system cloud hybrid, to secure the whole process and each component in system architecture.
9. Design, build and implement a new innovative adaptive system model for mobile banking application.

### **1.6 Thesis Structure:**

The Structure of the thesis separated into Six chapters. The first chapter provides the goals and objectives of the thesis and describes the thesis structure. The second chapter will be a brief of all previous works in the field of mobile cloud solutions. The third chapter will talk about my system structure approach and system analyst based on software engineering life cycle. The fourth chapter that will speak to the core of the thesis subject which is system design model & results of experimental work and conclusions of the thesis. Also, future works and recommendation to build a new era of mobile payment application in the Palestinian market.

## **Chapter Two**

### **2. Literature Review**

#### **2.1 Overview of Mobile cloud & Applications**

(Amit K. Sharma,2013) state that the concept of mobile cloud computing MCC refers to build a cloud infrastructure for mobile applications, so that power consumption, storage, and data processing are on the edge of cloud computing but run the mobile application will be at the side of mobile devices, which make the mobile devices work as mobile subscriber.

Mobile cloud computing merge two technologies with each other, mobile computing, and cloud computing together based on the definition of (Han Qi, 2014).

Mobile computing divided into three parts which are hardware such as mobile devices, software such as applications installed on mobile devices, and communications such as infrastructure network component.

Cloud computing is a set of groups of virtual servers work together in a distributed manner over the internet.

Mobile-Cloud-Computing from another point of view is defined that all processing of data will happen outside of the mobile devices which as cloud environment that will lead to minimize the computing at the mobile side and do all computing into a cloud environment. Computing includes CPU, memory and storage aspects that ensure less power consumption and storage at the level of mobile devices. So, using mobile application tools to connect to the internet (Cloud) that satisfied or achieve the concept mobile-cloud-computing MCC (Hoang Dinh Thai,2015).

### 2.1.1 Mobile-Cloud-Computing-Architectures

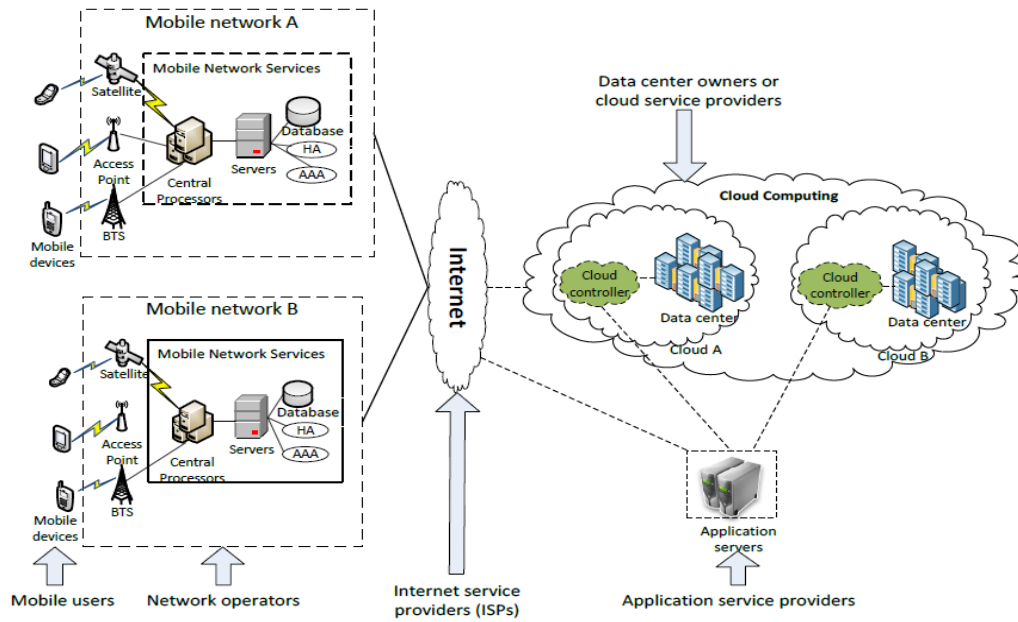


Fig. 2.1 Mobile-Cloud-Computing (MCC) Architecture - (Hoang Dinh Thai,2015).

Figure 2.1 is the architecture of mobile cloud computing that describes how can end users use their mobile phones to access mobile providers network using the internet; then they can get access to a cloud environment and use all different applications and services (Hoang Dinh Thai,2015).



Fig. 2.2 Cloud-Computing-Structure Services - (Hoang Dinh Thai,2015).

Figure 2.2 defines the structure of cloud computing services that divide the cloud up to four different types. Cloud computing service layers describe as follows:

- Data centers layer that contains the hardware and utility services such as power, UPS, Cooling, Generators...etc.
- Infrastructure layer that contains hardware of IT components such as servers even physical or virtual, network devices “Switches & Routers” in addition to storage devices.
- Platform layer that contains custom applications that already created and setup based on needs of end users such as Microsoft Azure.
- The software layer that contains software based on end-user needs such as Salesforce.

MCC Basic architecture consists of multiple components, the private cloud (On-premise), public cloud (off-premise), and a mobile application.

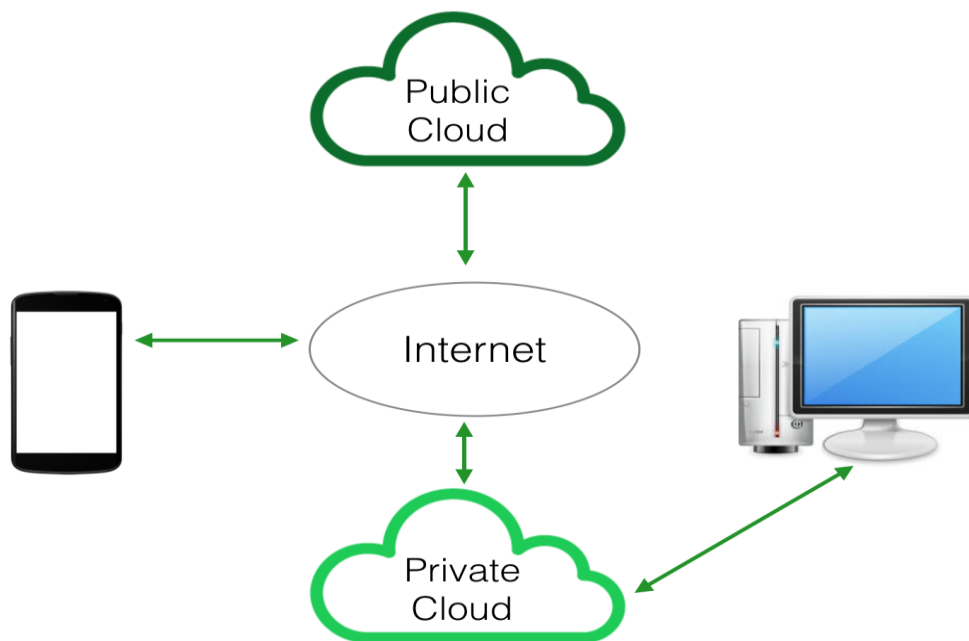


Fig. 2.3: MCC Basic Architecture

Fig 2.3 shows basic architecture of mobile cloud computing that contains private cloud, public cloud, mobile devices, and bank servers.

- **Public Cloud (off-premise):**

The public cloud (off-premise) runs the electronic banking services that are given to the customers, the authentication services and it holds a backup for the internal banking data to guarantee the availability of the information even when internal services in the private cloud goes down. Also, it provides the low-latency usage, scalability and the availability of the customers due to the robust infrastructure which is offered by the public cloud providers sub as Microsoft, Google, and Amazon.

The public cloud contains the APIs (application development interface) of the online services that integrate with the mobile application.

The Public Cloud layer contains the following servers:

1. Cognitive API.
2. SMS Gateway (based on two-factor authentication 2FA).
3. Ticketing System.
4. High Availability HA central system servers such as Mobile servers, Mobile Applications, and Data Base servers.

- **Private Cloud (On-premise):**

The private cloud (On-premise) use for internal banking operations, such as money transfers, customer relationships, and management. The private cloud allows the bank to retain control and apply rigorous security with lower cost and effort. So, it decreases the total cost of ownership of software licenses and reduces the deployment resources.

The private cloud contains internal banking web applications, databases, security, and network solutions.

- The Private Cloud layer (On-premise) contains following servers:

1. Web Application Firewall
2. Web Application Servers
3. Database Servers
4. Security and event logging management servers (SIEM)



### 2.1.2 Benefits of using Mobile Cloud Computing:

There are a lot of benefits that we can conclude using mobile cloud computing like:

- Battery lifetime Extension
  - Improving data storage capacity and power consumption
  - Enhancing reliability
  - Dynamic provisioning of resources.
  - Scalability.
  - Multitenancy.
  - Conveniently of integration.
- Mobile banking channel considers the lowest cost channel is comparing to other channels that customers contact their banking environment such as Fig 2.4:
1. Call Center
  2. Branch
  3. ATM
  4. Mobile
  5. IVR
  6. USSD
  7. Online

## Business Benefits

### • Reduced costs

**Average transaction cost in the US**  
(includes labor and IT costs)

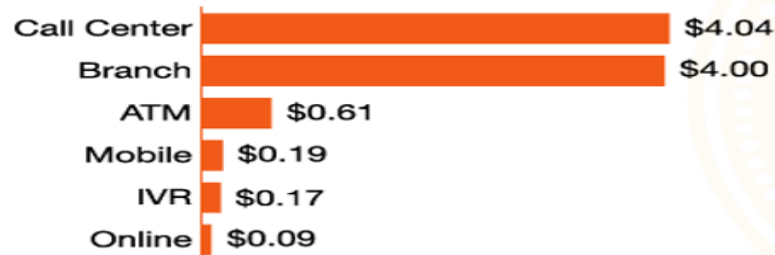


Fig 2.4 Cost average transaction of different banking e-channels

Figure 2.4 shows the advantages of mobile banking for the financial institution to be adding to the benefit of the financial transaction. Moreover, how the banking sector benefits from adopting e-channels services such as mobile application to reduce their costs, also this figure shows the average transaction cost in US dollar for each e-channels in the bank. Mobile banking application considers from lowest cost channel that most of the bank try to encourage their customer to adopt it to do their financial transactions.

### **2.1.3 Mobile Applications & Mobile Cloud Computing Applications:**

There are a lot of different types of mobile cloud applications that can be vary based on nature of data that will be used through these mobile applications, such as for learning, health, games, banking or commerce ...etc.

#### **2.1.3.1 Mobile-Commerce**

These applications are mainly used to serve financial processes, such as user account transactions, payments, transfer or shopping online and even announcing for new products as described by (Yang X, Pan T, Shen J, 2010).

These applications had difficulties such as low network bandwidth, multifaceted of mobile configurations and targeted suspicions activity that affect security parts of the mobile system. This type of applications is combined on the cloud computing system to tackle above mentioned concerns (Amit K. Sharma,2013).

Mobile phone devices are targets for theft and lost when using these devices as business tools; many confidential data are stored on them, many business applications installed on these mobile phones. It is very dangerous to keep all these data and applications without protection.

#### **2.1.3.2 Mobile banking applications**

Most of the worldwide banks are providing their customers with an application to monitor and access their account details using mobile banking application using internet or GSM to do a lot of processes and operations (E Turban, D King, J Lee, M Warkentin, H Chung, 2008) such as:

- check balances
- monitor transactions

- locate branches or ATMs
- Transfer funds
- Mobile top up
- Bill payment

The Bank of Palestine bank (BOP.com) offers many mobile banking services, one of these services is Banke application.

The mobile banking services vary depending on the nature of the channel used in mobile devices such as the following:

1. IVR
2. USSD
3. SMS

- (IVR): is short for interactive voice response services, it is considering an e-channel that banks use to facilitate to their customers to make some inquiries related to their banking accounts such the balance and credit card details. The process began by customer call IVR banking system and follow up the directions he/she hear through the call, sometimes can be shorted using a programmed menu and sometimes be transferred to call center agent based on nature of customers complains. IVR channel considers more expensive comparing with others banking channels [Banking\_Baraka Willy\_2013].
- [USSD]: is abbreviation to unstructured supplementary service data that used for multiple services such as callback service, location services, and mobile service. Banking depends on such this service to facilitate their customer to contact different banking channels for whom not own a smartphone such as old age peoples through programming menu. USSD is session based unlike other banking channels such as SMS. Both SMS and USSD lack of security aspects that should be addressed before using them mainly when they use in critical applications like financial services “Banks” and put all necessary security controls and countermeasure that make bank channels service more secures [Gadde Ramesh\_2016].

- (SMS): is a short message service with the format of a text message. Banks use this channel by allowing the customers to send SMS using their mobile devices to mobile banking application back-end server and reply to the customer with requested data within a specific limited character reach up to 160 characters' maximum. SMS channel used mainly as a form of alerts and notifications to bank customers and sometimes used in OTP as the authentication process. Moreover, SMS not guarantee to be delivered to a bank customer sometimes [(Kevin and Justin, 2008; Tibabu Beza,2018)].

[M. Niranjnamurthy,2013] subject was to study and analyze what the benefits, barriers, and limitations that mobile phone applications (E & M-commerce a) face in nowadays are. The researcher also discusses how much the growth of using these utilities to do their needs from buying goods in automated ways. Moreover, he displays what the right status of security subjects in this field such as authentication, confidentiality, availability, and privacy of data that has been exchanged between customers and service providers and financial services providers. In spite of this, the researcher did not provide any idea/s about how to enhance and increase the security issues in these systems.

[ R. O. Akinyede\_2010] subject was about how to secure customers PIN when serving online and mobile banking applications. Researcher builds a new way and framework to secure mobile payment transactions between customers, merchant, and bank (issuer or Acquirer). The framework uses a 3DES which is s a symmetric-key algorithm for the encryption and decryption of electronic data. In spite of that, the works suffer from insufficiency since he uses same encryption algorithm for encryption and decryption process that is easy can be compromised if one of sender or receiver has been hacked or attacked by external parties or person.

### **2.1.3.3 Mobile payment applications**

These applications using point of sale machines (POS) to transfer money between different parties such as person or companies or purchase a product from various merchants. These applications required that mobile devices have a feature of contactless devices to be enabled in both POS and mobile phones to process the

transactions within a very low distance that not exceed ten centimeters between these devices.

We have two types based on the structure of the transaction and third based on authentication service, one called proximity and second, call remote payments and third one biometric as describe below:

### **1- Mobile Proximity Payments**

This type sometimes called contactless payment that depended on a wireless protocol called NFC, so when the mobile connected with POS the data will begin transfer between them to the payment process and the distance should not exceed some od centimeters (Ecma International: Standard ECMA-352, 2003).

### **2- Mobile Remote Payments**

This type depends on two companies the banking application and mobile operator to process the cycle even is just exploring the customer accounts or also to do some transaction such as fund transfer or any other financial processes services, mostly using SMS or USSD services.

[Vanessa Pegueros,2012] discuss one of an essential line of business in financial organizations which are mobile banking and mobile payments applications. The researcher explores the security challenges facing these applications and how to identify, analyze and mitigate the risks of using these critical applications. Moreover, the researcher discusses the different type of payment solutions in different worldwide markets and recommend to adopt a rigorous risk mitigation solution depends on clear risk management standards.

[Kalkidan Gezahegn\_2016] study the social part of the usage of mobile banking application in the Ethiopian countryside and explore adoption model that reinforce his research. The research used two model for seeking the research idea, the first one is Technology acceptance and second is Innovation diffusion theory. Also, the study chooses some of the Ethiopian banking working in the country that offers mobile banking application. After analysis of gathering information from the field, the researcher concludes that perceived ease of use, trust and risk factors which are most

important factors that influence the adoption of mobile banking application channel comparing with others channels that financial institution present to their customers.

#### **2.1.4 Mobile with Biometric Recognition:**

The Biometric technologies can be classified as physiological and behavioral [Jasvinder Pal Singh, 2013].

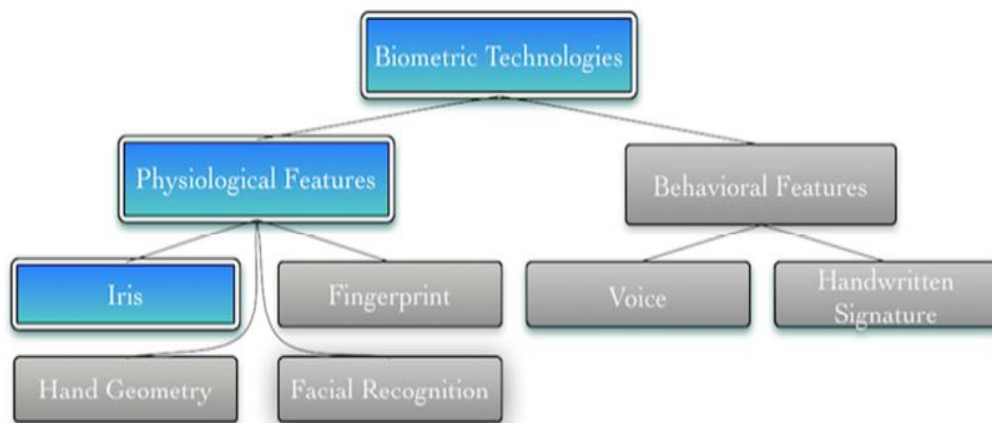


Fig 2.5 Biometric types.

Figure 2.5 shows different types of existence biometric services that most of the organization these days using some of these technologies or a mix of them at least to authenticate their customers when they try to access the banking applications through their mobile devices. These methods divide to two categories one as behavioral and one as physical that described as follows:

- Iris recognition.
- Signature recognition.
- Face Recognition.
- Fingerprint recognition.
- Voice recognition.

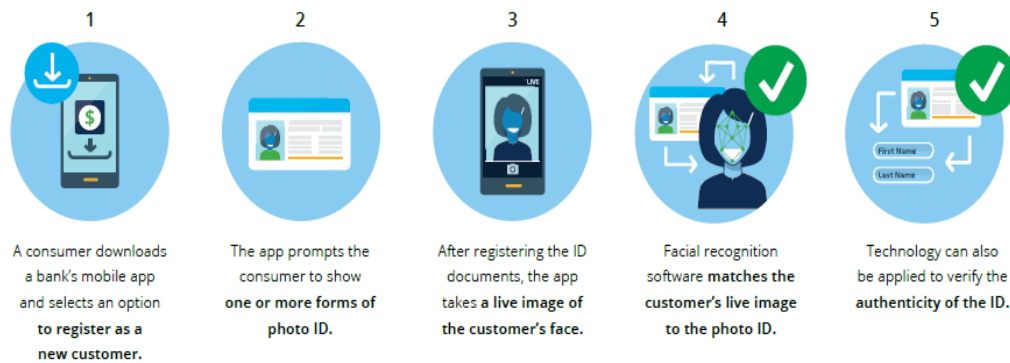
Most of the biometric authentication research has been increased because of the enormous improvement to sensors in new smartphones [Fridman, Weber, Greenstadt, & Kam, 2017].

[Sudana, Putra, & ARISMANDIKA, 2014] create a new technology using face recognition called Eigenface mechanism on mobile devices that operate under android system. The methodology used in these techniques is color segmentation plus pattern to form the recognition phase with accuracy reach up to 94 %.

[Smith-Creasey, Albalooshi, & Rajarajan, 2018] use a continuous image that produced by phone camera to protect the authentication process from spoofing attacks. The researcher use in addition to standardizing texture features lives face images through distance algorithm and LBP license detection techniques to avoid the spoofing issues.

Facial recognition considers one of a most robust method to enhance and apply the idea of getting rid of using passwords. Each time the client or customer need to login to an online banking application, it must capture the face of the customer to enable him to log in. Protecting from spoofing issues, the system needs to use special algorithms to analyze the face image of the customer and verify it is original not a copy of the photo or video images. The aware company says that all biometric of the customers should be taken before, then comparing with store images a patterned before permit access.

Face recognition is an excellent tool to register new customers without reach the bank branches or offices, this process is one of the life cycles for know your customer process (KYC). So, the banking clients need to enroll their face using a mobile device and no need to access the banking premises [Ahmad Tolba, 2005].



This biometric ID checking process is proving just as effective as if done by a bank employee. It is a convenient, secure way for customers to confirm their identities during the enrollment process without visiting branches. These facial images can be used for security functions in the future.

Fig 2.6 Enrollment Process

Figure 2.6 shows the steps for enrollment phase steps from 1 to 5. To improve customer experience of mobile banking application access “login”, this model of using biometric method instead of traditional passwords method can enhance customer convenience and also increase security issues, since the customer need to remember each time to access the mobile banking application the long password characters, so we replace it with face recognition to apply success of ease of use and improve the security aspects.

#### 2.1.4.1 Face Recognition:

##### Overview and different research history:

[Renu Bhatia\_2013] discuss biometric techniques that exist nowadays like iris, fingerprint, voice, and face recognition methods and where to use these techniques in a different line of our lives such airport, prison, forensic and accessing banking applications. The researcher also discusses how biometrics differ from each other from various aspects, the accuracy, user acceptance, stability, ease of use and error incidence. Moreover, the researcher built a comparison matrix for these aspects and come with the result that face recognition is highly considered, reliable and accurate to be used in security access and replace traditional methodology such as using a password. The research topic will be recognized as one of the resources that we will use in our thesis.



Biometric tactic uses different of user characteristics [Ahmad Tolba, 2005] one of them is using the face of the end users or customers that called face recognition method, this method becomes increasingly used these days because of ease of use, but it is still vulnerable of using fake faces. Spoofing attacks that come with using this method can be solved by using liveness detection tactics that will be explored in the next section.

#### **2.1.4.2 Liveness Detection – Face Recognition:**

This method that called liveness detection [tactic used in all biometric space such as fingerprint, voice and face and so on. The process will create a profile depend on human characteristics of his or her face and create a dedicated pattern consists of a group of parts include face lines, eye blinking and lips moving and so on [Saptarshi Chakraborty, and Dhrubajyoti Das, 2014]. This way will try to avoid spoofing techniques using fake photo and fake video or even using the 3D face of the user's face that will try to access the application. Using liveness detection within a face recognition phase will improve and enhance the security level of authentication and authorization the customers when trying to locate their mobile banking application as we try to do in this thesis.

Below items describe a different type of detection with their advantages of using liveness detection method.

#### **Advantages:**

- The texture will be easy to use
- Hard to spoof by a fake photo of the user's face
- Hard to spoof by a fake video of the user's face
- No need for user intervention
- Independent of face texture

There are two types of categories to detect the liveness of the agent who will use the mobile application using face recognition method. The first type shows how the customer will contact and access the mobile banking application using face images to his face and it can add some challenges when the customer tries to do some movement to his face. The second type by change some parts of his face such as

blinking to his or her eye, or move the lips and so on. If the pattern of images matches the customer can access the application otherwise the clients cannot access. 3D images consider more robust and more secure than 2D face recognition and consider less spoofing.



Fig 2.7 A generic face recognition system

Figure 2.7 shows a generic face recognition process phases which begin with face detection, face extraction, and face recognition; below sections describe each process in detail.

#### **2.1.4.3 Face detection:**

Facial components will be identified and compared with information on main database container, then taken image will be divided to two parts one with the texture of the face of the user and one for background effects of the image then create image template or profile that will be used on next phase which as face recognition.

Then, compare two images then the output will be created face map that enables the customer as a validated process or not.

#### **2.1.4.4 Face Extraction:**

This method will try to extract some information of face components such as nose, mouth, and eye and study the geometry of the whole face to create a template that will also be used the information from the first phase of detection.

#### **2.1.4.5 Face Recognition:**

This phase will take the final one that combines both the identification and validated the stored images of the customer with current live face image when the customer

tries to log in to the mobile application if it is matched then access will be given otherwise is deny. [Avinash Kumar Singh\_2014].

Reference's [Renu Bhatia\_2013] discuss biometric techniques that exist nowadays like iris, fingerprint, voice and face recognition methods and where to use these techniques in a different line of our lives such airport, prison, forensic and accessing banking applications. The researcher also discusses how biometrics differ from each other from various aspects, the accuracy, user acceptance, stability, ease of use and error incidence. Moreover, the researcher built a comparison matrix for these aspects and come with the result that face recognition is highly considered, reliable and accurate to be used in security access and replace traditional methodology such as user a password. The research topic will be recognized as one of the resources that we will use in our thesis.



Fig. 2.8 Samples of Spoof Images

Figure 2.8 shows the differences between real and fake face images for the customer.

#### **2.1.4.6 Face Recognition Mechanism:**

Any biometric system consists of two parts; the first part is enrollment and the second part is recognition. We use face techniques in this research to meet with user experience expectation and create a new channel of bank account opening and minimize the need of the customer to reach the bank's offices. Also, using biometrics such as face recognition make accessing sensitive application more secure based on multiple factors of authentication (Deepak S, 2015).

Biometric systems have the lowest error rate based on (Anil K. Jain, 2015). Face recognition method has a low error rate for both the identification phase and

verification phase. Identification phase we use, FMR and FNMR rates, to measure the accuracy of the images captured during this phase. Meanwhile verification phases we use FPIR and FNIR to measure the accuracy rate in this phase.

➤ Face Recognition SDK flow:

We choose Zoom SDK to implement in this research to simulate the face recognition phase. Zoom is a product for Face Tech company for liveness detection that established a solution depends on AI techniques to capture human face characteristics and compare them with real stored images, which solve the weakness that is found using the traditional way of passwords [Avinash Kumar Singh, 2014].

Flow process begins to identify user's face features such as nose, mouth, eye, hair, and so on, in addition to background environment keeping mobile camera in moving by users to catch the all changes that will happened to these features within (20s – 30s) as a maximum allowable accepted period , then create 3D profile for user face to be used in process of registration, enrollment, authentication and verification phases.

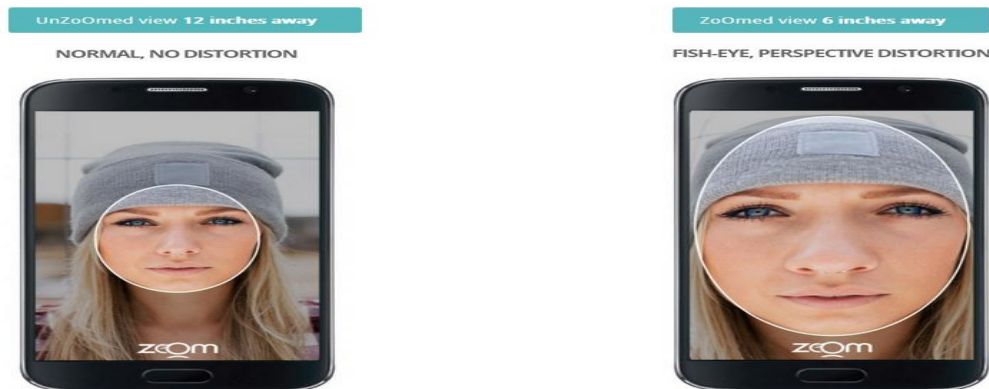


Fig 2.9 Image Capture

Figure 2.9 shows the trial capture image that will be produced using mobile devices

#### 2.1.4.7 Old Biometric techniques still weak:

- Old biometric technologies still using traditional easy to capture the user features and do not depend on liveness detection tactic.

