Sudan University of Science and Technology

Collage of Graduate Studies

USER AUTHENTICATION USING SMART PHONE AND ONE TIME PASSWORD

التحقق من المستخدم بإستخدام الهاتف الذكي وكلمة السر لمرة واحدة

A Thesis Submitted in Partial Fulfillment of the Requirements of M.Sc. in Computer Science (Information Security Track)

Prepared By: Abdelmagid Gafer Abdelmagid Tatai

The Supervisor: Dr. Faisal Mohammed Abdallah

July 2017

Sudan University of Science and Technology

Collage of Graduate Studies

USER AUTHENTICATION USING SMART PHONE AND ONE TIME PASSWORD

التحقق من المستخدم بإستخدام الهاتف الذكي وكلمة السر لمرة واحدة

A Thesis Submitted in Partial Fulfillment of the Requirements of M.Sc. in Computer Science (Information Security Track)

Prepared By: Abdelmagid Gafer Abdelmagid Tatai

The Supervisor: Dr. Faisal Mohammed Abdallah

July 2017

الآيـــة

قال تعالى:

(هُوَ ٱلَّذِيٓ أَنزَلَ عَلَيۡكَ ٱلۡكِتَٰبَ مِنۡهُ ءَايَٰتٞ مُّحۡكَمَٰتٌ هُنَّ أُمُّ ٱلۡكِتَٰبِ وَأُخَرُ
مُتَشَٰبِهَٰتٞۖ فَأَمَّا ٱلَّذِينَ فِي قُلُوبِهِمۡ زَيۡغٞ فَيَتَّبِعُونَ مَا تَشَٰبَهَ مِنۡهُ ٱبۡتِغَآءَ ٱلۡفِتۡنَةِ
وَٱبۡتِغَآءَ تَأۡوِيلِهِۦۖ وَمَا يَعۡلَمُ تَأۡوِيلَهُۥٓ إِلَّا ٱللَّهُۗ وَٱلرَّٰسِخُونَ فِي ٱلۡعِلۡمِ يَقُولُونَ
ءَامَنَّا بِهِۦ كُلّٞ مِّنۡ عِندِ رَبِّنَاۗ وَمَا يَذَّكَّرُ إِلَّآ أُوْلُواْ ٱلۡأَلۡبَٰبِ)

صدق الله العظيم

سورة آل عمران الآية ﴿7﴾

الحمد لله

الحمد لله الذي خلق كل شيءٍ وقدّره، الحمد لله الذي له الأمر جميعاً ومدبره

الحمد لله الأول لا شيء قبله، الحمد لله الآخر لا شيء بعده الحمد لله الظاهر فوق كل شيء وقاهره، الحمد لله الباطن لا يخفى عليه شيء ومُبصره، الحمد لله مالك الملك كله وحاكمه، الحمد لله الحي الذي لا يموت الحمد لله بعدد ما خلق، الحمد لله ملئ السموات والأرض.

الحمد لله في سرِّي وفي علني ... والحمد لله في حُزني وفي سَعدي
الحمد لله عمّا كنت أعلَمُهُ ... والحمد لله عَمَّا غابَ عن خَلَدي
الحمد لله من عمَّت فضائلُه ... وأنعُمُ الله أعيت منطِق العددِ
فالحمد لله ث مَّ الشُكرُ يتبَعُه ... والحمد لله عن شكري وعن حمدي

DEDICATION

Who taught me how to take the science of wealth ... To whom I try to achieve a dream as long as he sees...

To who gave me the fruits of his life ... To who taught me patience ...

My father...

To the big heart ... To the rivers of tender tenderness ... And tried to grow up... To who will the heaven rise under their feet ... To who was her prayer the secret of our progress

My Mother...

To those who were almost ready to be apostles ... To those who enlightened our way with their knowledge ...

My distinguished teachers...

To those who joined us the path ... To whom we met with them without time were the sweetest memories ...

My friends...

To those who dream together ... To those who share the sweetness of life and happiness ... To whom we wish all beautiful ...

Our brothers...

ACKNOWLEDGEMENT

Thanks first and foremost to God Almighty who honored us in accomplishing this humble work, and I would like to express my deepest appreciation to all those who provided me the information to complete this research.

A special gratitude I give to my research supervisor, who contribution in stimulating suggestions and encouragement helped me to coordinate my project especially in writing this report.

Dr. Faisal Mohammed Abdallah

Furthermore I would also like to acknowledge with much appreciation the crucial role of the.

Sudan University of Science and Technology Collage of Graduate Studies

Last but not the least, I would like to thank my family:, for help me and supporting me spiritually throughout my life.

My parents, brothers and my sisters

ABSTRACT

Authentication is the process of verifying a user's identity when the user is requesting services from any secure IT system, the default for all user logons whether local or remote has always been reliant upon the humble password, in the past this has been good enough, but now days that we used to conduct our world and business using password for authentication is not secure any more.

A more secure method is this thesis proposed the two-factor authentication that verifies not only the username/password pair, but also requires a second factor to authenticate.

The proposed method is been implemented using asp.net and java android, this method is been analysis for most know attack and the result obtain is reasonable in term of security attack.

technical application is been developed that provides a high level of protection through the use of a two factor authentication mechanism via one time password technology, where the first factor is the user name and password, and the second factor is the generated one time password by smart phone.