- If liveness exists, still using simple methods that depend on simple details such as blinking eyes and lips movements that can be easily spoofed using a photo for the user.
- New designed techniques used by Zoom can stop most of all threats.
- Can be used for high and critical applications such as financial transaction using mobile banking and internet banking applications.

➤ **Spoofing Methods:**

There are three methods to spoof face recognition:

1. Picture or photo as 2D for a user.
2. Video in motion for a user.
3. 3D photo or video for a user.

Our proposal using ZDK form Zoom can eliminate all these threats even using 2D paper photos & digital images like:

1. High-end resolution images.
2. Photos or video avatars
3. Sleeping users.
4. Identical twins

So, the output of using such these techniques cannot be spoofable when user try to access by an attacker to reproduce same media or video using top technology tools available in the market [Avinash Kumar Singh, 2014].

➤ **Image Cloud Storage:**

1. The image once taken is stored in the cloud storage in Zoom.
2. Then, will be sent to the private bank database.

#### **2.1.4.8 Face Recognition Algorithms & SDK:**

ZoOm Hybrid Authentication [Avinash Kumar Singh, 2014] merge device and server-side features to be run over image data stored in the cloud that will use for Mobi-cash application. SDK biometric represent face map that takes from live video up to 3 seconds as biometric data.

## **2.2 - Cloud Computing Technologies:**

### **Cloud Computing Overview:**

Computing is the study of how the process of utilizing computer technology to design and build a CS includes both hardware and software to collect a various type of information.

There are several and different types of computing that vary depending on structure and services that they offer, such as distributed computing, cluster computing, utility computing, grid computing, cloud computing, edge computing. The increasing demand for Internet and increasing computers power and high speed of networks bandwidth, in addition to the lower cost of product components, are changing how we can use this computing. Internet, Parallel computer and distributed system begin a new era of cloud computing.

Cloud Computing have two type of services, one for deployment topology and second for service delivery as describes below:

- **Deployment Models:**

Describe the way and methods of access to the cloud and where the cloud is located from geographically respective. Cloud types consist of four categories: Public, Private, Hybrid, and Community [Carlos Rompante, 2017].

- **Service Models**

These models define how the end users can access the services, different types of modules which are SAAS, IAAS and PAAS [Carlos Rompante, 2017].

### **2.3 CC & MCC threats and Vulnerabilities:**

There many vulnerabilities using cloud computing technologies besides the benefits of using it. We will present some of them that our thesis will face and how we will solve it by introducing ways of mitigation process cycle [ Pericherla Satya Suryateja, 2018] and [Qijun Gu and Mina Guirguis,2014].

[Sarang V. Hatwar,2015] discuss cloud security from all aspects and explore most of the vulnerabilities at cloud computing environment and suggest countermeasures to protect from each of these threats. Also, the researcher investigates the open stack concept that used in a cloud computing environment. Moreover, most of the discussed vulnerabilities have been picking up from cloud security alliance research.

We will study and analyze some of the related works in both cloud, and mobile cloud computation security issues based on vulnerabilities & threats list as below:

- Session hijacking
- Reliability and availabilities of cloud services
- Insecure Cryptography
- Organization data protection
- Cloud Structure model
- Insecure API
- Malicious Insider and outsider
- Data loss and data leakage
- Identity Theft
- Device theft
- Virus attacks
- Virtual machine attacks
- Misuse of Access rights
- Limited resources
- Low Bandwidth
- SMS Attacks
- Communications channel attacks

#### **2.4 Compliance:**

Data and information of an organization for their customers should be kept safely and securely. Banks must follow international industry standards and comply with regulations to meet with these requirements.

Reference's [Jalil Totonchi, 2010] focus his research on speaking about how much the importance of protection financial services application such as mobile banking that used as a payment gateway for banking customers. Also, he discusses what are the capabilities and limitation using such these application from security perspectives — the researcher focus to address the security issues in mobile banking applications from risk, regulatory and legal

aspects. In spite of this, the researcher did not give theoretical or practical solutions to tackle security issues in mobile banking applications.

[Imran Ashraf,2012] discuss the security controls and actions that have been taken to address security issues of mobile banking application and to divide them into multiple categories. The researcher also explains some threats that face each of users, mobile devices, banking application, and governance. Moreover, the researcher explores the type of mobile banking application such as SMS and mobile website banking. In spite of that the research discusses mobile banking environment from audit perspective even, he addresses security issues of the mobile banking from multiple security aspects begin from the user, application, data, and end of risk aspects.

In Palestine, the authority's organization for financial service is PMA that issue and circulate their instructions to these institutions to keep people information and their money in a secure place. Moreover, industry regulations also should be addressed and need to be followed, the essential standards for the financial organization are PCI (Jing Liu, Yang Xiao, 2010). Payment card industry considers a form of minimum standard for data security required to comply with it and contains 12 requirements and over 300 of controls as shown in below table 2.1 of PCI-DSS requirements.



Table 2.1 PCI DSS Requirements

<b>Control Objectives</b>	<b>Security Requirements</b>
Build and Maintain a Secure Network	<ul style="list-style-type: none"> <li>• Install and maintain a firewall configuration to protect cardholder data</li> <li>• Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ul>
Protect Cardholder Data	<ul style="list-style-type: none"> <li>• Protect stored cardholder data</li> <li>• Encrypt transmission of cardholder data and sensitive information across public networks</li> </ul>
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> <li>• Use and regularly update anti-virus software</li> <li>• Develop and maintain secure systems and applications</li> </ul>
Implement Strong Access Control Measures	<ul style="list-style-type: none"> <li>• Restrict access to cardholder data by business need-to-know</li> <li>• Assign a unique ID to each person with computer access</li> <li>• Restrict physical access to cardholder data</li> </ul>
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> <li>• Track and monitor all access to network resources and cardholder data</li> <li>• Regularly test security systems and processes</li> </ul>
Maintain an Information Security Policy	<ul style="list-style-type: none"> <li>• Maintain a policy that addresses information security for employees and contractors</li> </ul>

**Summary:**

We review a lot of previous works in the field of cloud and mobile cloud computing and shows what are the different types of payment system platforms like mobile banking and mobile payment. In addition to highlight of critical issues in mobile payment system from security perspectives that contains most of threats and vulnerabilities.

## Chapter Three

### 3. System Analysis

#### 3.1 Current Systems:

Most nowadays banking operations are done using the bank local servers only, but in the proposed system, the banking operations will have used a hybrid model that some of the infrastructure components are using through cloud services like Microsoft Azure with off-premise private cloud and some of the others using the bank local environment servers as On-premise cloud depends on the demand for each feature or operation.

#### ➤ **Mobile Banking Application in Palestine:**

Based on PMA report [PMA Payment System, 2013] that describe the status of banking sectors in Palestine, state that we have 15 working banks, seven local banks, eight foreign banks with almost around 300 branches in offices, 500 ATM, 5000 POS, and 60,000 credit cards. PMA has their cash incoming as below image. The report also shows there are 1- 4 ATM for every 10,000 people which still consider low comparing with most of the world countries and that because of political issues caused by the Israeli occupation. So, this is why I choose my thesis to be one of aspect to enhance the Palestinian situation in term of payments and commerce.

The mobile application becomes one of the essential pillars to push the idea of financial inclusion in Palestine and the best way to reach all people.

Most of nowadays applications use traditional way to authenticate users with ID and password that needs to keep remember the password each time when he or she needs to access the mobile banking application and sometimes use a weak password that exposes the user for a lot of threats such as man in the middle and phishing attacks that leads to stolen the password quickly.

Banks try to enforce the users to use a complex and long password to protect the users from such these attacks, and the whole process becomes complicated and not user-friendly and not very secure to use.

The main difference between mobile payment and mobile banking is in the way of transferring money, Mobile banking is a part of electronic banking doing financial

transactions which the customer uses mobile communication techniques in conjunction with mobile devices' [Barati & Mohammadi, 2009] & [Pousttchi & Schurig, 2004].

Mobile payments alternatively, are a way to pay for goods in online shopping sites using a mobile device, while mobile banking is based on the banks own systems and infrastructure [Mallat , 2006]. An example of mobile banking is accessing the internet banking site of a bank using the phone's web browser or a dedicated application installed on the mobile phone.

Two factor or multiple authentications have been a rise to solve such these issues using customer information that has been knowing or have our own, such as pin cards and biometric service like a fingerprint and face images of the customers.

### ***3.1.1 Issues with the current system design:***

- Deficiency of security of data.
- Data needs high availability.
- Authentication methods for the transactions must be reliable in the whole process of the Authentication phase.
- More latency.

### **3.2 Proposed System (Mobi-Cash)**

The proposed system is developed to improve and enhanced its functionaries and overcome and solve all issues that described in the above section.

Mobi-cash focuses into four categories (Mobile, application, Service Providers, Data Center(network, host, storage, OS)).

#### **➤ Mobi- Cash as Mobile Banking Application:**

Mobi-cash in the cloud in conjunction with ZoOm On-Device SDK provides several advantages over device-only authentication:

- 3D depth, and liveness detection
- The real-time video feed from the camera
- Security controls are shared with the application
- User-Friendly

- Multi devices and multi user's configuration
- The application is controlling the authentication system
  - Requirements:
  - Device Requirements:
    - iOS 8.3
    - Android 4.3
  - The application must include the standard ZoOm SDK Version 6.1
    - Cloud / Server / Cluster Requirements
      - Ubuntu / RedHat/ CentOS
      - Development and small Production environment (up to 20 authentications/second)
      - Large-scale (up to 100+ authentications/second)
    - Generating Encryption Keys
 

Set up your encryption keys, using Public Key Infrastructure PKI using public and private keys.
    - On-Device Enrollment and Authentication:

#### 1. Initialization

Initialization launches a network transaction to verify the app token license.

#### 2. Enrollment

Enrollment is the first step and called registration, so it is the process of capturing a base face map associated with the user. A base face map can be obtained from either the Enrollment or Verification modes. Key elements when deciding between using Enrollment Mode and Verification Mode:

- To set up a purely server-side authentication solution, it is recommended to use Verification Mode. We recommend this as it does not create a facemap and store it on the device, which is unnecessary if you are only doing server-side authentication.
- To also perform matching on the device, use Enrollment Mode.
- Both modes allow you as the application developer to retrieve the face map from the result object.

#### a) Authentication

Once the user has successfully enrolled and has biometric data securely stored on the server, you can kick off an authentication flow at any time. To perform server-side authentication only, use Verification Mode with retrieve Zoom Biometric flag set to true to attempt to authenticate the user. Note, you can also use Authentication Mode if the user is enrolled on the device to perform authentication on both the client and server (and on the client only for offline, poorly networked, or other use cases).

#### b) Mobi-Cash Face map

The face map can be accessed on the standard response objects. Once the face map bytes are obtained, the application is responsible and has full control over how this data is uploaded.

##### ➤ Performing User Authentication on Cloud:

On the cloud server/cluster, after receiving the Mobi-cash face map saved on the cloud then lookup begin fetching for user face profile.

#### a) Initializing

The initialize calluses your app token and server token to validate the SDK and sends some usage data to off-premise cloud servers like the version of ZoOm SDK being used and the OS it is being run on. Calling initialize is required to use other functions of the SDK.

#### b) Performing Face maps Comparison Matching

As an example of how you would initialize ZoOm Hybrid and compare two face maps that have been captured from the device.

#### c) Generating Face maps from a Single Image

We can create a Mobi-cash face map from an image. Off-premise server will return a user face map as long as it determines that the image can be used for authentication. To generate this, do the following:

#### d) Verifying Face maps

We can also obtain the necessary information from the face maps being used by your application. The possible types of a facemap are:

- Device: A Face map that was created using a Mobi-cash app on the device.

- Image: A Face map that was created from an image.

➤ Important security notes regarding face map verification:

The ZoOm SDK library functions that operate on face maps assume that these face maps have been encrypted and generated by unaltered code generated by the Mobi-cash iOS or Android SDKs. It is conceivable that, since the Hybrid APIs accept arbitrary data, that malicious data can be constructed and submitted to the Hybrid APIs with the objective of crashing the process, leading to a potential denial of service attack. To prevent such attacks, Face Tec recommends that at a process outside the primary process performing authenticate calls to be set up in a sandboxed fashion for the specific purpose of checking for the validity of face map data using the get face map Info valid API. This way, a system can be architected that can continue to operate on well-formed face map data despite the submission of lousy face map data to perform a denial of service attack.

a) Preparing Face maps

ZoOm SDK keeping Mobi-cash software is always being updated with the latest and greatest recognition models.

b) Verifying Face maps

You can also obtain relevant information from the face maps being used by your application. The possible types of a facemap are:

- Device: A Face map that was created using a Mobi-cash app on the device.
- Image: A Face map that was created from an image.

➤ Getting Liveness Result from Face maps

To retrieve liveness result from a face map.

➤ Getting Metrics from Face maps

To retrieve metrics from authentication such as match score or if Mobi-cash detected the user was wearing glasses from authentication results or face map creations.

➤ Continuous Learning

Upon successful authentication, you may obtain a new Mobi-cash face map that will improve performance over time.

There are two scenarios where a new face map will not be available on the Mobi-cash Authentication Result object

- Authentication failed.
- Either of the face maps passed into authentication was generated from a single image.
- Hardware Requirements and Benchmarks:
  - Web/Upload Server Resources: Each authentication Mobi-cash face map is ~50-100KB.
  - Storage of Face maps: Storage of Mobi-cash face maps will presumably be done in a database.
  - Face map Compare Time: Mobi-cash face map Comparison time will rely on CPU hardware setup. Mobi-cash authentication times will be in the 3-30ms range, per processor on most modern, mid-grade processors.

### **3.2.1 SMS & OTP Algorithm:**

#### **➤ OTP:**

(TOTP) [Emiliano De Cristofaro, 2014 ] is a one-time password, is an algorithm that calculates the password from a shared secret key and the current time. TOTP is a hash-based code called (HMAC). It consists of a secret key with the current timestamp using a cryptographic hash function to generate a one time password.

Google Authentication tool is designed by generating an HMAC-SHA1 token, which uses a 10 byte encoded shared secret as a key and separated into a 30-second interval as inputs. The Output results are 80-byte token changed to a 40 character hexadecimal string; the least significant hex digit is then used to calculate a 0-15 offset. The offset is then used to read the next eight hex digits from the offset. The resulting eight hex digits are then AND'd with 0x7FFFFFFF (2,147,483,647), then the modulo of the resultant integer and 1,000,000 is calculated, which produces the correct code for those 30 seconds (George Watkins, 2011).

Reference's [Wencheng Yang\_2013] that use OTP mechanism and proposed fingerprint and its vein as a biometric form to authenticate users when using mobile payment application. The researcher about the barriers of using biometric techniques

from technical and social perspectives. Technical part deal with how security levels in biometric templates and recognition accuracy, from on other hand social parts explore what level of acceptance of use for the end user to replace their password with biometric types such as fingerprint, face, and iris. Moreover, researcher injects OTP techniques to be added at the infrastructure level of the biometric cycle. In spite of this, the research did not discuss others security issues such as mobile, mobile banking applications and banking environment.

➤ **TOTP Algorithm:**

The current timestamp is twisted into an integer time counter (TC) by defining the start of (T0) till (TI). For example:

$$TC = \text{floor}((\text{unixtime}(\text{now}) - \text{unixtime}(T0)) / TI),$$

$$\text{TOTP} = \text{HOTP}(\text{SecretKey}, TC),$$

TOTP-Value = TOTP mod 10d, where d is the desired number of digits of the one-time password.

**SMS:**

We use an open source SMS gateway that provides services of messaging from the local Palestinian company “ MTC company based in Gaza.”

Other tools that have been used in our solution will be described below in next sections for hardware and software tools.

➤ **Cryptography**

the original form of a message is called plaintext (P), and the encrypted message form is called ciphertext (c). The encryption process is formed to transfer plain text to cipher text, and a decryption process is a form of transfer from ciphertext to plain text. Basic operation with and without encryption and decryption keys are illustrated as follows:

- 1- Encryption  $\rightarrow C = E(P)$
- 2- Decryption  $\rightarrow P = D(C)$
- 3- requirement:  $P = D(E(P))$  – without keys
- 4- Encryption key: KE



- 5- Decryption key:  $KD$
- 6-  $C = E (KE, P)$
- 7-  $P = D (KD, E (KE, P))$

➤ **Advanced encryption standard (AES)**

AES symmetric algorithm is a repeated block cipher with a fixed block length of 128 and a variable key length. We use this algorithm to encrypt and decrypt the draft stored in a storage container in both on-premise and cloud environment to ensure confidentiality and integrity of data.

**3.3 Benefits of the proposed system design:**

- Reduces the time and the effort of the traditional banking operations.
- Reliable authentication methods for the transactions.
- High availability.
- Minimize the latency.
- Greater efficiency.
- User friendliness.
- The data will reduce data damages.
- Bill payment.
- Mobile Top-Up.
- Fraud security.
- Subscription fees payments.

**3.4 Software development on Mobile Applications:**

As in Software development life cycle, any software application will pass through these phases to set up the application [H.K. Flora,2014].

1. Planning
2. Analysis
3. Design
4. Implementation
5. Testing
6. Validation

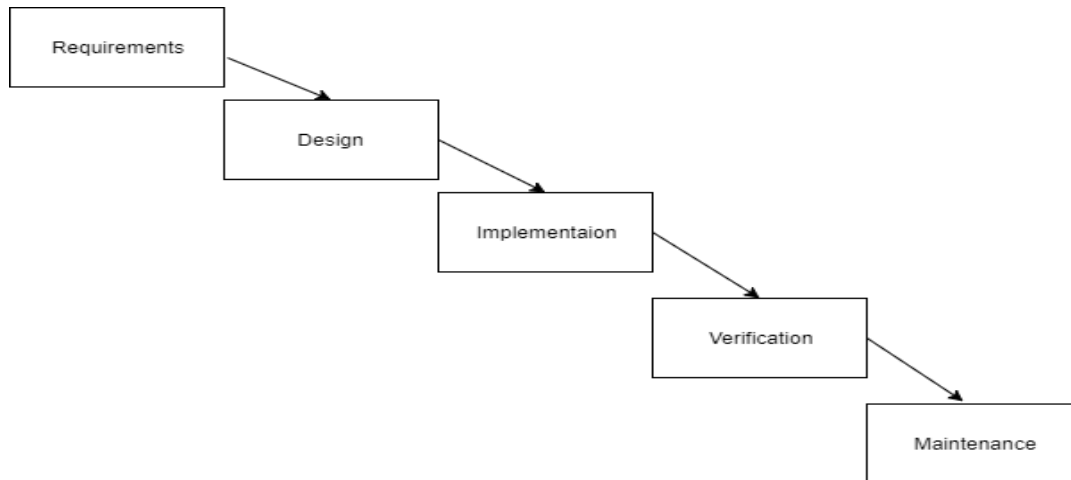


Fig. 3.1 Software Architecture Diagram

Figure 3.1 describes software architecture phases to build and develop mobile banking application. Also, we inject agility process “**Agile Development - Scrum**” in the building of our software mobile banking application to satisfying customers’ needs and absorb all required changes to our proposed solution.

### **3.5 Mobile Devices:**

As we intend to develop a new mobile banking application, we should give a brief about these mobile devices types and their operating system that existing right now.

- **Mobile Phones:**

All these mobile devices that use for only SMS and calling and does not contains any other features such as cameras and video and gaming and consider has low-end mobiles that use just for primary users.

- **Smart Phones:**

These services work as mobile phones and Mobile technologies such as 3G. Also have many features such as multitasking operating systems, high-resolution cameras with video recording capabilities. These devices that we will target them in our thesis for a banking application.

#### **3.5.1 Mobile Devices Operating System:**

Most smartphone device OS is using IOS such as in Apple mobile devices, and others using Android such as Samsung and Huawei, and other such as

windows mobile. These operating systems OS [Ganiyu Rafiu Adesina, 2014] some of them as open sources like Android and some of them, are paid such as like Windows mobile. IOS and blackberry are proprietary to their mother companies.

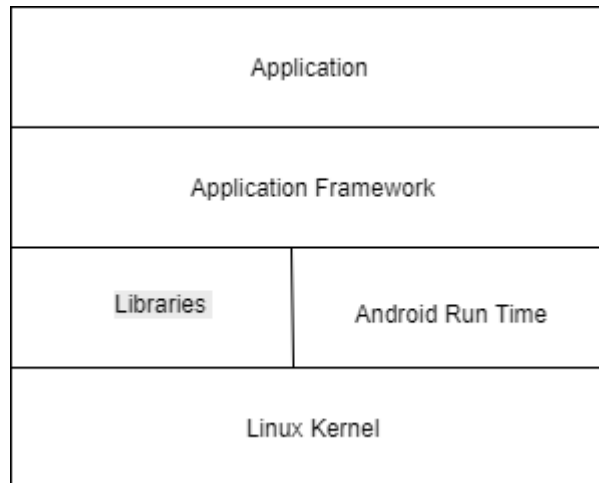


Fig. 3.2 Android OS Kernel [Ganiyu Rafiu Adesina, 2014]

Fig 3.2 shows the OS kernel for the mobile Android platform that we will use and depend on it in the thesis that consist application, framework, libraries, android run tome, and Linux kernel.

### 3.6 Feasibility Study:

It is a survey made before beginning a project and must lead to a decision for:

- Proceed in the project
- Stop the Project
- Re-think to do more studying

Sometimes need to check if the project requires a proper budget and need to build the appropriate team to do the project with objective met with time plan of the project.

Benefits of this study are to show how the strengths and weaknesses of an existing solution and proposed the proper solution which is the objective of this thesis.

Significant feasibility components Study is:

- Technical Feasibility
- Financial Feasibility
- Resources and time Feasibility

- Risk & Legal Feasibility.

### **3.6.1 Technical Feasibility.**

The software of mobile banking application will be developed to cover all required functions and excluding all limitations. The major components are the mobile software tools that used to build and develop the software such as HTML, MYSQL, CSS, JavaScript, PHP, Laravel.

### **3.6.2 Financial Feasibility.**

Mobi-Cash developed by the very lowest cost using different open source software and programs and mix than in a new model of infrastructure using a hybrid cloud environment as in chapter 4 Table 4.1 of hardware and software requirements.

### **3.6.3 Resources and time Feasibility**

- Mobile devices
- Payment methods
- Cloud computing
- Laptop
- Draw.io

For the public cloud we used Microsoft Azure, and for the private cloud, we have used Linux based server and some security solutions like Mod-Security.

### **3.6.4 Risk & Legal Feasibilities:**

This section of the study has many contexts such as:

- Size of software regarding the number of line codes
- Size of software regarding the number of programs
- Size of regarding the database

### **3.6.5 User & System requirements:**

Hardware and software requirements and specifications that should include the software provider and constraints which it should be operating in, and it is consist of following:

- Mobile Phone
- Public Cloud
- Private Cloud
- Laptop

- Oracle VM
- Software development tools

#### **3.6.6 Functional requirements:**

It describes how the system will behave to deliver the required output and respond to system inputs and how to act in term of the following subjects:

- User authentication.
- Payments
- Transactions
- Transfers
- Register and create accounts

#### **3.6.7 Non-Functional requirements:**

It is described what the system services issues will be regards some of the system constraints such as following

- Security
- High availability
- Reliability
- Scalability
- High performance
- Timing
- Development process & Standards

#### **3.6.8 Domain Requirements:**

It describes from where the problems or issues can come from even it is functional or non-functional. Such as following:

- Speed
- Size
- Ease of use
- Relatability
- Robustness
- Portability

### **3.7 Mitigation methods to tackle most of the Vulnerabilities and threats of cloud & Mobile Cloud computing:**

#### **Threats:**

##### **1- Session hijacking:**

That happens by using or stealing cookies and customer or end user's credentials to gain unauthorized access to remote servers and application that customer use to serf his/her web or mobile application.

[X. Zhang, 2009] proposed a new framework and mode for elastic application to be used between mobile devices and cloud

This type of attack can be mitigating by using a strong authentications service such as we proposed in the thesis using biometric authentication service "Face Recognition."

##### **2- Reliability and availabilities of cloud services:**

Infrastructure service can be a blackout and suffering from unavailable at some or certain time such what happened to [Amazon at 2008] that will affect the end user usage of the system that these clouds provide. Some cloud providers also suffer from of weak change management that affects a directly to the end-user behavior of their software's such as happened to [Microsoft Skype service in 2018].

We propose to use the hybrid model of investiture components to serve the available by using private and public cloud scenarios.

##### **3- Insecure Cryptography:**

Most of the cloud environment could or may use improper cryptography algorithms that enable hackers to interrupt their traffic and figure out how to breach it such VMware servers even in windows or Linux platforms.

Cloud provides.

[T. Meng, 2015] proposed a method to transfer computing parts from mobile devices to the server side. Timing attacks are most concerns in this research since encryption techniques cannot be protected by such these threats unless

using a new offloading method such as the research use. Also, the researcher uses quantification analysis to evaluate the proposed system.

[P. K. Tysowski, 2013] introduced new key management system to secure data between mobile devices and mobile cloud environment.

Public cloud providers use their encryption keys, but in our model, we use our certificates such as Comodo (mobile – API cloud), Comodo (API – API), SSL/TLS Zoom login certificate (Mobile – Zoom API).

#### **4- Organization data protection:**

Most of the companies that go and use cloud environment forget in most cases to be sure what they will do when the engagement with a specific cloud provider and what about their data in use in term of privacy and security. This a massive data breach most of the client forget to tackle it.

[Y. Yu, 2014] proposed a secure protocol that used both of asymmetric key and proxy signature to guarantee the integrity of data that has been transferred to cloud storage by the end mobile user devices.

Most of the companies that go and use cloud environment need to be sure that they have a very strong SLA between them and has a proper validation and verification processes.

#### **5- Cloud Structure model:**

Most of the cloud providers sometimes change their IT service delivery such as servers, storage and so on, so that the end user may lose their control of this service and expose their data and service for breaches and out of service.

[M. Ali, 2015], a proposed a new model to secure data sharing between user's storage cloud environment, this model was named by the researcher as SEDAC.

We use at least two cloud service providers, such Virtual private server that we use it from Aruba and Azure.

#### **6- Insecure API:**

Most of developer and cloud providers use Cloud API to let programmer set up their interfaces to use in their framework and system design, some of these

API use clear text authentication and body of transaction that exposes the end user to disclose their private information.

[L. Tang, 2015] proposed a new security mechanism to secure web API service to ensure an end to end security in mobile cloud computing

To mitigate these issues, we use Cloud flare WAF, Data log management and monitoring, Comodo Certificate for API.

#### **7- Malicious Insider and outsider:**

Most clouds protect from an external malicious process using an antivirus and Malware software's, but the weak point comes from an insider that can have access to confidential information without proper privileges even the cloud providers can present some solution such firewall and intrusion detection system, but the misconfiguration and tuning is the biggest issue in these systems.

[J. Tan,2014] proposed STOVE model which is abbreviation to strict, observable, verifiable data and execution models to secure mobile devices and their OS and application from unwanted or malicious programs.

To mitigate such these threats for malware and virus that may face multilayer of the proposed solution we add following programs to minimize such these threats.

(AV for Mobile. AV at Server, AV workstation we use a Kaspersky, and for logging & monitoring and SIEM we use an elastic stack,)

#### **8- Data loss and data leakage:**

This threat considers the most critical issue of using cloud environment since client information exposes of lost because improper backup solution and leakage because missing monitoring system that reviews all data in and out of client systems.

References [D. Popa, 2013] Proposed new framework to secure data in transit between the mobile cloud computing application components such as mobile devices and mobile cloud application.



To protect our solution from such these threats, we are using token in DB, SIEM, FW, Access list.

## **9- Identity Theft:**

Is a considers one of the shapes of fraud techniques that used to trick the user and use his or her credentials to access the end user private information? Some of these issues come from using very weak password m keynoters or phishing attacks to a cloud environment.

[A. N. Khan, 2013] proposed a light version of security mechanism to secure the mobile user's identity using dynamic credential from different dedicated attacks of password guessing methodologies.

Our module to protect when the device is stolen or lost, we use Face recognition, SMS utilities to protect mobile banking application and Two-factor authentication from Google OTP to safeguard internal users "Banking employees."

## **Vulnerabilities :**

### **1- Device theft:**

Many customers expose to lost or stolen their devices, so their data will be disclosed to unauthorized users and leak confidential information. Therefore geolocation can be protected from such this threat.

[H. Zhang, 2015] Proposed new model for location-based service by introducing a trust proxy server to access by a mobile node before access LSB server.

We use a Pin code application, Face recognition, SMS.

### **2- Virus attacks:**

Mobile devices and their applications expose to be infected by malware and viruses that can harm the end users that use a very critical application such as internet banking and others.

[Kevin Curran, 2015] Proposed security mechanism cover mobile devices threats.

Our Mitigation approach we use a Kaspersky software to protect client and server side such as Mobile devices, Banking teller station, Server in both premise and cloud environment).

### **3- Misuse of Access rights:**

Mobile devices need to be configured very well to activate pin access to the mobile devices and especially to critical applications installed on the mobile, so sometimes these applications can steal their credential and give unauthorized access to vital information.

[F. A. Alvi,2015] also discuss some security problems using a cloud computing environment and explore what the most challenges facing cloud computing are.

Mobile devices need to be configured very well to activate pin access to the mobile devices and especially to critical applications installed on the mobile, so sometimes these applications can steal their credentials and give unauthorized access to critical information.

We use to add to pin access a SIEM elastic stack search tools and logging & monitoring to validate user and interface access rights for the mobile application and 2FA from Google OTP for web application access by banking employees.

### **4- Limited resources:**

A mobile device that already created to be used for calling aspects, after the revolution of smartphones, is considered to work as mini laptops, so most mobile devices suffer from limited resources for all computing resources.

[S. Kungspisdan,2005] research subject was about the constraint of wireless communication using mobile devices that also suffer from low computing resources.

Our mobile application, in general, uses a less resource from web application by using restful between Mobi-Cash API, Zoom Login API.

### **5- Low Bandwidth:**

When using mobile devices to surf the internet and used some applications such banking application suffer from low bandwidth because of both limitations on low device power and low bandwidth even using Wi-Fi or 3G connectivity that will reflect poorly of use and complicity to handle such critical process such financial transactions.

Reference's [ Liu Jinsheng,2013] subject was about to build and design a new identification recognition system for mobile payment system using J2ME over wireless public key infrastructure WPKI and do reciprocal authentication between customers and banking payment gateway.

This factor considers the most benefit of using cloud solution to overcome bandwidth issues using mobile application.

### **6- Communications channel attacks:**

Most of the mobile cloud solution expose to many attacks that block using their applications on communication level (AAAD) such as:

- Access-Control.
- Authentication
- Availability
- Data-Integrity.

[H. Wang,2014] proposed a solution to address some of security and privacy between the user and cloud environment for media exchange between them.

Our web application that uses by banking employees, we use a 2FA Google OTP as mitigation for such these attacks, additional to WAF tools.

### **Summary:**

We analysis current banking applications used in payment system and proposed new model to handle all issues facing payment system at three levels, environment using hybrid cloud; security and compliance.

Moreover, we use scrum agile development process cycle to build and design of our system structure.

## **Chapter Four**

### **4. System Design and Implementation**

Based on deep learning and study of different methods, techniques and algorithms concerning our major problem we inspire our approach. (Mobi-Cash).

Mobi-Cash is mobile banking application that developed to improve and enhanced its functionalities and overcome and solve all issues facing cloud model architecture and designed to use On-premise and an off-premise cloud environment to build the mobile application. Also, it is addressing most of vulnerabilities and threats facing mobile cloud security aspects and divide into four categories (Mobile, application, Service Providers, Data Center(network, host, storage, OS)) and achieved most of below key elements of this new model. As Shows in Figure 4.1.

- Reduces the time and the effort of the traditional banking operations.
- Reliable authentication methods for the transactions
- High availability
- Minimize the latency
- Greater efficiency
- User friendliness
- The data will reduce data damages
- Bill payment
- Mobile Top-Up
- Fraud security
- Subscription fees payments

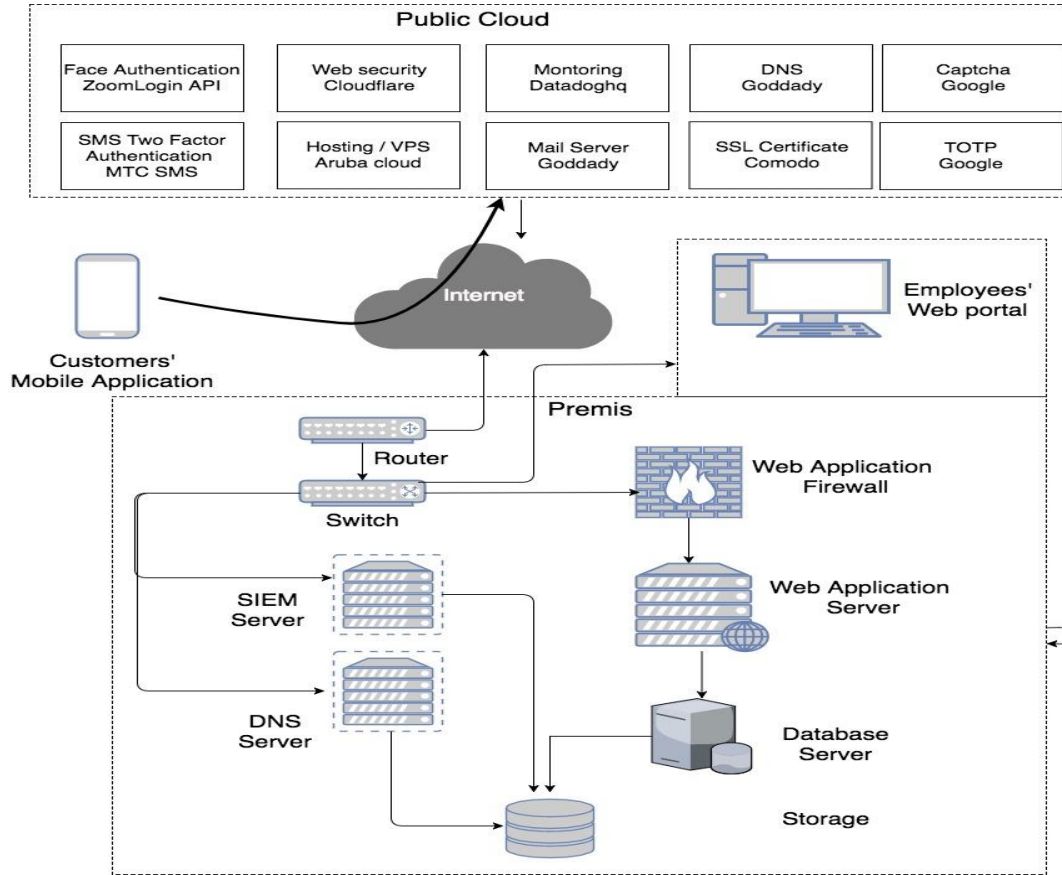


Fig. 4.1: our System & Structural Model (Mobi-Cash)

- The new model design have three main categories :
1. We build our infrastructure model of the platform on the basis of a hybrid model environment (local and cloud).
  2. We build our Access system model of the platform on the basis of risk-based and adaptive authentication mechanism using biometric techniques (Face Recognition).
  3. We build The compliance model of the platform to match with local regulatory bodies in Palestine (PMA) , and international standard of payment card industries (PCI).
  4. System structure get acceptance from experts in IT field in banking sector. (Appendix F).

#### 4.1 Our Public Cloud Layers

The public cloud (off-premise – Private cloud) as in Fig 4.2 runs the electronic

banking services that are given to the customers, the authentication services and it holds a backup for the internal banking data to guarantee the availability of the information even when internal services in the private cloud goes down.

Also, it provides the low-latency usage, scalability and the availability of the customers due to the robust infrastructure which is offered by the public cloud providers such as Microsoft, Google, and Amazon.

Public cloud layer structure interaction diagram as in fig 4.2 , shows the system components that consist of following:

#### 1. **Web Application Server.** (Customer API)

- Functionalities :
  1. Customers authentication.
  2. Transactions handling.
  3. Customers information.
- Database:
  1. MySQL Store users' information and transactions.
- Programming Language:
  1. PHP/Laravel implementing the main API Laravel.
- Encryption:
  1. Tokens / AES-256-CBC Encrypt sensitive data and JSON Web Tokens (JWT) (Authentication Tokens).
  2. TLS SHA256-RSA / 2048 Bits ; Encrypt HTTP traffic.
- Protocol:
  1. HTTPS – TCP / Encrypted HTTP traffic
  2. SSH – TCP / Encrypted remote Access to the server
  3. GIT / Source code control
- Integrations:
  - ZoomLogin: 3D face authentication and liveness detection.
- MTC SMS: delivering SMS OTP codes to the customers.
- CloudFlare: Web application firewall.

- GeoNames: Geographical axes lookup.
- OS: Ubuntu server.
- HTTP Server: Apache.
- Hosting VPS from Aruba is Navicosoft pre-installs scripts including PHP5/Perl/Python & maintains all the software which you need in your server.
- between the API and the Mobile Application.

## 2. SMS Server.

**SMS** (short message service) is It used for Delivering OTP via SMS.

Random OTP Length as input in below formula:

$OTP = random() * OTP\_Length(6)$

To generate a six-value OTP code we use a random function the returns a value from 0 to 1 then we take the output of multiplying its value with 6 to get a six-digit code.

## 3. **DNS Server** – External part with GoDaddy.

Domain Name Servers (DNS) This DNS level work to serve external request that received by internal DNS server in private cloud environment.

## 4. Mail Server.

**mail server** used to send verification emails to employee account manager to activate and approve or decline a specific request/s such as add payee and register new mobile client users.

GoDaddy SMTP Gateway was used to do this task process.

## 5. Captcha & TOTP services from Google.

Captcha (Completely Automated Public Turing) , that used in authentication cycle process to distinguish between human and computer action.

## 6. **SSL** Certificates from GoDaddy.

SSL (secure sockets layer) certificate is a digital certificate that both authenticates the identity of a website, and encrypts sensitive

information so that any passwords, addresses or credit card numbers can not be intercepted or read by anyone other than the intended recipient.

7. **Face Authentication** form Zoom.

Using liveness detection within a face recognition phase will improve and enhance the security level of authentication and authorization the customers when trying to locate there mobile banking application as we try to do in this thesis. Liveness & 3D depth detection methodology / approach / techniques have been adopted in this thesis and choose Zoom login SDK.

8. Web Application Firewall and Monitoring system by Cloudflare.

Web application firewall (WAF) is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. While proxies generally protect clients, WAFs protect servers.

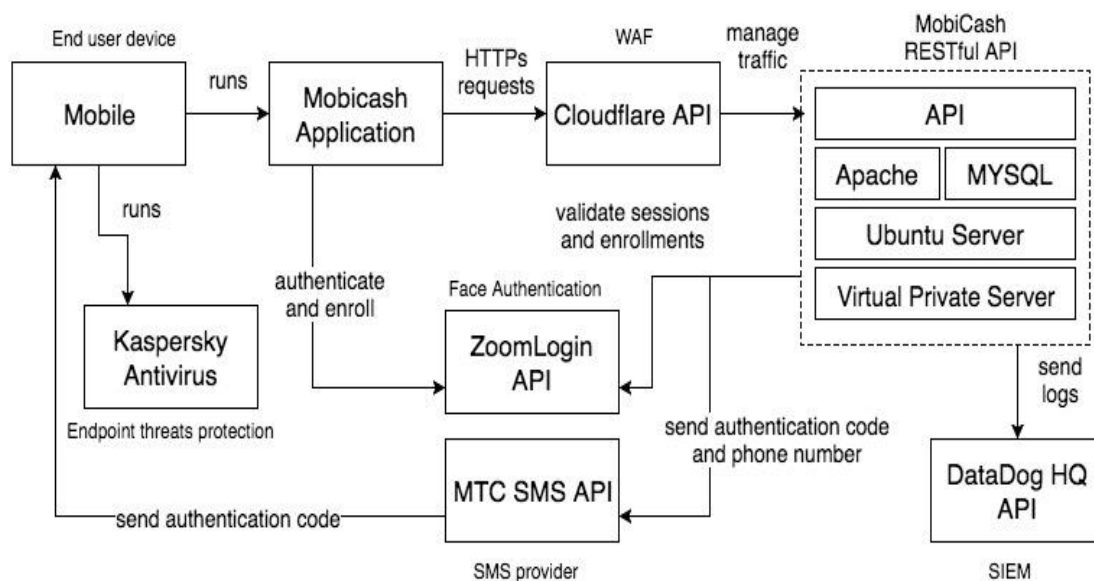


Fig 4.2 Public Layer Interaction block diagram



- Enrollment & Registration Process:
- Downloads the mobile banking application.
- Choose ID based on Bank rules and protocols.
- Banking Employees linkage the ID to a banking account.
- Authentication of Mobile number.
- SMS activation.

➤ Authentication Process:

- Face Capture phase:
  1. Customer use mobile device.
  2. Mobile device camera opened.
  3. The face image is taken.
- Bank teller & customer employees:
  1. Employee login to a web application using two-factor authentication by username and Google OTP
  2. linkage the Mobile ID with a banking account.
- Face Recognition Phase and Logon MobCash:
  1. Face images that have been taken are identified and varified.
- Face Images Store Phase:
  1. Face image will transfer to the dedicated cloud.
  2. Face images validation profile has become created to allow the customer to access the mobile application based on saved face images.

**Algorithm 1: Registration Phase**


---

```

Start
Open registration page
Fill registration customer details ID1 and create INDEX CLIENT
Send ID1 account manager for approval
    if (FLAG==Success) then
        Capture face successfully for ID1
    else
        FLAG ← FAILS
        Manual check by the account manager
    end if
Calculate INDEX NEW CLIENT (Face map) ← INDEX CLIENT * FACE Image
Store face map in public cloud storage DB
Registration successful for ID1
Stop

```

**Algorithm 2: Login Phase**


---

```

Start
Open login page
Insert the login username for ID1
Show captcha
Insert captcha
    if (FLAG==Successful) then
        Login ID1
        SMS created and send to ID1
    else
        Return to login page
    end if
Open SMS verification code page
Insert verification code
Capture the face of ID1 and create INDEXCLIENT
Compare INDEX CLIENT with NEW INDEX CLIENT (ID1 + Face Image)
    if (FLAG== Successful) then
        Open security status result
        if (FLAG== Successful) then
            Login ID1 successful
        else
            FLAG ← FAILS
            Login failed
        end if
    end if
Stop

```

## 4.2 Our Private Cloud Layers

The private cloud (On-premise) use for internal banking operations, such as money transfers, customer relationships, and management. The private cloud allows the bank to retain control and apply rigorous security with lower cost and effort. So, it decreases the total cost of ownership of software licenses and reduces the deployment resources.

- Private cloud layer structure interaction diagram as in fig 4.3 , shwos the system components that consist of following:

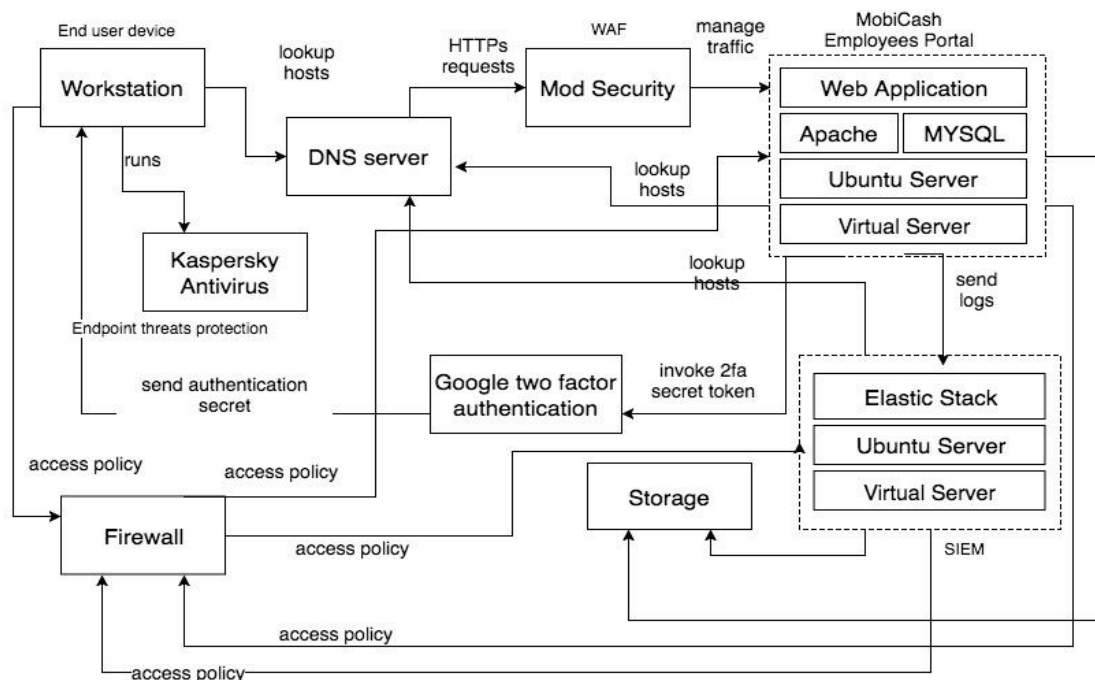


Fig 4.3 Private Layer Interaction block diagram

### 1. Web Application Servers.(Employee Administration portal)

Same as in Public cloud but with different functionalities as following:

- Customers approval and reporting.
- Payees requests approval and reporting.
- Virtual Cards issuing.
- Cash flow withdraw/ deposit.

### 2. Database Servers.

MySQL server: relational database, It's used to store users' information and transactions.

3. Web Application Firewall.

Mod-Security is a toolkit for real-time web application monitoring, logging, and access control work as WAF.

4. Network Security Management Server.

Security Onion IDS It is used for monitoring your network for security related events and It used to identify vulnerabilities or expiring SSL certificates.

5. Security and event logging management servers (SIEM).

Elastic Stack is security, security information and event management (SIEM) , It works as central logging and records all events for all system, network and application in the infrastructure environment.

6. Storage & Backup System.

Storage is used to store all customer and employees data and information, such as HP , IBM and DELL EMC storage.

Backup is the process of backing up the operating system, files and system-specific useful/essential data. Backup is a process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost, it can be hardware or software.

7. Domain Name System Server.(Internal Part)

8. Active Directory Service Server.

**Algorithm 3:** Pin Change

```

Start
Request new pin for secured service for ID1
  if (FLAG== Successful) then
    Insert the PIN code
  New service requested success
  else
    Request new PIN code
  end if
Stop
  
```

**Algorithm 4: Reset Password**


---

```

Start
Open reset password menu
Insert the current password ID1
  if (FLAG==Successful) then
    send mail with a new password for ID1 mail
Teller approved ID1 request
password changed
  else
    no password changed
  end if
Stop

```

**Algorithm 5: Forget Password**


---

```

Start
Open forget password menu
Insert the login name and mobile phone of ID1
  if (FLAG==Successful) then
    send mail with a new password for ID1 mail
Teller approved ID1 request
password changed and send a new password to ID1 mail
  else
    no password changed
  end if
Stop

```

**Algorithm 6: Teller Login with OTP**


---

```

Start
Open teller (T1) login page
Insert username and password for T1
  if (FLAG==Successful) then
    Send OTP to T1 mobile
    insert new OTP
    FLAG ← SUCCESS
Open web server page
  else
    Open T1 login page again
  end if
Stop

```

### 4.3 Our Mobile Application Layers:

- This layer will concern mobile application and authentication services depend on biometric services as authenticated the customer.
- The mobile application is used by the customers to check their accounts and proceed with their online banking operations. For transaction process will use PIN created by client after logon the Mobile application.
- Mobile Application Layer contains the following services:
- Identification Services & Authentication Services using face recognition.
- Geolocation using Google Geonames.
- SMS using local company to deliver this service.

### 4.4 Development & Experimental Results:

- Public Cloud:
  1. Face Authentication – API: ZoomLogin
  2. SMS Authentication – API: Twilio SMS
  3. Web Security/DNS Security, Web Application Firewall, Cloud flare.
  4. Hosting/VPS Customers' API: Aruba cloud Ubuntu\_Apachserver  
MYSQL
  5. DNS & Business Mail [admin@mobi-cash.com](mailto:admin@mobi-cash.com): Godaddy
  6. SSL certificate: Comodo
- Private Cloud: (On-Premise)
  1. Hosting Employees Web Portal: Linux server (Apache Server) /  
MYSQL.
  2. SIEM: Elastic Search (Centos)
  3. Web Application Firewall: CacheGaurd (Ubuntu)
  4. Two Factor Authentication, Google OTP
- Software Tools:
  1. PHP Laravel: Web Application and RESTful API
  2. Android SDK: Mobile Application
  3. MYSQL: Database
  4. GROK: Share local web server on public - Testing Environment

5. Valet: Laravel Development Environment
  6. Git: Source Code Version Control and Collaboration
  7. Draw.io: Drawing Diagrams
  8. Google Drive: Documentation
  9. Photoshop: Graphics
  10. VMWare: Virtual Machines
  11. CAPTCHA
- Hardware Tools:
    1. Mobile: Android 5.1, RAM 2GB
    2. Laptop: I7, Windows, 16 GB ram
  - Table 5.1 shows all hardware and software specification used to design and build Mobi-cash application.

Table 4.1 Hardware &amp; Software Specifications

Public Cloud (Off-Premise)		Private Cloud (On-Premise)		Software Tools		Hardware Tools	
Service	Provider	Service	Provider	Name	Purpose	Device	Specifications
Face Authentication - API	Zoom Login	Hosting Employees Web Portal	Linux server (Apache Server) / MYSQL	PHP Laravel	Web Application and RESTful API	Mobile	Android 5.1, RAM 2GB
SMS Authentication - API	MTC SMS	SIEM	Elastic Search (Centos)	Android SDK	Mobile Application	Laptop	I7, Windows, 16 GB ram
Web Security / DNS Security, Web Application Firewall, Monitoring	Cloudflare	Web Application Firewall	MoD Security	MYSQL	Database		

Hosting / VPS Customers' API	Aruba cloud Ubuntu / Apache server / MYSQL			NGROK	Share local web server on public - Testing Environme nt		
DNS	GoDadd y			Valet	Laravel Developme nt Environme nt		
SSL certificate	Comodo			Git	Source Code Version Control and Collaborati on		
				<a href="#">Draw.io</a>	Drawing Diagrams		
				Google Drive	Documenta tion		
				Photoshop	Graphics		
				VMWare	Virtual Machines		



## Chapter Five

### 5 Experimental Results of Implementation:

#### 5.1 Part # 1: Hybrid cloud model

##### ➤ Cloud Comparison:

Based on studying and analysis related works in the cloud and mobile cloud computing analysis and design from security architecture respective in chapter two, we make a table of comparison between thesis new model of Mobi-Cash and others research for private, public and hybrid clouds [R. Balasubramanian, 2012]. Criteria of evaluation items shown in Table 4.2 describe the level of coverages of these items at the scale of (High, Medium, and Low) for each type of cloud environment (Private Cloud; Public Cloud; Hybrid Cloud (On-Premise & Off-Premise); Hybrid Cloud (Off-Premise)).

[Kathleen Jungck\_2011] use key elements property that we choose to do the evaluation and comparison between others related works and our proposed model.

The criteria's are:

- Data Security
- Cost Variations
- Control
- Compliance
- Service Level Agreement
- Data Transfer & Integrations
- Compatibilities of Applications & Programs
- Performance
- Availability
- IT Operation Models & Organizational Structure
- Time and Resources
- Fast Deployment and Productivity

- Scalability and Flexibility
- Non-Lock-In
- Management and Migration

Table 5.1 Mobile Cloud Computation Security Comparison -related works

Item Discription	Private Cloud	Public Cloud	Hybrid Cloud	Mobi-Cash Cloud
Data Security	High	Low	Medium	High
Cost Variations	High	Low	Medium	Medium
Control	High	Low	Low	High
Compliance	Medium	Low	Low	Medium
Service Level Agreement	Medium	Low	Low	Medium
Data Transfer & Integrations	High	Low	Low	High
Compatibilities of Applications & Programs	High	Low	Low	High
Performance	Medium	Low	High	High
Availability	Low	High	High	High
IT Operation Models & Organizational Structure	High	Low	Low	High
Time and Resources	High	Low	Low	High
Fast Deployment and Productivity	Low	High	High	High
Scalability and Flexibility	Low	High	High	High
Non-Lock-In	High	Low	Low	High
Management and Migration	High	Low	Low	High

- In this research chooses a small key of elements to make the comparison, and the average gives the hybrid cloud off-premise from two cloud providers the best scores. Mobi-Cash model was designed in two cloud model which is On-premise and public cloud (off-premise), also that the public cloud has two cloud service providers one from Zoom and one from Microsoft Azure.
- The result as shown below chart diagrams between these cloud models shows that newly introduced model by this thesis gives the best results with high and medium confidence comparing with other current cloud models.

- Mobile banking questionnaire in appendix G, show that experts opinion prefer to use our system structure (Mobi-Cash) with average score of 4/5.

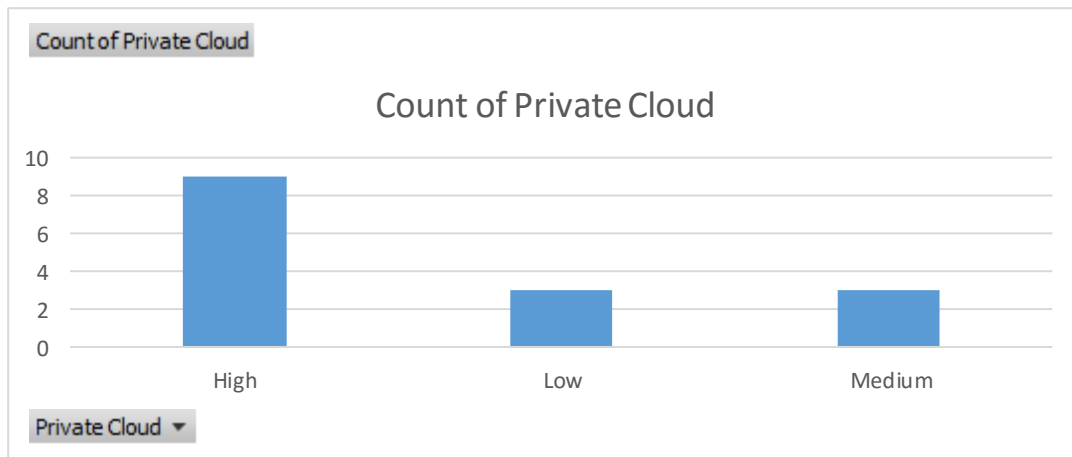


Fig 5.1 Private Cloud

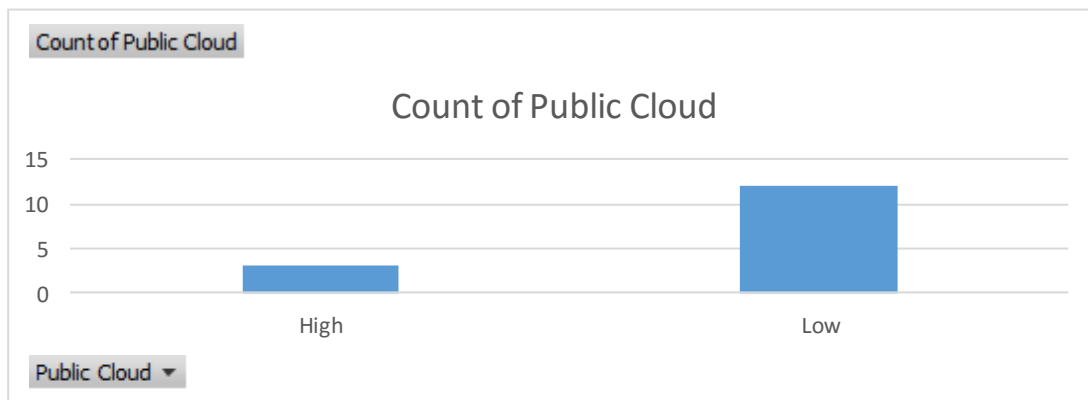


Fig 5.2 Public Cloud

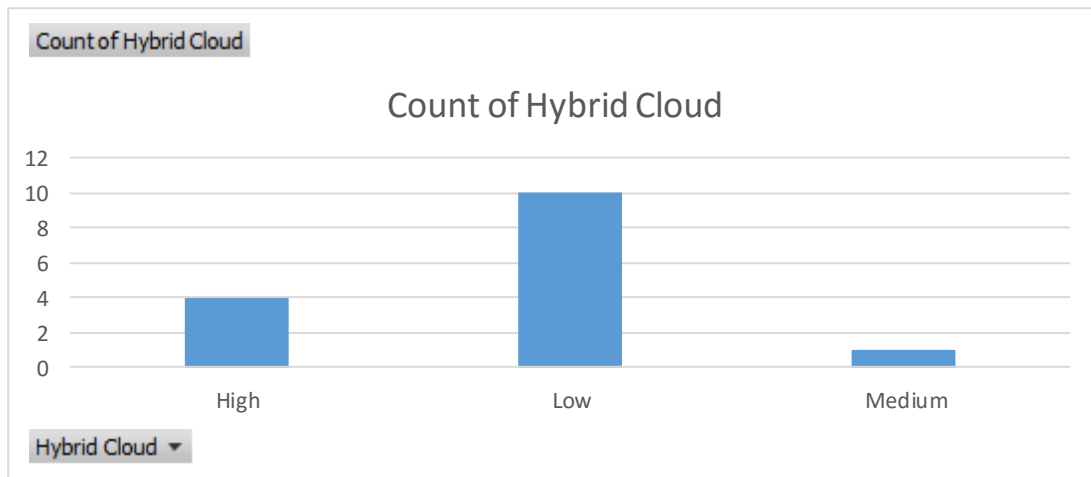


Fig 5.3 Hybrid Cloud

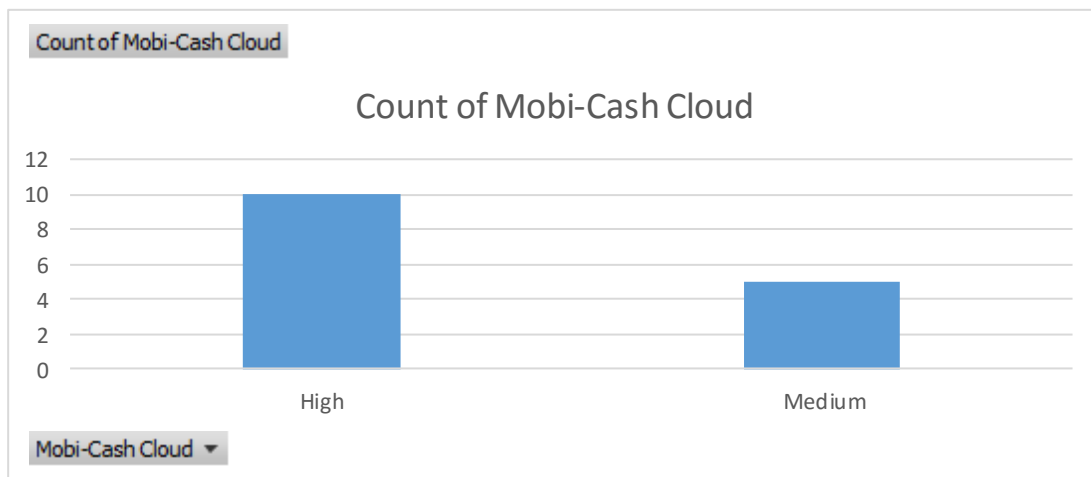


Fig 5.4 Hybrid Cloud “Mobi-Cash”

## 5.2 Part # 2: Security Mobile Payment Comparison

➤ Security measures and controls:

Table 4.3 shows a comparison of security issues in related works (study & analysis described in chapter 3 and 4) of mobile cloud computing depend following security schemes:

- Dynamic credential generations such as using biometric service instead of password.
- Location Privacy
- Secure data communication
- Authentication
- Data Confidentiality
- Access Control
- Data Integrity
- Identity Protection

Each related works covers one or two of these security schemes only. These works describe in brief in Table 4.4.

➤ **Mobi-cash** shows that use a set of combination of security schemes that consist of following with high scalability:

1. Seamless password authentication – no password needed.
2. Biometric authentication using face recognition SMS OTP.
3. Identity protection using random ID creation and encryption, in addition to Firewall and WAF system.
4. Secure access control using SSL certificate and Bomgar system.
5. Data Integrity by following software life cycle and use access control. The system from Bomgar, also, to using Kaspersky AV on mobile devices. And servers in the banking environment.
6. Data Confidentiality using encryption software and access control system.

7. Data Availability using hybrid cloud model, private cloud (On-premise) and public cloud in private mode (Off-premise).
8. Secure data communication using SSL certificate by Comodo.
9. Location Privacy using Google maps.

Table 5.2 Security Mobile payment Comparison

Item Discription	Niranjana-murthy M,2013	Imran Ashraf ,2012	Raphael Akinyede,2010	Wencheng Yang , 2013	Zijiang Hao , 2015	Our Approach Mobi-Cash
Access using Username / Password	Yes	Yes	Yes	Yes	Yes	Yes
Access using Biometric	NO	NO	NO	Yes	NO	Yes
Data Storage (Premise & Cloud) Security (Encryption)	Yes	Yes	Partial(3 DES)	Partial - No cloud	Yes	Yes
Data Integrity & Identity Protection	Yes	Yes	Yes	Yes	Yes	Yes
Data Privacy	NO	Yes	Yes	Yes	Yes	Yes
Cost Variations	NO	NO	NO	NO	Yes	Yes
Control	NO	Yes	Yes	NO	Yes	Yes
Compliance	NO	Yes	NO	NO	NO	Yes
Service Level Agreement	NO	Yes	NO	NO	Yes	Yes

Data Transfer & Integrations	NO	Yes	Yes	Yes	Yes	Yes
Compatibilities of Applications & Programs	NO	Yes	NO	NO	Yes	Yes
Performance	Yes	Yes	NO	NO	Yes	Yes
Availability	Yes	Yes	NO	NO	Yes	Yes
IT Operation Models & Organizational Structure	NO	NO	NO	NO	NO	Yes
Time and Resources	NO	NO	NO	Yes	Yes	Yes
Fast Deployment and Productivity	NO	NO	NO	Yes	Yes	Yes
Scalability and Flexibility	NO	NO	NO	Yes	Yes	Yes
Non-Lock-In	NO	NO	NO	NO	NO	Yes
Management and Migration	NO	NO	NO	NO	Yes	Yes
Location Privacy	NO	NO	NO	NO	NO	Yes
Secure data communication	NO	NO	NO	NO	NO	Yes

- Mobile banking questionnaire in appendix G, show that experts' opinion for securing mobile banking application using above table items criteria's and get average score of 4/5.

Table 5.3 Security of Mobile cloud computing-related works

Works	Proposed Features	Schemes Security	Technical Approaches	Scalability
H. Wang, 2014 [29]	Secure data storage and sharing in mobile media cloud	Authentication	Scalable watermarking and Reed-Solomon coding	High
M. R. Baharon, 2015 [30]	Data storage security	Data Confidentiality	Homomorphic encryption	Low
Y. Yu, 2014 [31]	A public auditing protocol for secure data storage and sharing	Data Integrity & Identity Protection	Asymmetric group key agreement and proxy re-signature	Medium
M. Bahrami and M. Singhal, 2015 [32]	A lightweight data privacy preserving method	Data Privacy	Pseudo-random permutation method	Medium
V. Odelu, 2016 [33]	CP-ABE-CSCTSK (CP-ABE- constant size ciphertext and secret keys)	Access Control	Ciphertext-policy attribute-based encryption (CP-ABE) algorithm	Medium
M. Ali, 2015 [34]	Secure Data Sharing in Clouds (SeDaSC)	Secure Data Searching	Advanced Encryption Standard and symmetric encryption	High
Y. Xia, 2015 [35]	TinMan	Secure Offloading	Trusted node, SSL session injection and TCP payload replacement	Medium
T. Meng, 2015 [36]	Security analysis of offloading under timing attacks	Defend Timing Attack	Modified cryptographic system	Low
S. Y. Vaezpour,	SWAP, an aware security	Protecting data leakage	Dynamic allocation and	High



2016 [37]	provisioning and migration approach	from phone clones	migration of phone clones	
Z. Hao, 2015 [38]	SMOC, secure mobile cloud platform	Secure application cloning on VM	Hardware virtualization, a proposed file system	Medium
H. Liang, 2014 [39]	Security isolation and migration approach for VM deployment	Secure VM deployment	The mandatory access control mechanism, security label in socket communication	Medium
D. Popa , 2013 [40]	SMC, a security framework for mobile clod applications	secure data communication	Trusted managers, application signature verification	Medium
P. K. Tysowski, 2013 [41]	A protocol for secure mobile applications	Application security	Attribute-based encryption, group keying mechanism and re-encryption	High
J. Tan, 2014 [42]	STOVE model	Secure application execution	Trusted party, strong isolation and verification	High
L. Tang, 2015 [43]	Strong API security for securing MCC	Web API security	encryption, public key infrastructure, transport layer handshake protocol	Medium
X. Zhang, 2009 [44]	The secure elastic application model	Authentication, secure communication and migration	Trusted managers	High
H. Zhang, 2015 [45]	Preserving location-based information survey applications	Location Privacy	System-level cloning of mobile devices	Medium
A. N. Khan, 2013 [46]	Identity privacy protection approach	Identity Privacy	Dynamic credential generations	High

Mobi Cash	Dynamic credential generations , Location Privacy , secure data communication , Authentication , Data Confidentiality , Access Control , Data Integrity & Identity Protection	Dynamic credential generations , Location Privacy , secure data communication , Authentication , Data Confidentiality , Access Control , Data Integrity & Identity Protection	Dynamic credential generations , Location Privacy , secure data communication , Authentication , Data Confidentiality , Access Control , Data Integrity & Identity Protection	High
-----------	---	---	---	------

- **Below images** is proof of concept attack result showing that the WAF system is working and block attacks from login to mobile banking system Mobi-Cash.

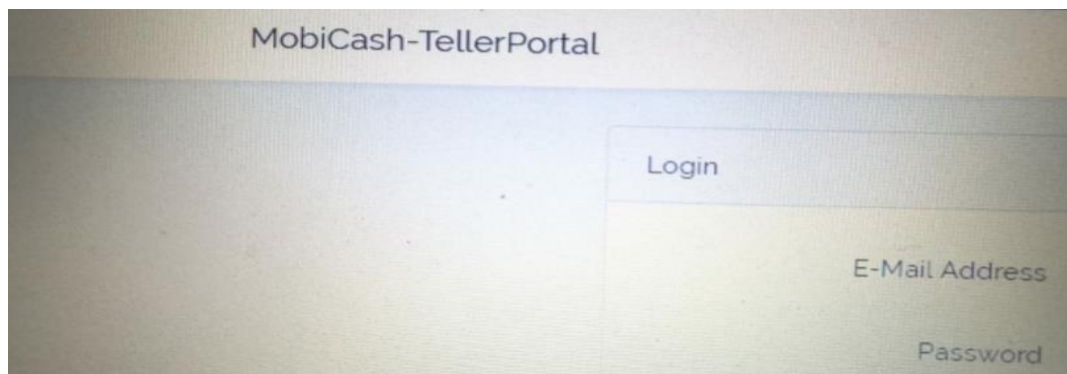


Fig. 5.5 Web Access before attack

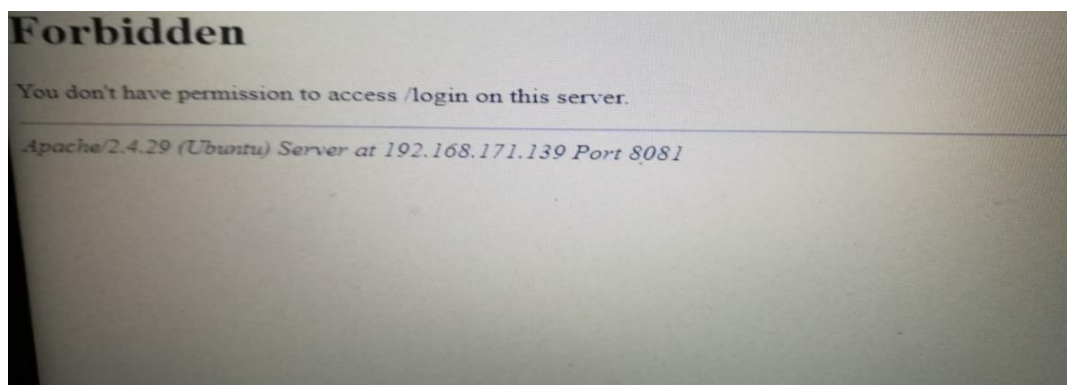


Fig. 5.6 Web Access after attack

### 5.3 Part # 3: PCI Compliance

➤ PCI Defining processing security requirements:

Mobi-cash uses PCI checklist sheet as below table to ensure applying most of the PCI requirements onto its design to comply fully with 12 standards requirements as below table 4.5. A full detailed checklist contains more than 300 controls, but we will point to it in indexes for this thesis. As a result of we manage to apply almost 70 % of the requirements (PCI SSC Quick Reference Guide v3.2, 2016).

Table 5.4 PCI DSS Requirements

Control Objectives	Security Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

**Summary :**

Mobi-Cash, follow internal guides and instructions for local regulations issued by Palestinian Money Authority PMA as described in their publications[ PMA PaymentSystem,2013] for financial inclusion and global payment system in the Palestinian market. Also, PMA builds new systems to such as reconsolidation system, national switch and mobile national switch to sustain the strength of financial sectors by adopting new electronics financial transaction in the market and encourage all people to use new e-channel provided by banks such online banking, mobile banking, and mobile payments. Moreover, PMA endorses new legal charter for electronic financial transactions to be used in dispute between people and companies using different channels of payment systems.

## **Chapter 6**

### **6. Conclusion and Future Work:**

#### **6.1 Conclusion:**

- We proof on our demonstration that we manage to give better results comparing with related works for each part mentioned in our objectives and goals of this research.
- Our research can be considered as foundation key base for any applied research works in the field of payment system.
- We manage also, to introduce and build new secure payment system that will be valid to work in market that targeting any financial service organization like banks , payment and fintech companies.

As a conclusion of our work on this thesis, we try to tackle and solve most of the challenges and constraints that our Palestinian market needs to cope with world market in the term of payment aspects and create a new model to use a new method of payments using mobile application using their smart mobile phones.

Issues that have been resolved by the proposed solution in thesis summaries as follows:

- 1- Local Regulations by PMA: Based on the nature of my works on the bank of Palestine, we met with PMA and discussed how must the current policies moreover, procedures should be changed to facilitate to introduce a new way of payment such as mobile banking application and mobile payment, especially to endorse new regulation for electronic transactions and procedures to assist the type of electronic document that will be used in e-forms and e-signature , since the electornics legesation not adopted in the Palestine yet completely.

- 2- Internal Banking modules: Most of core banking system need to be changed or upgrade to add new modules that can be fitted with new payment modules using their external services such as internet banking and mobile banking. Digital transformation “Digitalization” considers the latest approach to adopt and support such these new features.
- 3- User authentication: Most internet banking and mobile banking still use traditional user authentication such as username and password to access their web and mail application, and because a vast attack surfaces to financial services banks should be using a new adaptive authentication model such as Biometric techniques to get rid of traditional authentication way using user password and mitigate the massive attack of such this method of authentication.  
  
Mobi-Cash, use a very innovated method depended on biometric face recognition and added two level for authentication using SMS and OTP process to prove login user access to such this critical application “Mobile or Web Banking applications” is the same user that try to get access, not another person or automatic tools such botnet.
- 4- Threats & Vulnerabilities issues by using cloud computing and mobile cloud computing have been mitigated by using our thesis approach and methodology that explains in-depth details in Chapter 4 by using many tools such as Kaspersky for Virus and malware; Elastic stack for SIEM ; Mode-security and cloud flare as WAF ; Face recognition from ZoOm for logging issues; Secure API; SMS tools ; SSL certificates by Comodo.
- 5- Availability, Expandability & Reliability issues that face most of the local banking environment have been tackle based on our proposed solution by using hybrid environment that consists of private and public cloud environment works together to serve the idea behind this thesis.
- 6- Result based on experts opinion For System Structure Mobi-Cash:

- “ After Reviewing the high level design for the mobile payment system , the design is robust enough in security which is established in a very clear way in using the services of public and private cloud.”
- The design also getting benefit from the cloud services high availability by balancing the services through them.”

7- Cloud comparison result based on questionnaire has a result score of 3.8/5.

8- Security comparison result based on questionnaire has a result score of 4.6/5.

Finally, such these technologies for mobile application and mobile payment are very needed and required for our Palestinian market, since the Israeli occupation divide our land to small pieces of areas that not sufficiently connected to each other's and we cannot control our boards and cannot issue a national currency as in PMA report for financial inclusion [PMA Payment System, 2013]. This thesis will consider the first model to activate mobile payment using mobile banking application to facilitate for Palestinian people to do their financial transaction with very ease of use as a term of usability “customer experience” and more secure environment and considering availability to access their banking system from anywhere and at any time.

## **6.2 Future Works:**

Mobi-cash as new mobile banking application will open new opportunities to enable customers to open new banking account remotely and no need to visit the branch; this called Onboard account opening for a mobile banking application.

As future work for the developed mobile application, I will add blockchain, and AI tends to be used by the application to enable Palestinian to begin exchange cryptocurrencies till they success of issuing our national currency and taking all consideration of risk profile of using this technology and to improve transfer model in and out of Palestinian market.

Moreover, I will enhance the application to act as mobile payment using e-wallet to facilitate buying and selling all type of goods from inside and outside Palestine.



## **Bibliography:**

- [1] Y. Wang, Mobile Payment Security, Threats, and Challenges, Second international Conference, 1-5 (2016).
- [2] E Turban, D King, J Lee, M Warkentin, H Chung, Electronic Commerce-A Managerial Perspective Book, 9, 375-380 (2008).
- [3] A Rattrout , H Badir , Mobile Cloud Computing: Current Development and Research Challenges , IEEE , 1-9 (2013).
- [4] H Qi , Mobile Cloud Computing: Review, Trend, and Perspectives , IEEE 1-8 (2012).
- [5] H T Dinh, A survey of mobile cloud computing: architecture, applications, and approaches, Wireless Communications & Mobile Computing Conference, 1587-1611 (2011).
- [6] W O Victor, A Survey on Mobile Cloud Computing with Embedded Security Considerations, International Journal of Cloud Computing and Services, 53-66 (2014).
- [7] R Kumar, Comparison between Cloud Computing, Grid Computing, Cluster Computing and Virtualization, International Journal of Modern Computer Science and Applications (IJMCSA) 3, 1-5 (2015).
- [8] M Nazir, Cloud Computing: Overview & Current Research Challenges, IOSR Journal of Computer Engineering (IOSR-JCE), 14-22 (2012).
- [9] C Rompante, The Role of Cloud Computing in the Development of Information Systems for SMEs, Journal of Cloud Computing, 1-7 (2017).
- [10] W Shi, J Cao, Q Zhang, Y Li, L Xu , Edge Computing: Vision and Challenges, IEEE Internet of Things Journal, 637-646 (2016).
- [11] F Bonomi, R Milito, J Zhu, S Addepalli , Fog Computing and its Role in the Internet of Things, Proceedings of the first edition of the MCC , 1-3 (2012).
- [12] P S Suryateja , A Review :Threats and Vulnerabilities of Cloud Computing, International Journal of Computer Sciences & Engineering , 297-302 (2018).
- [13] Q Gu, M Guirguis, K.J. Han, High-Performance Cloud Auditing and Applications, Springer Science & Business Media New York, 1-11 (2014).

- [14] E Gorelik, Cloud Computing Models, Massachusetts Institute of Technology, 3,4,5 ,24-77 (2013).
- [15] S Singh, T Jangwal , Cost breakdown of Public Cloud Computing and Private Cloud Computing and security Issues, International Journal of Computer Science 17-31 (2012).
- [16] JP Singh, S Agrawal, An Approach for Human Gait Identification Based on Area, IOSR Journal of Computer Engineering, 33-36 (2013).
- [17] A Tolba , A Literature Review Face Recognition, International Journal of Signal Processing,88-103 (2005)
- [18] S Chakraborty, D Das, An overview of liveness detection, International Journal on Information Theory ,11-25 (2014).
- [19] OO Okediran, OT Arulogun, RA Ganiyu, CA Oyeleye ,A survey :Mobile operating systems and application development platforms, , International Journal of Advanced Networking and Applications, 2195-2201 (2014).
- [20] AK Singh, P Joshi, GC Nandi, Face liveness detection through face structure analysis, International Conference on. IEEE (ICSPCT), 1-5 (2014)
- [21] E De Cristofaro - Julien Freudiger, Greg Norcie, A Comparative Usability Study of Two Factor Authentication, 1-10 (2014).
- [22] R Balasubramanian, M Aramudhan, Security Issues: Public vs. Private vs. Hybrid Cloud Computing, International Journal of Computer Applications, 35-41 (2012).
- [23] H. Wang, S. Wu, M. Chen, and W. Wang, Security protection between users and the mobile media cloud, Communications Magazine, IEEE, 73-79 (2014).
- [24] M. R. Baharon, Q. Shi, and D. Llewellyn-Jones, A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing, International Conference on IEEE, 618-625 (2015).
- [25] Y. Yu, Y. Mu, J. Ni, J. Deng, and K. Huang, Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage, Network and System Security, Springer, 28-40 (2014).

- [25] M. Bahrami and M. Singhal, A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing, 3rd IEEE International Conference Mobile Cloud Computing, 189-198 (2015).
- [26] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, and K.-K. R. Choo, Pairing-based CP-ABE with constant-size ciphertexts and secret keys for a cloud environment, Computer Standards & Interfaces, 3-9 (2016).
- [27] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, et al., SeDaSC: Secure Data Sharing in Clouds, IEEE Systems Journal, 1-10, (2015).
- [28] Y. Xia, Y. Liu, C. Tan, M. Ma, H. Guan, B. Zang, et al., TinMan: eliminating confidential mobile data exposure with security-oriented offloading, in Proceedings of the Tenth European Conference on Computer Systems, 1-17 (2015).
- [29] T. Meng, Q. Wang, and K. Wolter, Model-based quantitative security analysis of mobile offloading systems under timing attacks, in Analytical and Stochastic Modelling Techniques and Applications, ed: Springer, 143-157 (2015).
- [30] S. Y. Vaezpour, R. Zhang, K. Wu, J. Wang, and G. C. Shoja, A New Approach to Mitigating Security Risks of Phone Clone Co-location Over Mobile Clouds, Journal of Network and Computer Applications, 171-184 (2016).
- [31] Z. Hao, Y. Tang, Y. Zhang, E. Novak, N. Carter, and Q. Li, SMOC: A secure mobile cloud computing platform, IEEE Conference in Computer Communications, 2668-2676 (2015).
- [32] H. Liang, C. Han, D. Zhang, and D. Wu, A Lightweight Security Isolation Approach for Virtual Machines Deployment, in Information Security and Cryptology, 516-529 (2014).
- [33] D. Popa, M. Cremene, M. Borda, and K. Boudaoud, A security framework for mobile cloud applications, Roedunet International Conference, 1-4 (2013).
- [34] P. K. Tysowski and M. A. Hasan, Hybrid Attribute-and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds, Cloud Computing, IEEE Transactions ,172-186 (2013).

- [35] J. Tan, R. Gandhi, and P. Narasimhan, STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications, IEEE 6th International Conference on Cloud Computing Technology and Science, 644-649 (2014).
- [36] L. Tang, L. Ouyang, and W.-T. Tsai, Multi-factor web API security for securing Mobile Cloud, 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2163-2168 (2015).
- [37] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, Securing elastic applications on mobile devices for cloud computing, Proceedings ACM workshop on Cloud computing security, 127-134 (2009).
- [38] H. Zhang, N. Yu, and Y. Wen, Mobile cloud computing based privacy protection in location-based information survey applications, Security and Communication Networks, 1006-1025 (2015).
- [39] A. N. Khan, M. M. Kiah, S. A. Madani, and M. Ali, Enhanced dynamic credential generation scheme for the protection of user identity in mobile cloud computing, The Journal of Supercomputing, 1687-1706 (2013).
- [40] G Watkins, Two Factor Authentication with Google Authenticator & LDAP, F5 Network Magazine, 1-6 (2011).
- [41] A Calder, G Williams, PCI SSC Quick Reference Guide v3.2, Security Standard Council, 1-40 (2016).
- [42] A K Jain, K Nandakumar, A Ross , 50 years of biometric research: Accomplishments, challenges, and opportunities , Pattern Recognition Letters , 1-27 (2016).
- [43] S Deepak, Face Recognition using Cloud-Based Security in Mobile Devices, International Journal of Innovative Research in Computer and Communication Engineering, 5705-5713 (2015).
- [44] I Ashraf , An overview of service models of cloud computing, International Journal of Multidisciplinary and Current Research, 779-783 ( 2014).  
An Overview of Service Models of Cloud Computing
- [45] H.Wang, S.Wu, M.Chen, W.Wang, Security protection between users and the mobile media cloud, Communications Magazine IEEE , 73-79 (2014).

- [46] M Usha, P Malathi, M PushpaRani , Security Threats in Mobile Cloud Computing, International Conference on Electronics and Communication Systems, 550-552 (2015).
- [47] A Banerjee, CM Dippon , Voluntary Relationships Among Mobile Network Operators and Mobile Virtual Network Operators: An Economic Explanation , Information Economics and Policy, 3-12 (2009).
- [48] M. Ali Green cloud on the horizon, In Proceedings of the 1st International Conference on Cloud Computing (CloudCom), Manila, 451–459 (2009).
- [49] A. K. Sharma, Mobile Cloud Computing (MCC): Open Research Issues, International Journal of Innovations in Engineering and Technology (IJIET), 24-27 (2013).
- [50] J. H. Christensen, Using RESTful web-services and cloud computing to create next-generation mobile applications, conference companion on Object-oriented programming systems languages and applications, 627-634, (2009).
- [51] L. Liu, R. Moulic, and D. Shea, Cloud Service Portal for Mobile Device Management, Proceedings of IEEE 7th International Conference January ,21-29 (2011).
- [52] I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud computing and grid computing 360-degree compared, Grid Computing Environments Workshop, 1-10 (2008).
- [53] RN. Calheiros, C. Vecchiola, D. Karunamoorthy, R Buyya, The Aneka platform and QoS-driven resource provisioning for elastic applications on hybrid Clouds, Future Generation Computer Systems, 861-870 (2012).
- [54] R. Buyya , CS. Yeo , S. Venugopal , J Broberg , I Brandic, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing the5th utility , Future Generation Computer Systems , 1-18 (2009).
- [55] Y. Huang, H. Su, W. Sun, JM. Zhang, CJ. Guo, JM. Xu , Framework for building a low-cost, scalable, and secured platform for Web-delivered business services IBM Journal of Research and Development , 1-14 (2010).

- [56] WT. Tsai, X. Sun, J. Balasooriya , Service-oriented cloud computing architecture, In Proceedings of the 7th International Conference on Information Technology, 684-689 (2010).
- [57] GH. Forman, J. Zahorjan, The Challenges of mobile computing, IEEE Computer Society Magazine, 38–47 (1994).
- [58] MY Qadri, Low Power Processor Architectures and Contemporary Techniques for Power Optimization – A Review, 927 - 942(2009).
- [59] LD. Paulson, Low-power chips for high-powered handhelds, IEEE Computer Society Magazine, 21 – 36 (2003).
- [60] U. Kremer, J. Hicks, J. Rehg, A compilation framework for power and energy management on mobile computers, In Proceedings of the 14th International Conference on Languages and Compilers for Parallel Computing, 115–131 (2001).
- [61] E. Cuervo, A. Balasubramanian, C. Dae-ki, Making Smartphones last longer with code offload, In Proceedings of the 8th International Conference on Mobile systems, applications, and services, 49–62 (2010).
- [62] E. Vartiainen, KV-V Mattila, The User Experience of Mobile photo sharing in the cloud, In Proceedings of the 9th International Conference on Mobile and Ubiquitous Multimedia, 1-10 (2010).
- [63] K. Kumar, Y. Lu, Cloud computing for mobile users: can offloading computation save energy, IEEE Computer Society, 51-56 (2010).
- [64] Zou P, Wang C, Liu Z, Bao D. Phosphor: a cloud-based DRM scheme with SIM card, In Proceedings of the 12th International Asia-Pacific on Web Conference, 1-26 (2010).
- [65] J. Oberheide, K. Veeraraghavan , E. Cooke , J. Flinn , F. Jahanian ,Virtualized in-cloud security services for mobile devices, In Proceedings of the 1st Workshop on Virtualization in Mobile Computing , 1-5 (2008).
- [66] X. Yang, T. Pan, J. Shen, On 3G mobile e-commerce platform based on cloud computing, Ubi-media Computing 3rd IEEE, 198-201 (2010).
- [67] J. Dai, Q. Zhou, A PKI-based mechanism for secure and efficient access to outsourced data, In Proceedings of the 2nd International Conference on Networking

moreover, Digital Society, 21- 29 (2010).

[68] Z. Leina , P. Tiejun , Y. Guoqing , Research of mobile security solution for fourth party logistics, In Proceedings of the 6th International Conference on Semantics Knowledge and Grid , 355 -358 (2010).

[69] H. Bouwman , Designing business models for mobile service bundles, Delft University of Technology , 1-21 (2014).

[70] M. El-Kabir Fareh, O. Kazary, M. Femmamy, S. Bourekkachey , An Agent-Based Approach for Resource Allocation in the Cloud Computing Environment, Computer Science Department, Publish in IEEE, 777-788 (2015).

[71] HowBiometricsExpand the Reach of Mobile, Aware Magazine, 1-11 (2016).

[72] G. Pan, Z. Wu, L. Sun, Liveness Detection for Face Recognition, Department of Computer Science, Zhejiang University China, 110-124 (2008).

[73] CT. Fan, WJ. Wang, YS. Chang, Agent-based Service Migration Framework in Hybrid Cloud Computing and Communications IEEE, 887- 892 (2011).

[74] DAB. Fernandes, Soares. Gomes, MM. Freire, Security Issues in Cloud Environments, Information Security, 1 62 (2014).

[75] N Kratzke, PC Quint , About Automatic Benchmarking of IaaS Cloud Service Providers for a World of Container Clusters , Journal of Cloud Computing Research , 16-34 (2015).

[76] B. Othmane, RSA Hebri , Cloud Computing & Multi-Agent Systems: A New Promising Approach for Distributed Data Mining , Information Technology Interfaces (ITI), 1 – 22 (2012).

[77] Distributed Management Task Force, Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol, An Interface for Managing Cloud Infrastructure, 1- 4 (2016).

[78] M. Hajibaba, S. Gorgin, A Review on Modern Distributed Computing Paradigms: Cloud Computing, Jungle Computing and Fog Computing, Journal of Computing and Information Technology (CIT), 69–84 (2014).

[79] J. Pourqasem1, S. Karimi, S.A. Edalatpanah, Comparison of Cloud and Grid Computing, American Journal of Software Engineering, 8-12 (2014).

- [80] Y. Wang, T. Uehara, R. Sasaki, Fog Computing: Issues and Challenges in Security and Forensics , College of Information Science & Engineering and Applications Conference (COMPSAC) IEEE , 53 – 59 (2015).
- [81] OWGA Edmonds, A. Papaspyrou, T. Metsch , Open Cloud Computing Interface - Core , The Open Cloud Computing Interface (OCCI) committee , 1-18 (2016).
- [82] P. vidya, Recent Trends in Cloud Computing: A Survey, International Journal of Advances in Computer Science and Technology, 65-69 (2013).
- [83] G. Fortino, W. Russo, Towards a Cloud-assisted and Agent-oriented Architecture for the Internet of Things, Università della Calabria – Italy, 1-6 (2013).
- [84] R. Patil Madhubala, Survey on Security Concerns in Cloud Computing, International Conference on Green Computing, 88-96 (2015).
- [85] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge Computing: Vision and Challenges, IEEE Internet of Things Journal ,3, 637-646 (2016).
- [86] H.K. Flora, X. Wang, and S. Chande, An Investigation into Mobile Application Development Processes: Challenges and Best Practices, Modern Education and Computer Science, 6, 1-9 (2014).
- [87] S. Kungspisidan, Modelling, Design, and Analysis of Secure Mobile Payment Systems , 5th International Workshop on Information Security Applications , 99 117 (2005).
- [88] L. L. Johnny, B. Judith, and J. H. P. Eloff, SMSSec: An end-to-end protocol for secure SMS, Developing Mobile Java Applications. Upper Saddle River, New Jersey: Prentice Hall, 174-179 (2008).
- [89] R. O. Akinyede, O. S. Adewale and B. K. Alese, Securing Mobile Payment Systems: Using Personal Identification Number (PIN) Method , Proceedings of the International Conference on Software Engineering and Intelligent Systems , 23 – 34 (2010).
- [90] L. Jinsheng, Design and Implementation of Mobile Payment Scheme based on WPKI and WAP Technology. Journal of Convergence Information Technology(JCIT) Volume8, 98-106 (2013).



- [91] M. Niranjanamurthy, Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security issues, International Journal of Advanced Research in Computer and Communication Engineering , 2360-2370 (2013).
- [92] S. V. Hatwar, Cloud Computing Security Aspects, Vulnerabilities and Countermeasures, International Journal of Computer Applications, 0975 – 8887 (2015).
- [93] FA. Alvi, BS. Choudary, N. Jaferry, E. Pathan , A review on cloud computing security issues & challenges, IAES Journal, 1-18 (2015)
- [94] I. Ashraf, Mobile Banking Security, Vrije Universiteit, Amsterdam, 1-70 (2012).
- [95] BW. Nyamtiga, A. Sam, LS. Laizer, Security Perspectives for Used vs. SMS In Mobile Banking, journal of technology enhancements and emerging, 38-43 (2013).
- [96] G. Ramesh, A Security Protocol for mobile-banking and payment using SMS and USSD in Ethiopia, International Journal of Research and Applications , 427-433 (2016).
- [97] T. Beza, Secure Mobile Banking FrameWork by Using Cryptography and Steganography Methods, Global Scienstfic Journal, 863- 882 (2018).
- [98] S. Pujitha , B. Mallu , SMS Based Mobile Banking , International Journal of Engineering Trends and Technology , 1211-1219 (2013).
- [99] K. Chikomo, M. Ki Chong, A. Arnab, A. Hutchison, Security of mobile banking, Andrew Hutchison, University of Cape Town Ronde South Africa 1-10 (2006).
- [100] J. Totonchi, Security of Mobile Banking, Proceedings International Conference on Rural Markets, 68-72 (2010).
- [101] V. Pegueros , Security of Mobile Banking and Payments , SANS Institute InfoSec Reading Room , 1-29 (2012).
- [102] W. Yang, Biometrics for Securing Mobile Payments: Benefits, Challenges, and Solutions, 6th International Congress on Image and Signal Processing, 1699-1704 (2013).
- [103] K. Gezahegn, Factors Influencing Usage of Mobile Banking in ADDIS ABABA, Addis Ababa University Master Program, 4 ,1-83 (2016)

- [104] R. Bhatia, Biometrics and Face Recognition Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering*, 93-99 (2013).
- [105] Y. Xia, Y. Liu, C. Tan, M. Ma, H. Guan, B. Zang, TinMan: Eliminating Confidential Mobile Data Exposure with Security Oriented Offloading, *Proceedings of the Tenth European Conference on Computer System*, 743-759 (2015).
- [106] H. Wang, S. Wu, M. Chen, and W. Wang, Security protection between users and the mobile media cloud, *Communications Magazine IEEE*, 73-79 (2014).
- [107] Y. Yu, Y. Mu, J. Ni, J. Deng, and K. Huang, Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage, *Springer in Network and System Security*, 28-40 (2014).
- [108] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, SeDaSC: Secure Data Sharing in Clouds, *IEEE Systems Journal*, 1-10 (2015).
- [109] T. Meng, Q. Wang, and K. Wolter, Model-based quantitative security analysis of mobile offloading systems under timing attacks, *Springer in Analytical and Stochastic Modelling Techniques and Applications*, 143-157 (2015).
- [110] Z. Hao, Y. Tang, Y. Zhang, E. Novak, N. Carter, and Q. Li, SMOC: A secure mobile cloud computing platform, *IEEE Conference in Computer Communications*, 2668-2676 (2015).
- [111] D. Popa, M. Cremene, M. Borda, and K. Boudaoud, A security framework for mobile cloud applications, *11<sup>th</sup> Roedunet International Conference*, 1-4 (2013).
- [112] P. K. Tysowski and M. A. Hasan, Hybrid Attribute-and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds, *IEEE Transactions on Cloud Computing*, 172-186 (2013).
- [113] J. Tan, R. Gandhi, and P. Narasimhan, STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications, *6<sup>th</sup> IEEE International Conference on Cloud Computing Technology and Science*, 644-649 (2014).

- [114] L. Tang, L. Ouyang, and W.-T. Tsai, Multi-factor web API security for securing Mobile Cloud, 12th International Conference on Fuzzy Systems and Knowledge Discovery, 2163-2168 (2015).
- [115] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, Securing elastic applications on mobile devices for cloud computing, Proceedings of ACM workshop on Cloud computing security, 127-134 (2009).
- [116] H. Zhang, N. Yu, and Y. Wen, Mobile cloud computing-based privacy protection in location-based information survey applications, Security and Communication Networks, 1006-1025 (2015).
- [117] A. N. Khan, M. M. Kiah, S. A. Madani, and M. Ali, Enhanced dynamic credential generation scheme for the protection of user identity in mobile cloud computing, The Journal of Supercomputing, 1687-1706 (2013).
- [118] HT. Dinh, C Lee, D. Niyato, P. Wang, Survey of Mobile Cloud Computing, Wireless communications and mobile computing, 1-32 (2013).
- [119] M. Alzubi , Unified Theory of Acceptance and Use of Technology (UTAUT) Model-Mobile Banking , Journal of Internet Banking and Commerce , (2017).
- [120] D. Lapin, Proposing a Cloud-based Operational Model for IT Infrastructure, Helsinki Metropolia University of Applied Sciences, 4, 38-58 (2014).
- [121] R. Nedzelsky, Hybrid cloud computing Security aspects and challenges, The Faculty of Informatics and Statistics, 1-8 (2015)
- [122] RO. Akinyede,OA.Esese, Development of a Secure Mobile E-Banking System , International Journal of Computer, 23-42 (2017).
- [123] B. Noonan, Factors Influencing the Adoption of the PCI, Master Program of Dublin University, 2, 6-27 (2015).
- [124] Q. Lin, W. Li, X. Ning, liveness detection through face structure analysis, Springer International Publishing AG, 637–645 (2016).
- [125] A. Lagorio, Liveness Detection based on 3D Face Shape Analysis, IEEE, 1-5 (2013).

## Appendices:

### A. Pseudo Codes: (Share by Below Link)

<https://drive.google.com/open?id=1wD1UI0cJ4dKek9NCzK0YPuchxGhf6pgU>

### B. Mobile and Web Application Interfaces Diagrams:

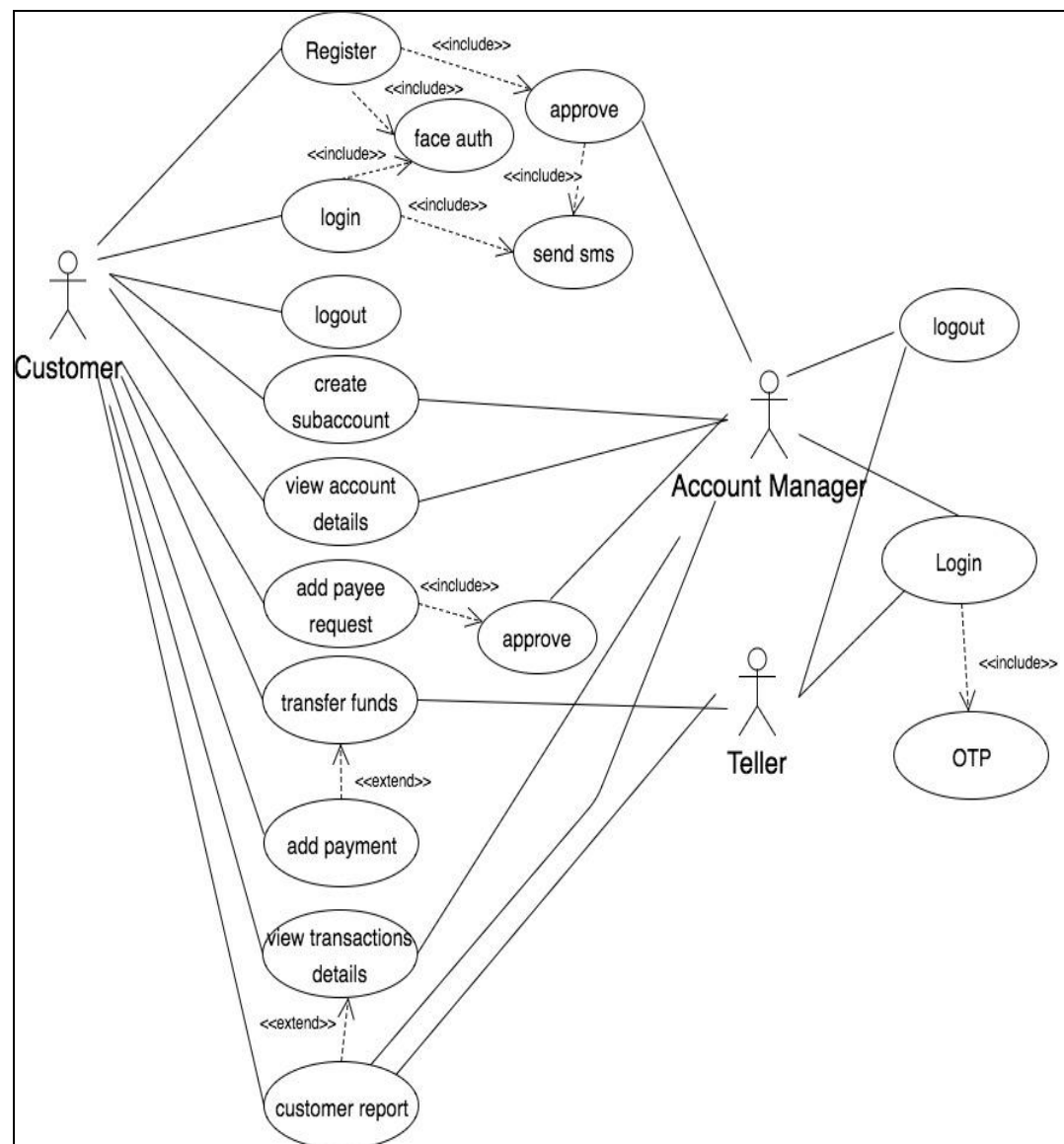


Fig 1: Customer Use Case Diagram

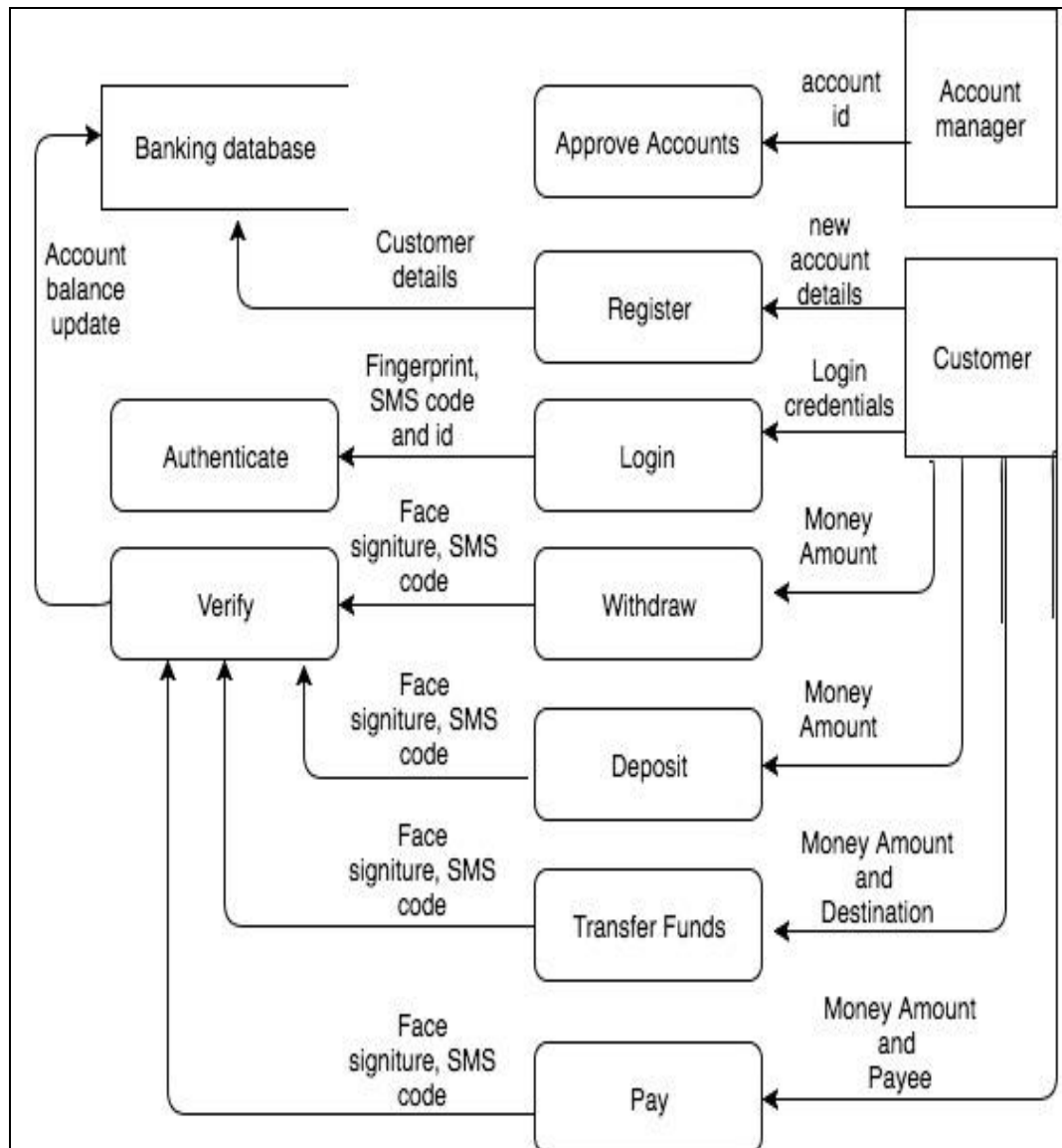


Fig 2: Data Flow Diagram

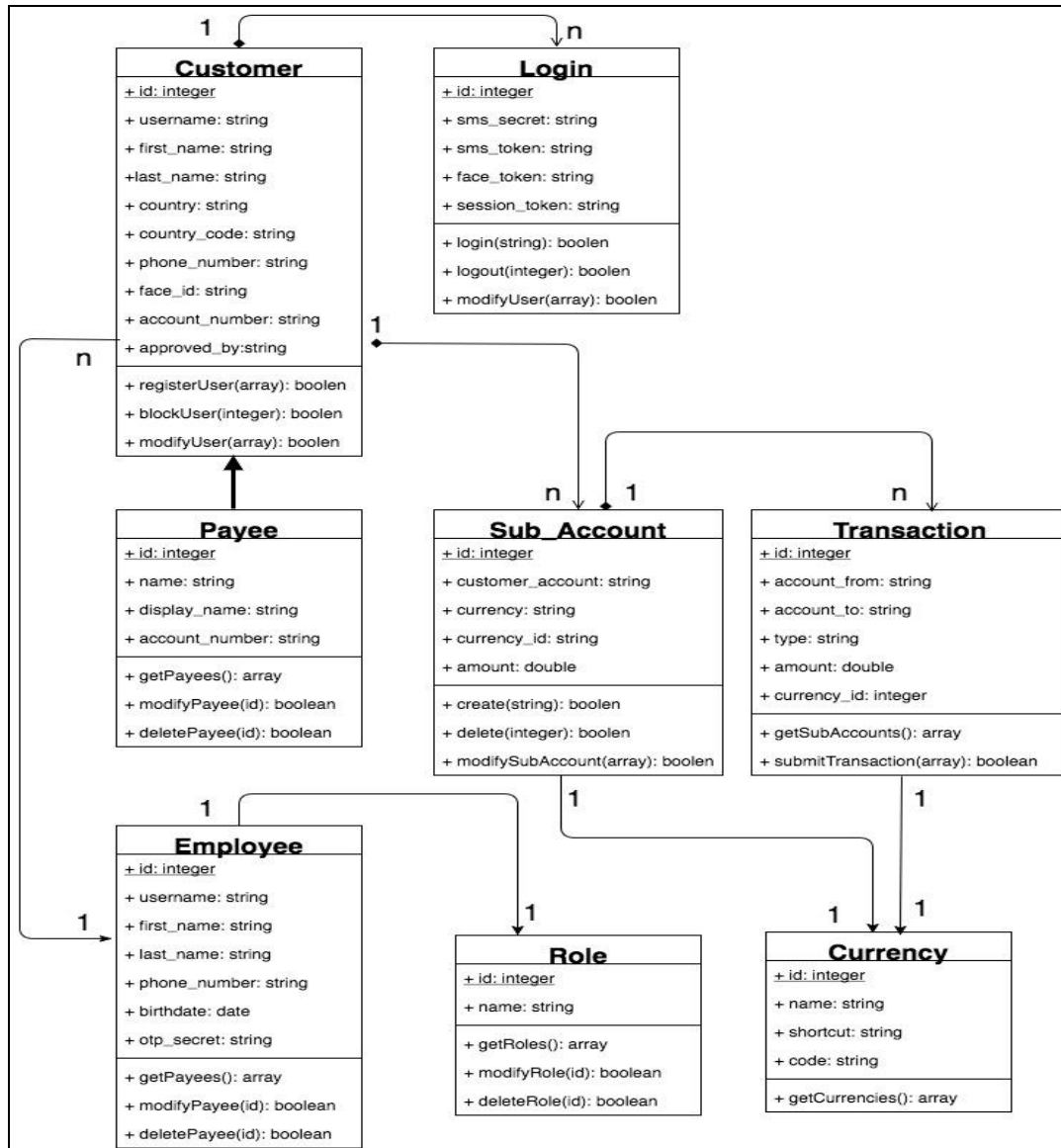


Fig 3: Entity-Relationship UML Class Diagram

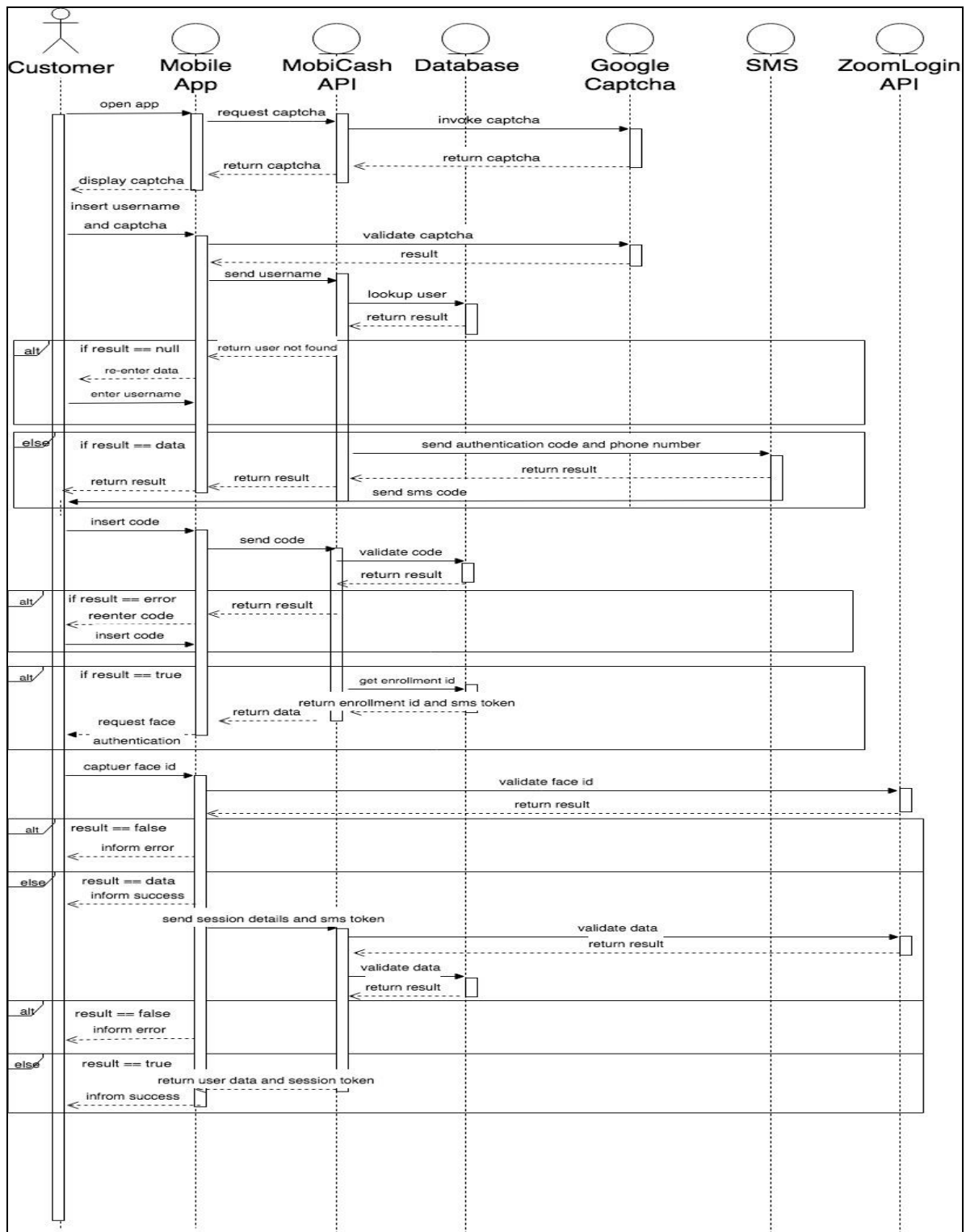


Fig 4: Customer Login Diagram

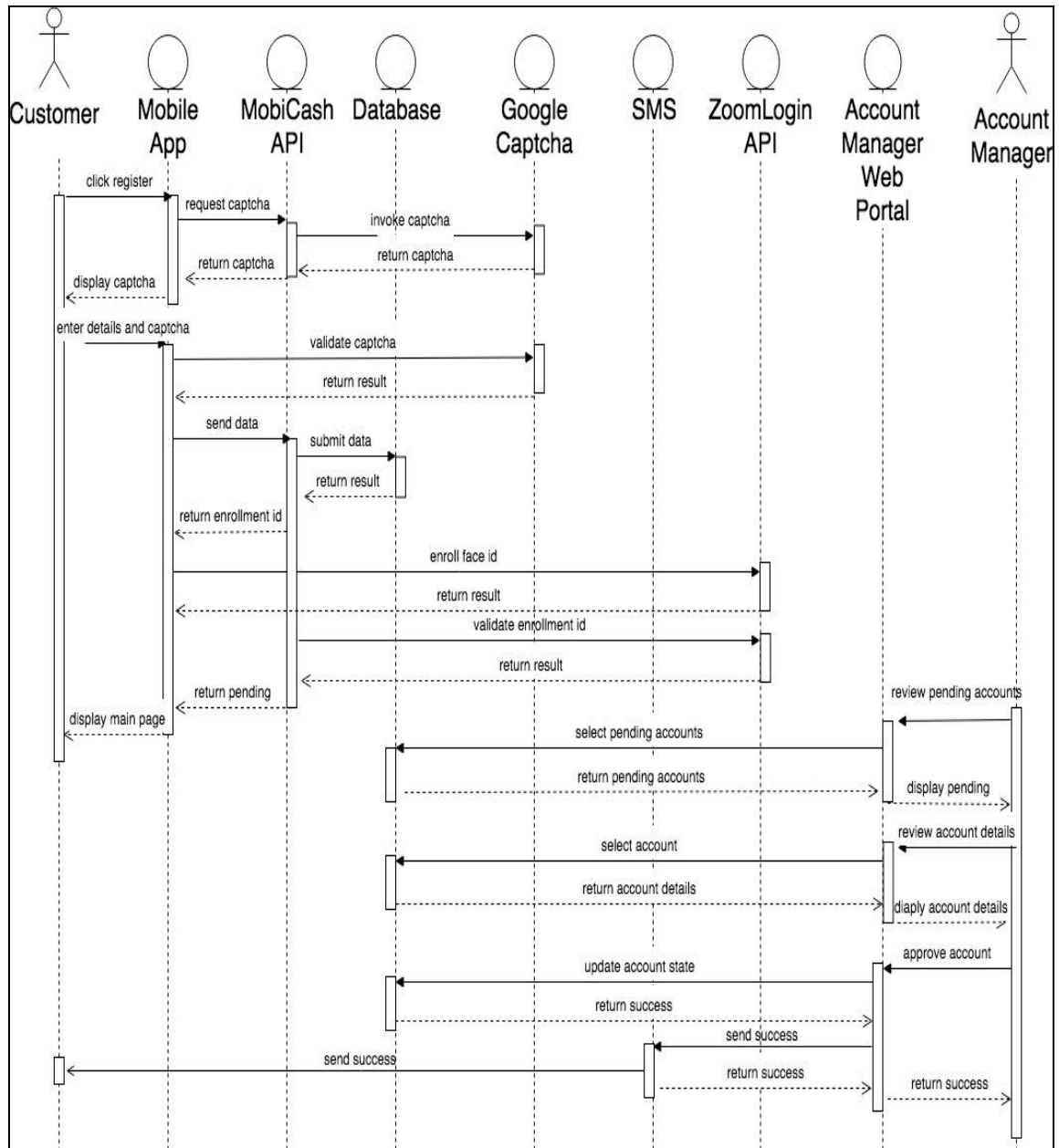


Fig 5: Customer Register Diagram



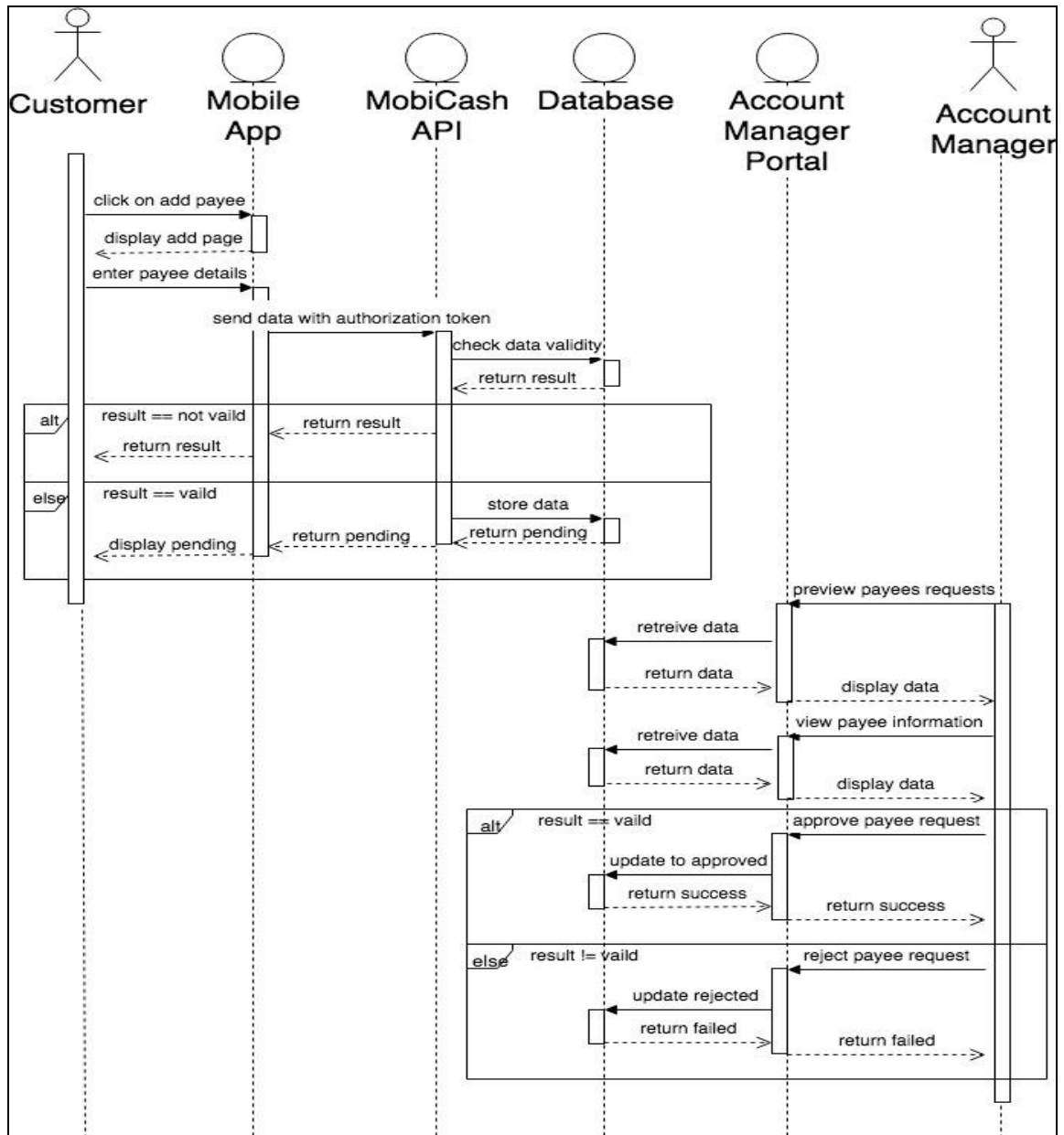


Fig 6: Customer Add payee Diagram

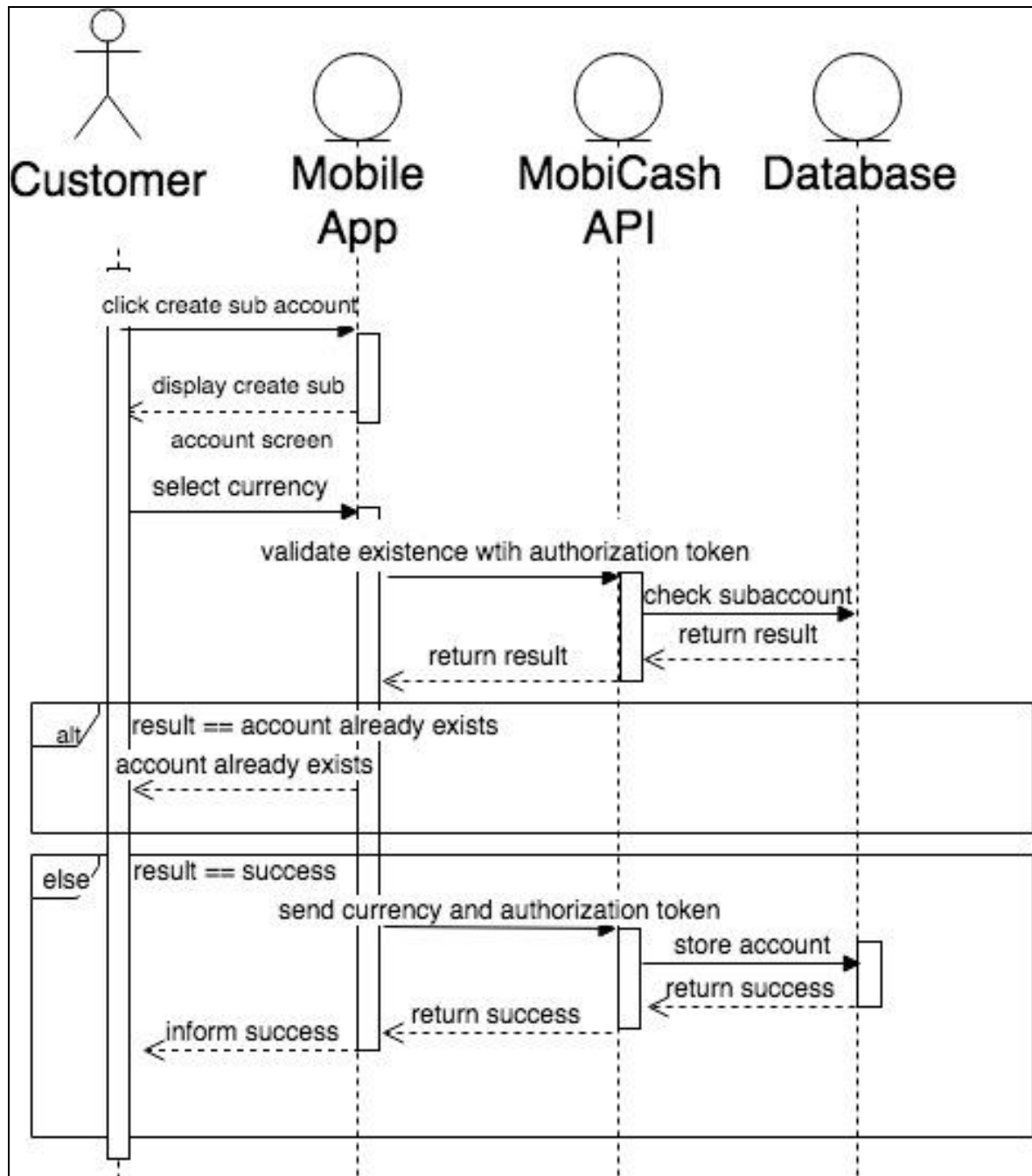


Fig 7: Customer Create Sub-Account Diagram

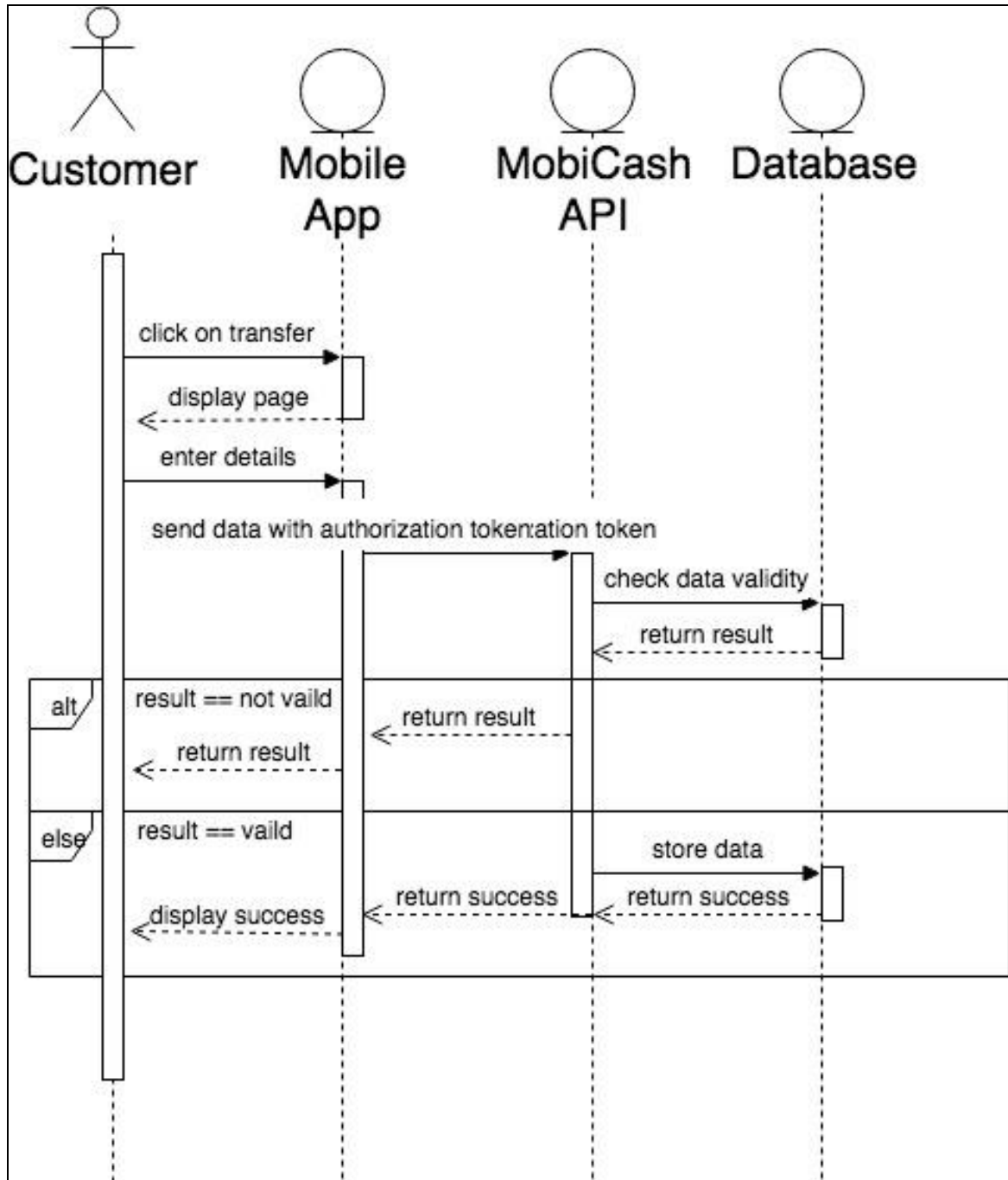


Fig 8 : Customer Submit Transaction Diagram

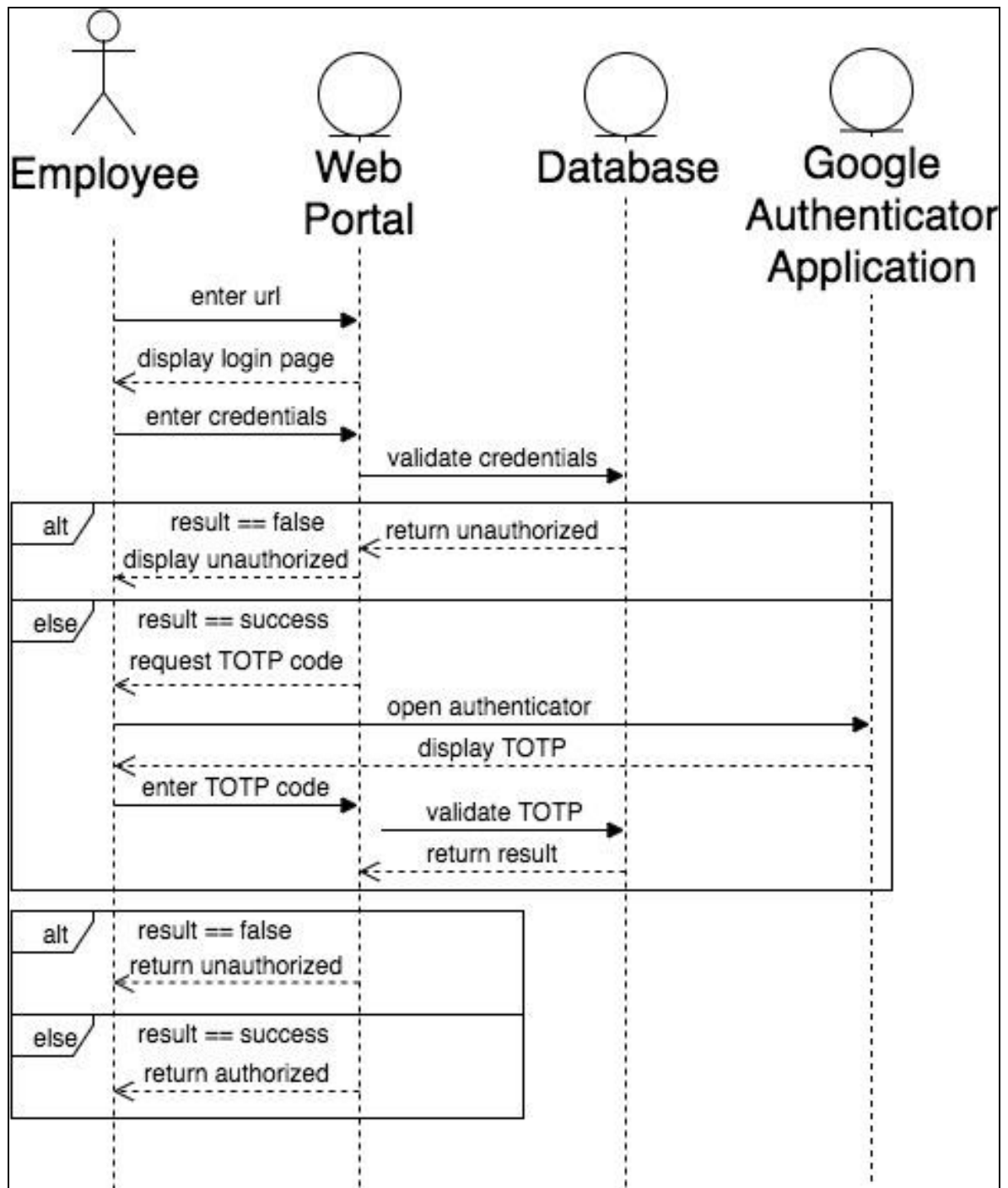


Fig 9 : Employee Login Diagram

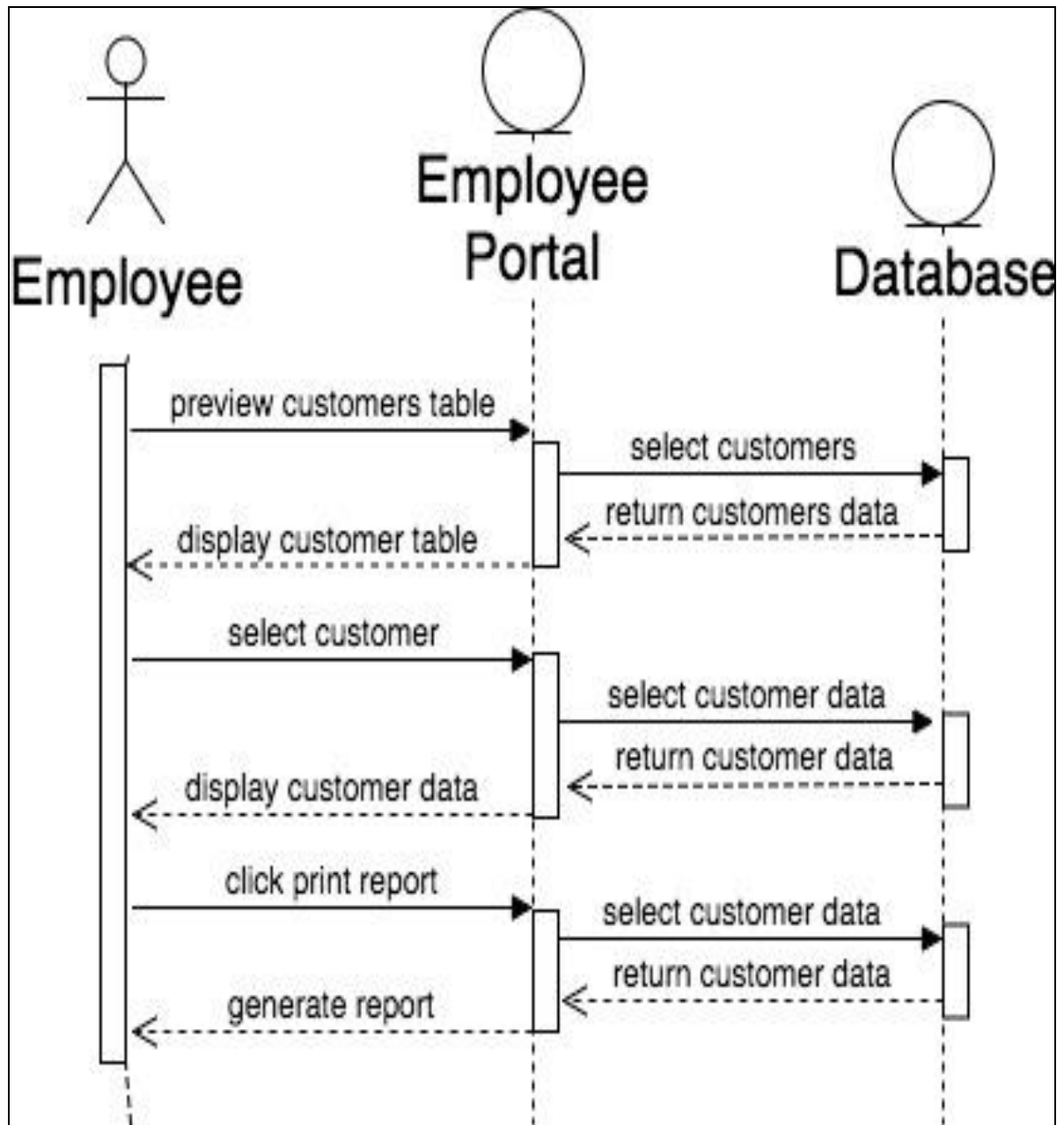


Fig 10 : Employee &amp; Customer Report Diagram

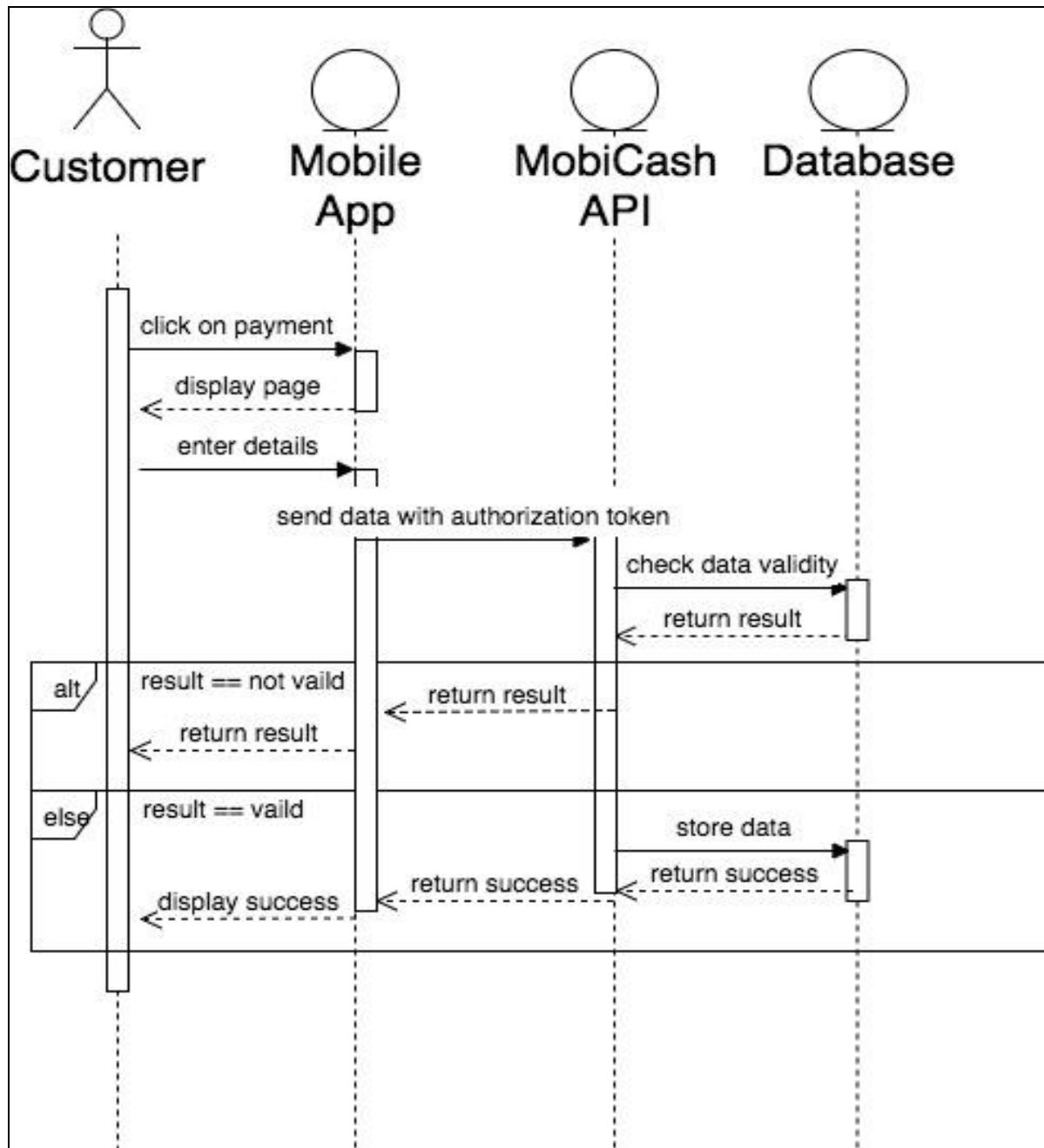


Fig 11: Customer Add Payment Diagram:

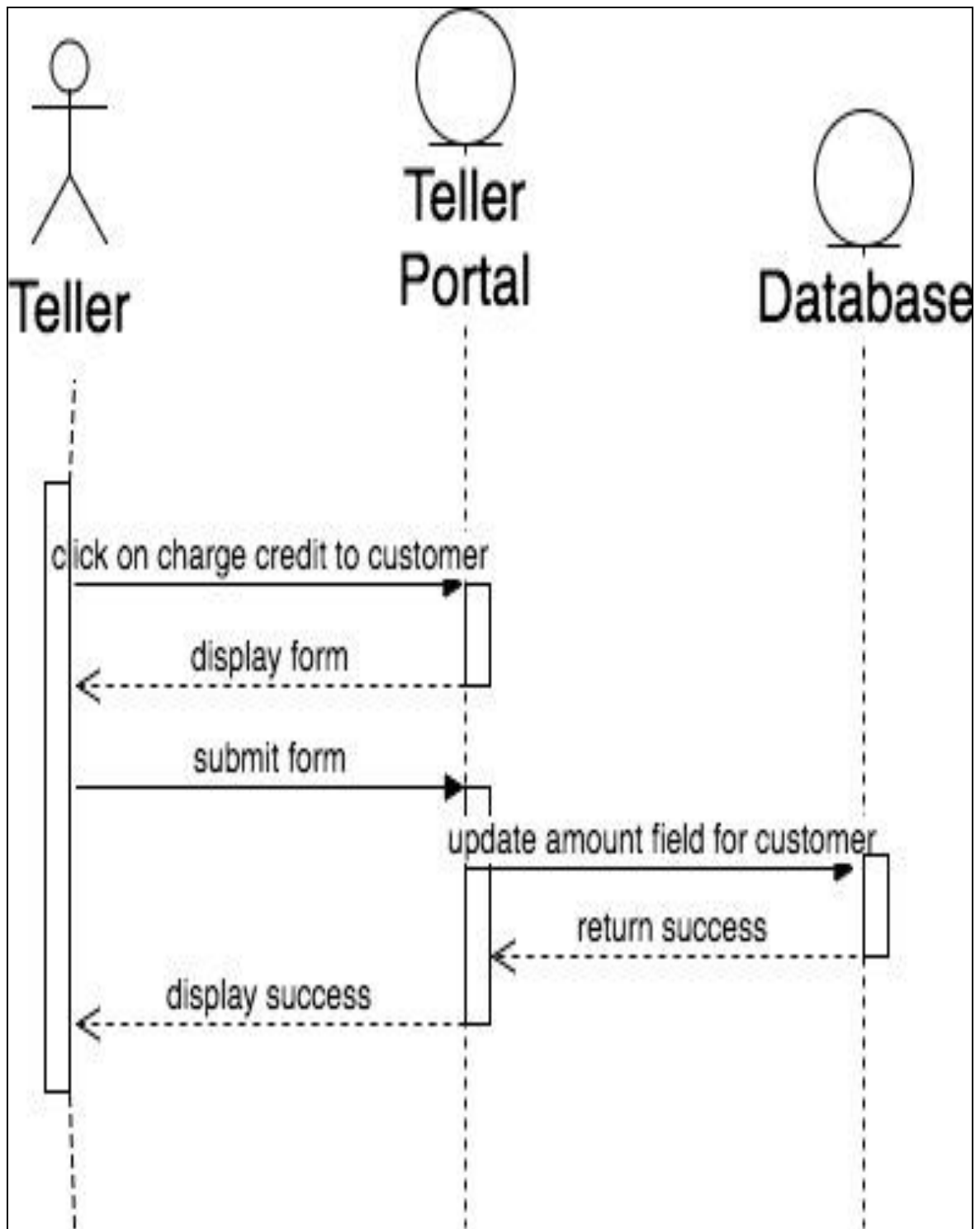


Fig 12: Employee Add Credit Diagram:

### C. Mobile & Web Application Images:

Mobi-Cash had two interfaces, one used by customers and called mobile banking application; second is used by bank employees called mobile web application.

#### C.1 Steps login-on to mobile banking application:

Security Status report of login users include User Geolocation, Face ID, Banking ID and SMS Token as show below Fig 1.

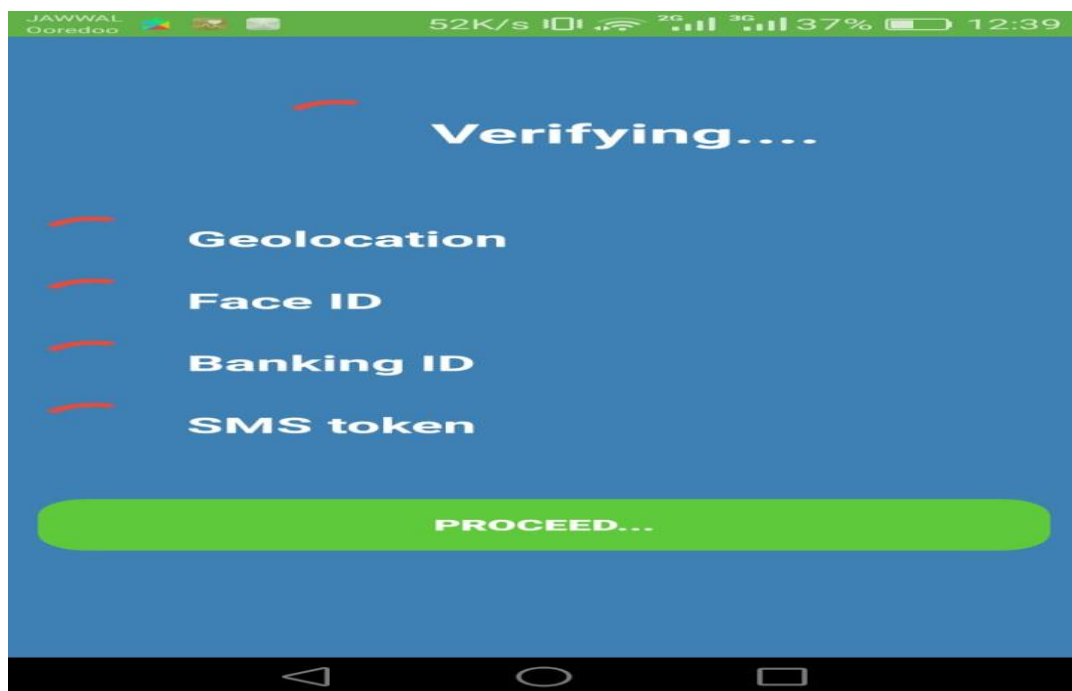


Fig 1: Security Status report



- **Step # 1:** User registration

JAWWAL Wataniya Mobile 780B/s 3G 2G 74% 02:42

**adel**  
Adel Hassan

Phone Number	599672110
Birthdate	1973-08-30
Country	palestine
City	ramallah
Country Code	972
email	adel7377@gmail.com

Home About us User

Fig 2: User Registration Page

- **Step #2:** User Login

JAWWAL Wataniya Mobile 171B/s 3G 2G 69% 01:48

**Mobica\$h**

BANKING-ID  
adel

**SIGN IN**

You don't have account ?  
Sing up

Fig 3: User Login Page

- **Step # 3:** User face capturing

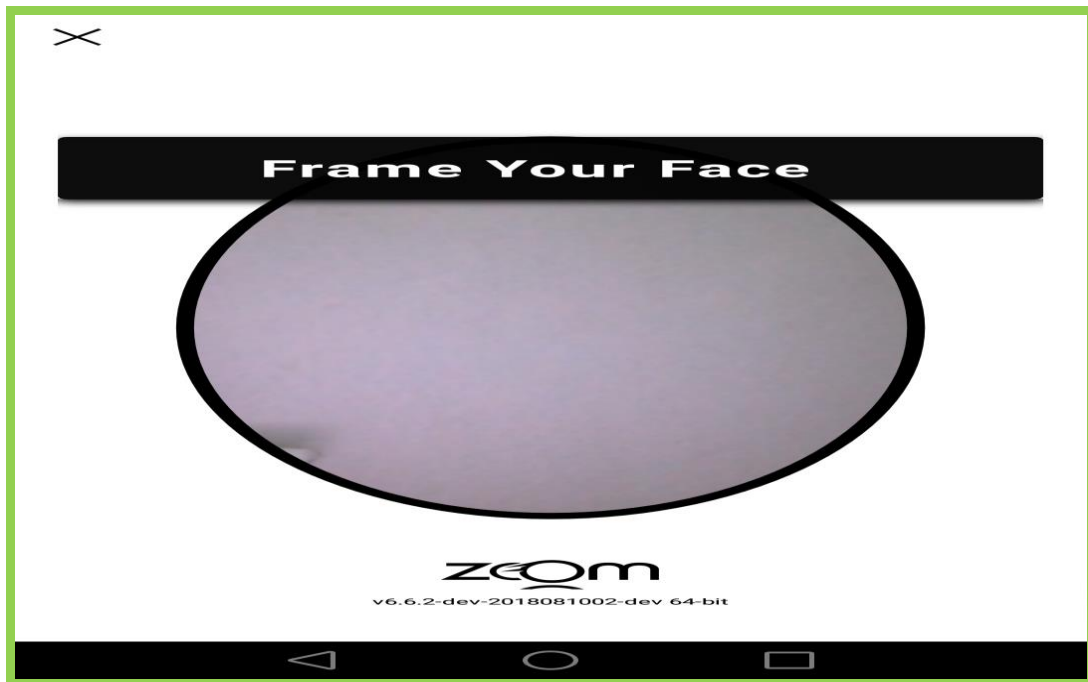


Fig 4: User Face Capture

- **Step # 4:** User creation profile include user account and face image

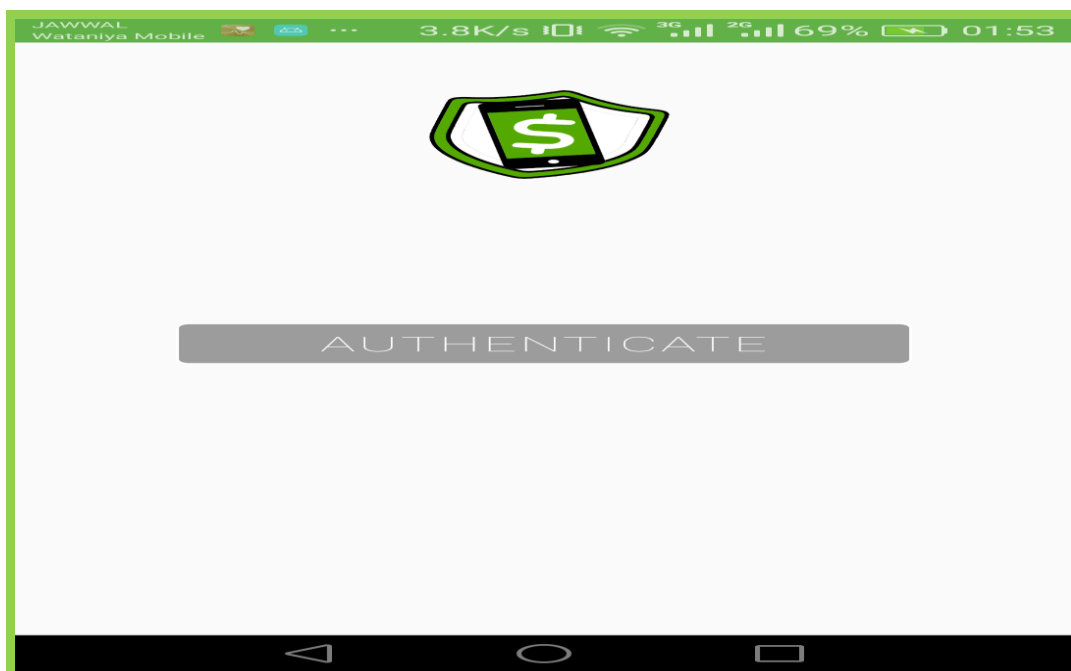


Fig 5: User Authentication Phase

- **Step # 5:** user login mobile banking application, the user captcha entered to go for the next step.

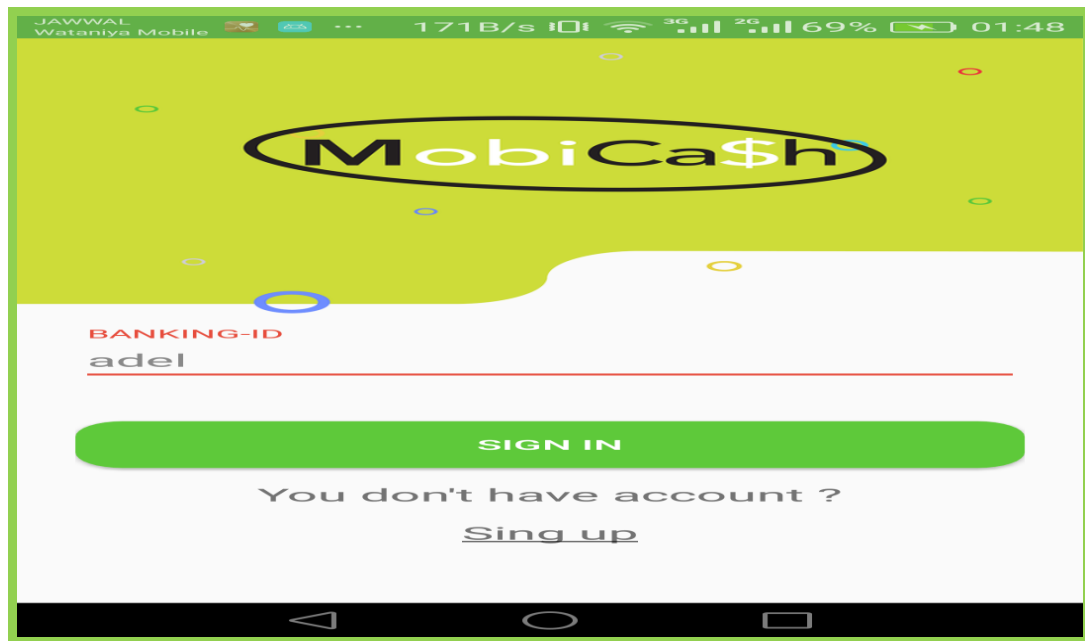
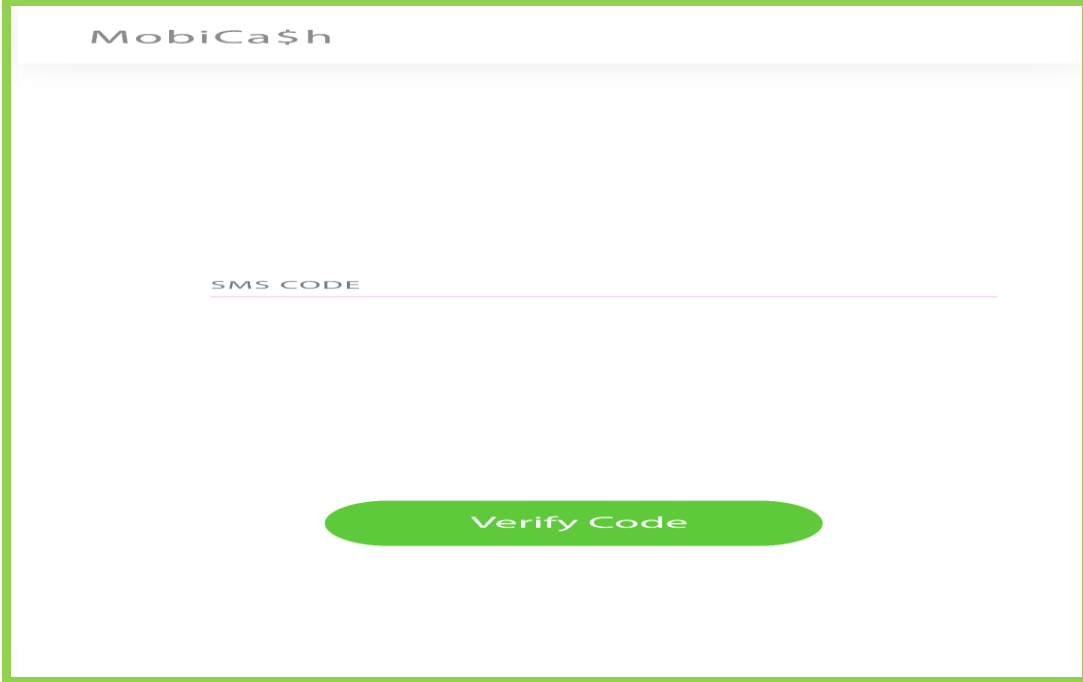


Fig 6: User Login Page after Success Registration

- **Step # 6 :** SMS OTP challange to user logon process



Fig 7: SMS OTP Login Page



MobiCa\$h

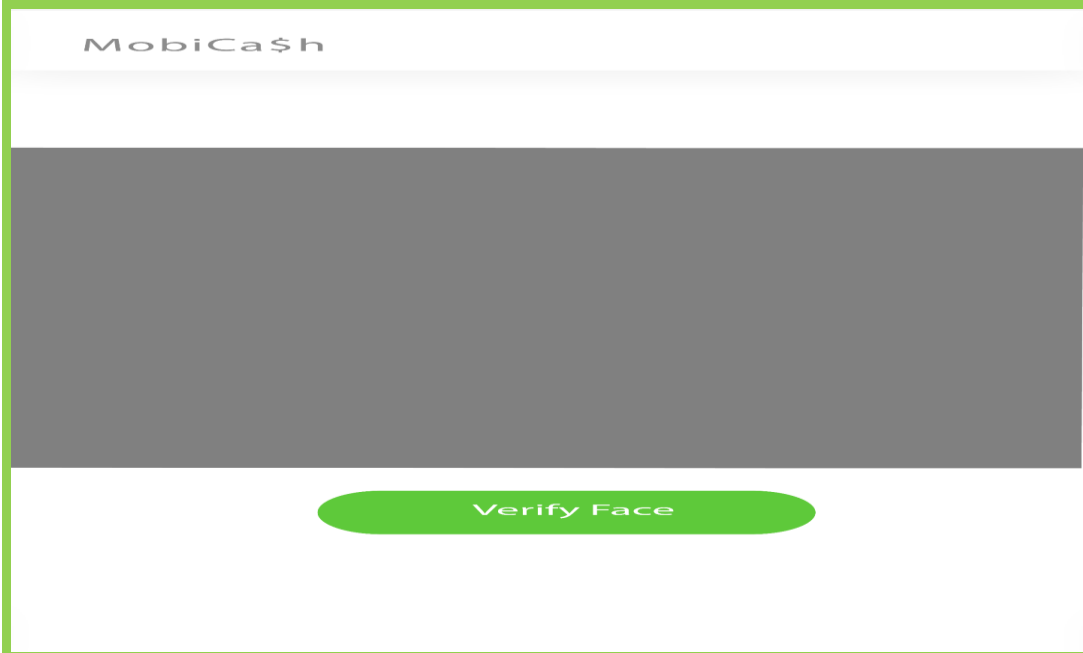
SMS CODE

Verify Code

This is a mobile application screen for SMS OTP verification. It features a white background with a light gray header bar at the top containing the text "MobiCa\$h". Below the header, there is a large, empty rectangular area for entering the SMS code. At the bottom of the screen, there is a green rounded rectangular button with the text "Verify Code" in white.

Fig 8: SMS OTP Verifaction Pahse

- **Step # 7** : face recognition



MobiCa\$h

Verify Face

This is a mobile application screen for face recognition. It features a white background with a light gray header bar at the top containing the text "MobiCa\$h". Below the header, there is a large, solid gray rectangular area for face recognition. At the bottom of the screen, there is a green rounded rectangular button with the text "Verify Face" in white.

Fig 9: Face Recognition Page

- **Step # 8 :** user logon to Mobi-Cash application

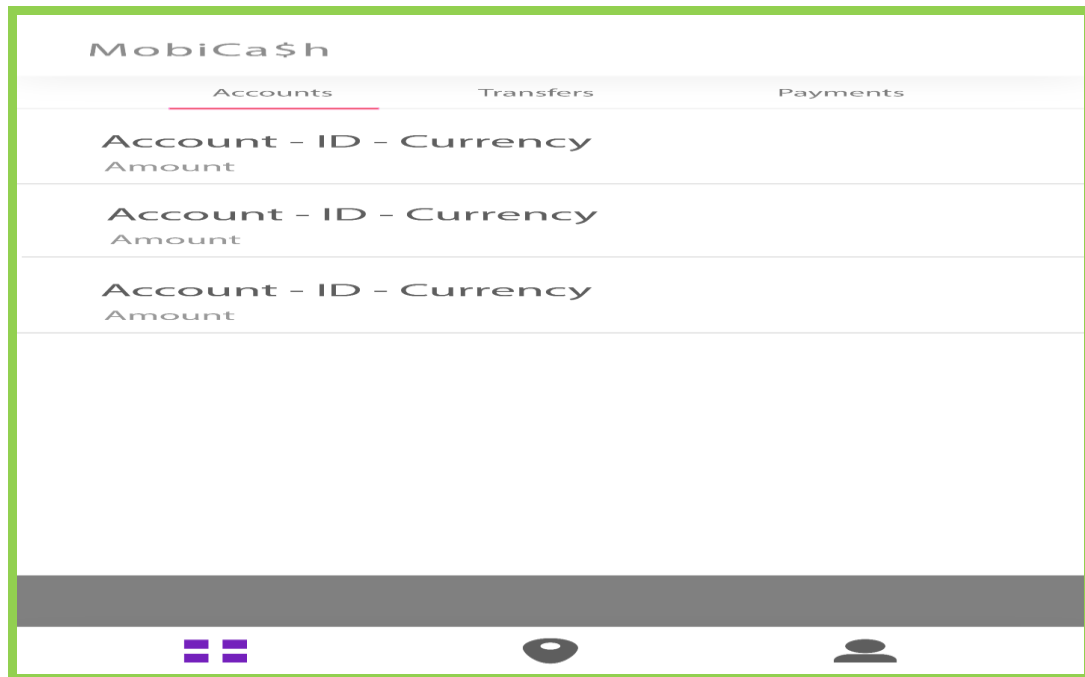


Fig 10: Mobi Cash Login Pages

- Step # 9:** user transfer from accounts process

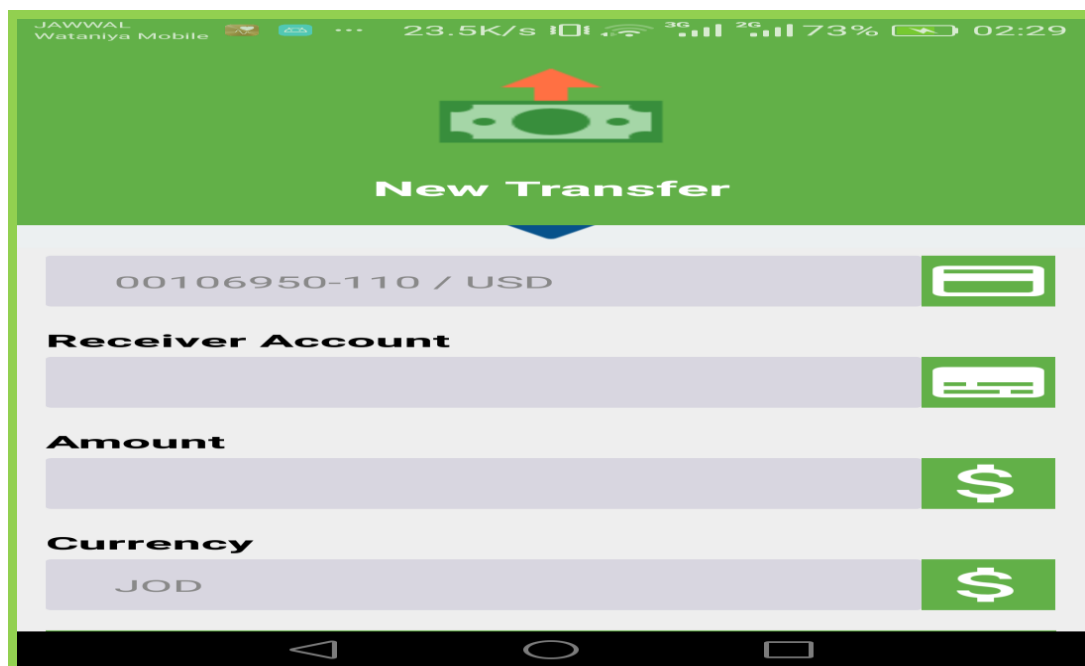
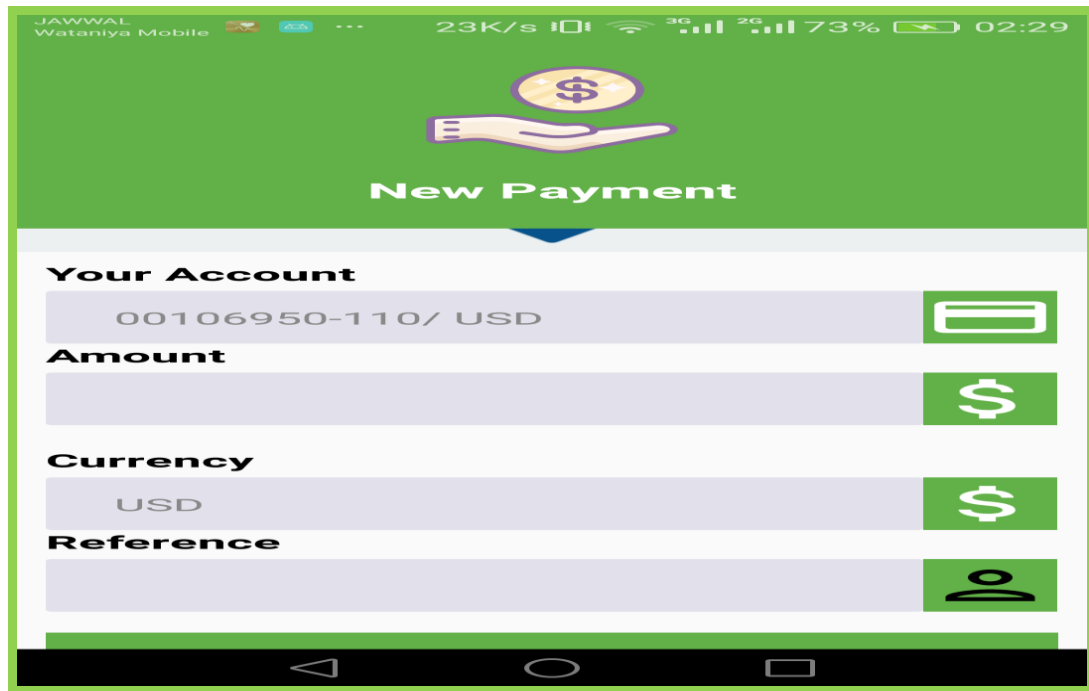


Fig 11 Mobi Cash Tarnsfer Accounts Page

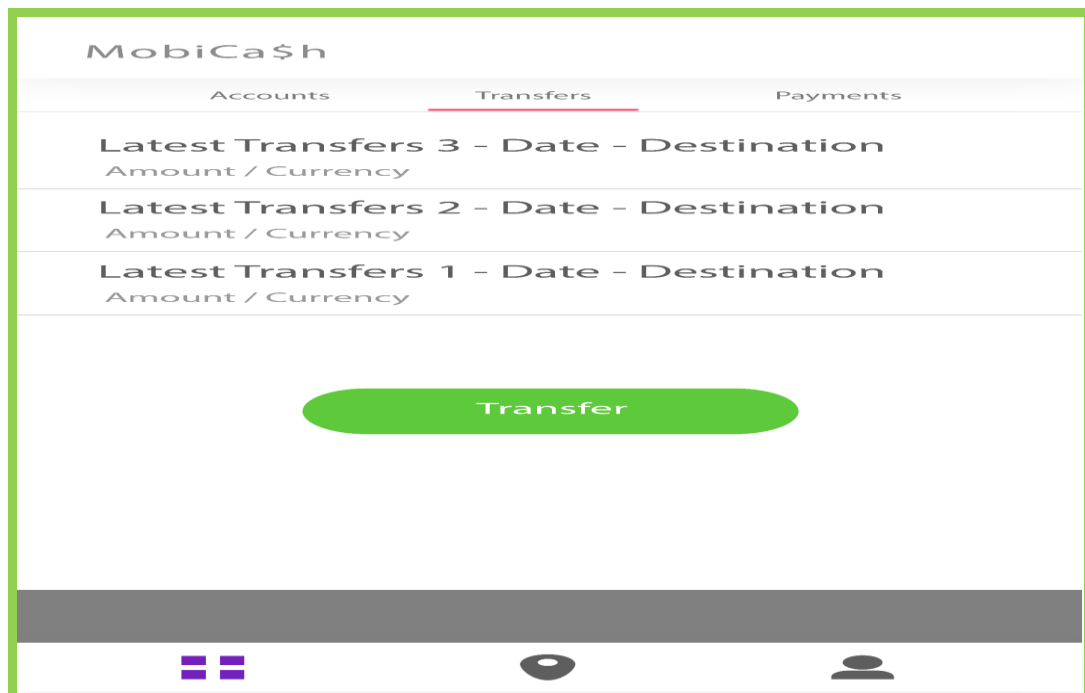


The image shows a mobile application interface for a new payment. At the top, there is a green header with a white icon of a hand holding a coin with a dollar sign. Below the header, the text "New Payment" is displayed. The main content area is divided into four sections, each with a label and a corresponding input field or button:

- Your Account:** A light blue input field containing the text "00106950-110/ USD" and a green button with a white icon of a document.
- Amount:** A light blue input field and a green button with a white dollar sign.
- Currency:** A light blue input field containing the text "USD" and a green button with a white dollar sign.
- Reference:** A light blue input field and a green button with a white icon of a document.

The bottom of the screen shows a black navigation bar with three white icons: a triangle, a circle, and a square.

Fig 12: Mobi Cash New Payment Page



The image shows a mobile application interface for the "MobiCa\$h" app. The top section has a white header with the text "MobiCa\$h". Below the header, there are three tabs: "Accounts", "Transfers", and "Payments". The "Transfers" tab is selected, indicated by a red underline. The main content area displays a list of the latest transfers, each with a title and a subtitle:

- Latest Transfers 3 - Date - Destination**  
Amount / Currency
- Latest Transfers 2 - Date - Destination**  
Amount / Currency
- Latest Transfers 1 - Date - Destination**  
Amount / Currency

Below the list, there is a large green button with the text "Transfer". The bottom of the screen shows a black navigation bar with three white icons: a square, a circle, and a person.

Fig 13: Mobi Cash Trasfer Status

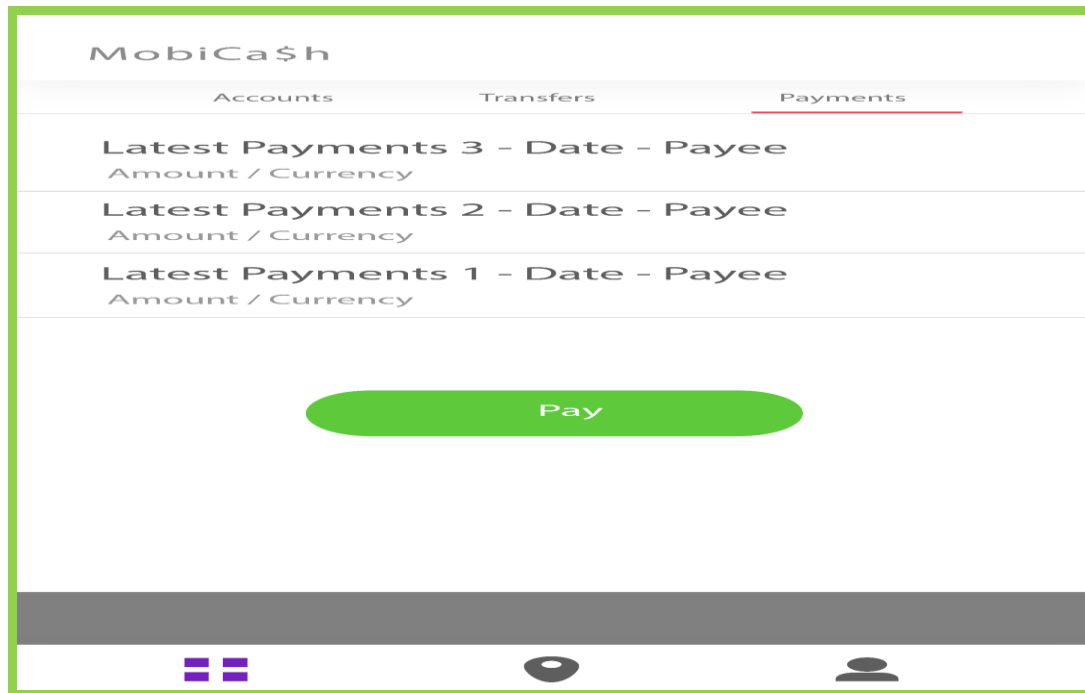


Fig 14: Mobi Cash Payment Status

#### D. Web Application Interface:

Teller uses a web application server website to approve user creation mobile banking application accounts using username and password in addition to OTP SMS as second-factor authentication to log in the system as shown below. Also, the website protected by SSL certificate from Comodo to secure communication channel between the teller and the mobile banking system. Fig 1.

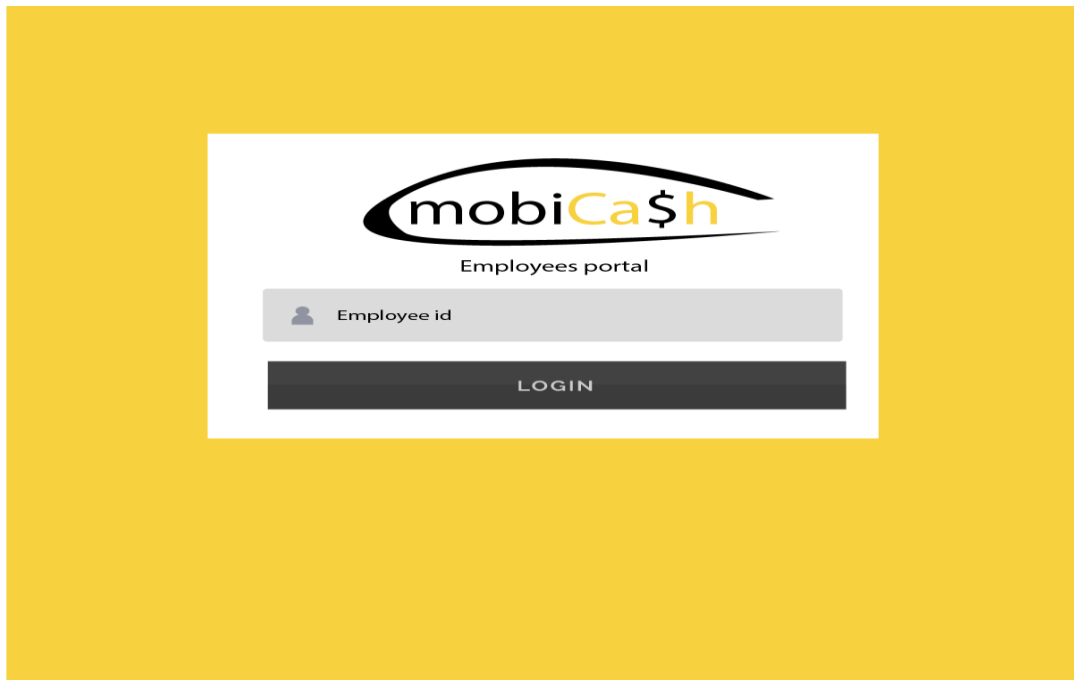


Fig 1: Web Portal Login Page

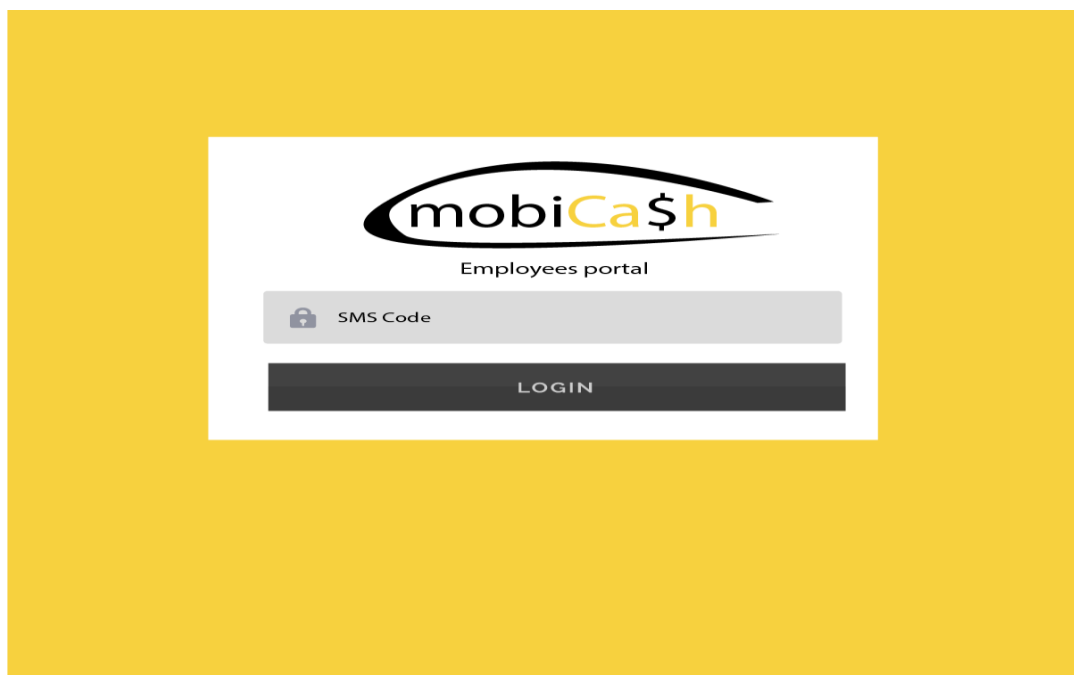


Fig 2 Web Portal SMS OTP Page



### E. Mobile Web Portal Reports:

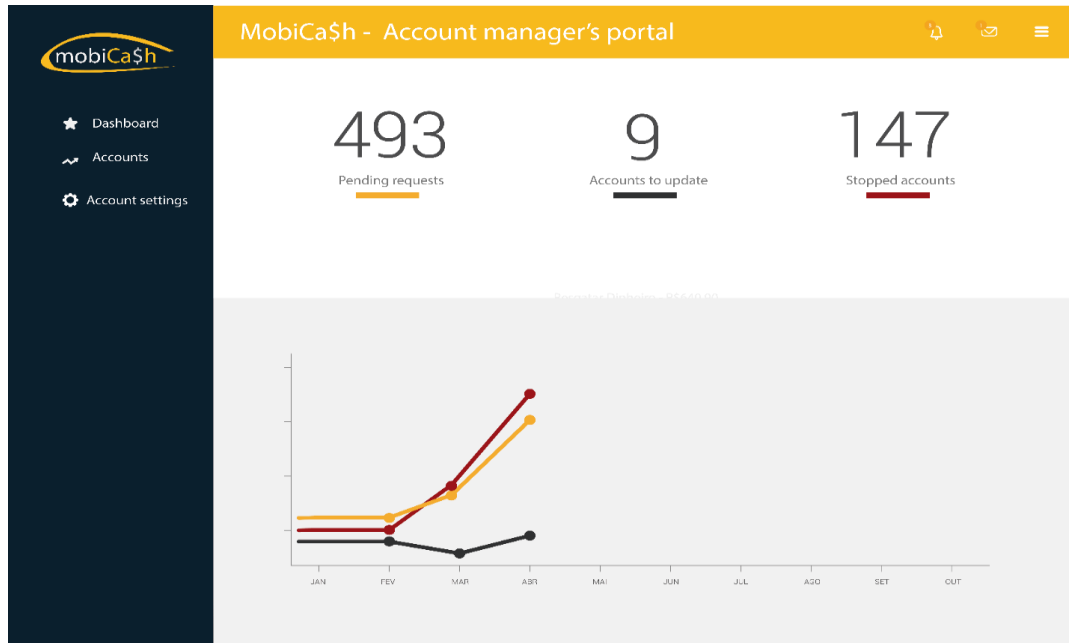


Fig1: Account Manger Portal – Pending Request Statistics

MobiCa\$h - Account manager's portal				
Accounts				Search <input type="text"/>
Date	Account ID	Account user	State	Actions
22/2/2018	AD0120100	Adel Hassan	Pending	
21/2/2018	MA1120100	Mohammed Ahmed	Active	

Fig2: Account Manger Portal – Pending Request Status

## **F: Experts Opinion For System Structure Mobi-Cash:**

### 1. Quoted:

- “ After Reviewing the high level design for the mobile payment system , the design is robust enough in security which is established in a very clear way in using the services of public and private cloud.”
- The design also getting benefit from the cloud services high availability by balancing the services through them.”

2. Cloud comparison result based on questionnaire has a result score of 3.8/5.

3. Security comparison result based on questionnaire has a result score of 4.6/5.

## **G: Mobile Banking Questionnaire and Experts response for our system structure (Mobi-Cash):**

### **Mobile Banking Questionnaire**

Arab American university of Palestine, faculty of graduate studies

This survey allows us to obtain information that will help in our master’s degree research in building a secure payment model using mobile banking system. Please answer the question to the best of your knowledge.

#### 1. Personal Information:

- Name:
  - Email:
  - Position:
2. Are you using mobile banking services? Yes ( ). No ( ).
3. Do you have an experience in cloud services? Yes ( ). No ( ).
4. How often are you using the mobile banking?
- Daily ( ).
  - Weekly ( ).

- Monthly ( ).
  - Rare ( ).
5. Do you have a problem with remembering your banking password? Yes ( ). No ( ).
  6. Do you trust that your password is secure enough to protect your account? Yes ( ). No ( ).
  7. Do you think using biometric service in authentication process of mobile banking will be more secure? Yes ( ). No ( ).
  8. Do you think follow local regulations and international standards such as PCI is important? Yes ( ). No ( ).
  9. Fill the fields with numbers 1 (Low) to 5 (High) to describe each row item according to the cloud topology in the columns.

Item Discription	Private Cloud	Public Cloud	Hybrid Cloud (Private +Public)	Hybrid Cloud (Private+ Private)
Data Security				
Cost Variations				
Control				
Compliance				
Service Level Agreement				
Data Transfer & Integrations				
Compatibilities of Applications & Programs				
Performance				
Availability				
IT Operation Models & Organizational Structure				
Time and Resources				
Fast Deployment and Productivity				
Scalability and Flexibility				
Non-Lock-In				
Management and Migration				

10. From security perspective, to what extent do you agree with the following statements:

Item Discription	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Access using Username / Password					
Access using Biometric					
Data Storage Security (Encryption)					
Data Privacy					
Location Privacy					
Control					
Compliance					
Secure data communication					
Data Confidentiality					
Access Control					
Availability					
Data Integrity					
Identity Protection					

**Any other suggestions:**

-----  
 -----

**Signature:**

THANK YOU VERY MUCH FOR YOUR VALUABLE TIME AND INFORMATION

## الملخص

تهدف هذه الرسالة إلى تقديم نموذج جديد لتحليل وتصميم وبناء وتطوير تطبيقات الهاتف المحمول المستخدم في عمليات الدفع الالكتروني في القطاع المصرفي في فلسطين بما فيها الناحية الامنية وناحية تجهيزات البنية التحتية الخاصة بها ،وتكون مبنية على أساس بيئة سحابية هجينة.

لقد قمنا في هذه الرسالة بعمل دراسات بحثية معمقة تعني باصول بناء وتصميم تكوينات تطبيقات الهاتف المحمول وطرق التراسل وتحليل الصور في بيئة ديناميكية معقدة وانية.

سوف تمر عملية التصميم والبناء للنموذج الجديد بثلاثة مراحل.

أولاً ، سنقوم ببناء وإعداد مكونات الأجهزة والبرمجيات الخاصة بتطبيقات الهاتف المحمول والبنية التحتية الخاصة به.

ثانياً ، استخدام طريقة المصادقة دون الحاجة إلى كلمة مرور "لا داعي لكلمة المرور: "لا يكفي تغيير سياسات كلمة المرور فقط وحن الوقت لتحويل المصادقة." ثالثاً ، بناء نموذج امتثال للتعامل مع المعايير المحلية والدولية مثل لوائح سلطة النقد الفلسطينية (PMA) ولوائح صناعة بطاقات الدفع (PCI).

ان طرق الدفع الموجودة حالياً في السوق الفلسطيني لها أشكال مختلفة من الدفع مثل الدفع النقدي ، أو الدفع عن طريق بطاقات السحب وبطاقات الائتمان وغيرها ، وبهذا ستوفر هذه الرسالة طريقة جديدة للدفع باستخدام الهواتف المحمولة لتسهيل قيام الأشخاص بتسديد فواتيرهم ودفع ثمن السلع والخدمات التي يشترونها.

حيث اننا سنعتمد في عملية تطوير تطبيق الخدمات المصرفية عبر الجوال باستخدام برنامج مفتوح المصدر لبناء معظم مكونات النظام. كما انه أيضًا ، سوف يتم بناء التطبيقات والخوادم الرئيسية علي بيئتين مختلفتين ، واحدة منهما ستكون علي بيئة داخل المؤسسة والثانية في علي بيئة السحابة الهجينة.

كما انه سنستخدم في عملية تسجيل الدخول للأشخاص وعملاء البنك من خلال تطبيق الجوال بطريقة آمنة وذلك باستخدام المصادقة الثنائية (2FA) وإزالة كلمة مرور التقليدية واستبدالها بمستويين من المصادقة.

أولاً ، سنستخدم رمزًا عشوائيًا فريدًا يتم إنشاؤه بواسطة النظام الأساسي للنظام ومن ثم أرسل اسم المستخدم كرسالة نصية إلى جهاز المستخدم.

ثانيًا ، استخدام عملية التقاط صورة الوجه للتحقق من صلاحية المستخدم للوصول إلى التطبيق.

وفي النهاية لابد من ذكر انه وعلي الصعيد العالمي بان أنظمة الدفع الالكترونية تحكمها العديد من التشريعات والقوانين التي يجب اتباعها من قبل جميع المؤسسات التي تقوم بتقديم الخدمات المالية ، من التشريعات والقوانين المتبعة محليا في السوق الفلسطيني يتم إصدارها من قبل سلطة النقد الفلسطينية، والاخري عالميا يتم اصدارها بواسطة كبري الشركات العالمية مثل شركتي فيزا و ماستر كارد.