المستخلص

التحقق هو عملية التأكُد من هوية المستخدم عندما يطلب المستخدم خدمات من أي نظام تقني آمن، وفي الوضع الافتراضي فأن جميع عملية تسجيل الدخول للمستخدمين الي حساباتهم تعتمد دائما على كلمة المرور الضعيفة، في الماضي كان هذا جيدا بما فيه الكفاية، ولكن في الحاضر لإجراء اعمالنا والأعمال التجارية باستخدام كلمة المرور للتحقق ليست آمنة بما فية الكفاية.

هناك طريقة أكثر أمنا مقترحة في هذا البحث وهي التحقق ثنائي المعامل الذي يتحقق ليس فقط اسم المستخدم و كلمة السر ، ولكن يتطلب أيضا عاملاً ثانيا للتحقق.

تم تنفيذ الطريقة المقترحة باستخدام asp.net و جافا (اندرويد)، وقد تم في هذا الأسلوب تحليل لمعظم الاختراقات الشائعة وكانت النتيجة الحصول على مستوي مقبول من الحماية.

وقد تم تطوير تطبيق تقني الذي يوفر مستوى عال من الحماية من خلال استخدام عاملي تحقق، يتمثل العامل الاول في اسم المستخدم وكلمة المرور بينما يتمثل العامل الثاني في كلمة السر لمرة واحدة التي لاتتكرر التي يتم توليدها عن طريق الهاتف الذكي للمستخدم.

.

Table of contents

CHAPTER ONE: INTRODUCTION

1.1 INTRODUCTION 1

1.2 THE PROBLEM 1

1.3 SIGNIFICANCE 2

1.4 HYPOTHESIS 2

1.5 OBJECTIVE 2

1.6 SCOPE.. 2

1.7 METHODOLGY 3

1.8 THESIS LAYOUT.. 4

CHAPTER TWO: THEORETICAL BACKGROUND & RELATED WOERKS

2.1 THEORETICAL BACKGROUND.. 5

2.1.1 PASSWORD 5

2.1.2 ONE TIME PASSWORD 6

2.1.3 CRYPTOGRAPHY.. 6

2.1.4 ENCRYPTION AND DECRYPTION.. 6

2.1.5 DATA ENCRYPTION STANDARD (DES).. 7

2.1.6 TRIPLE DATA ENCRYPTION STANDARD ALGRITHM.. 8

2.1.7 ADNAVCED ENCRYPTION STANDARD.. 8

2.1.8 AUTHENTICATION.. 8

2.1.9 TWO FACTOR AUTHENTICATION.. 9

2.2 RELATED WORK.. 10

CHAPTER THREE: METHODOLOGY

3.1 INTRODUCTION.. 14

3.2 SYSTEM COMPONENTS AND PLATFORM 14

3.3 HOW OTPs ARE GENERATED AND DISTRIBUTED 14

3.4 HOW THE SYSTEM WORKS 15

3.5 SYSTEM ENVIRONMENT 16

3.6 SYSTEM ANALYSIS 17

3.7 USE CASE DIAGRAM 17

3.8 SEQUENCE DIAGRAM 18

3.13 DEPLOYMENT DIAGRAM FOR SYSTEM COMPONENTSs 24

CHAPTER FOUR: IMPLEMENTATION

4.1 INTRODUCTION 25

4.2 SYSTEM SCREENS 25

4.2.1 REQUEST FOR ONE TIME PASSWORD SCREEN 25

4.2.3 THE LOGIN SCREEN FRO WEBSITE 29

4.2.4 THE MAIN SCREEN FOR ADMINISTRATOR SCREEN 31

4.2.5 USERS AND ACCOUNTS MANAGEMENT SCREEN 32

4.2.6 THE MAIN SCREEN FOR CUSTOMER 34

4.2.7 BALANCE STATEMENT SCREEN 35

4.2.8 DEPOSIT SCREEN 35

4.2.9 WITHDRAW SCREEN 36

4.2.10 BALANCE TRANSFER SCREEN 37

4.3 RESULTS 37

4.4 DISCUSSION AND ANALYSIS 38

4.4.2 MAN IN THE MIDDLE ATTACK 38

4.4.2 BRUTE FORCE ATTACK 38

4.4.2 STEAL OR LOSEU USER’S SMART PHONE 39

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1 CONCLUSION 40

5.3 RECOMMENDATIONS 40

REFERENCE 41

LIST OF FIGURES

Figure Number	Figure Name	Page Number
1.1	illustrates steps and system components	4
3.1	illustrates the UML Activity Diagram	16
3.2	illustrates the operations that can be performed by the customer	18
3.3	illustrates the Login operations that can be performed by the customer	19
3.4	illustrates the balance statement operations	20
3.5	illustrates the deposit operations	21
3.6	illustrates the withdraw operations	22
3.7	illustrates the balance transfer to another account operation	23
3.8	illustrates the Deployment Components	24
4.1	illustrates the system login page	25
4.2	illustrates the system login page	26
4.3	illustrates the serial number of smartphone not register	27
4.4	illustrates the system login page	28
4.5	illustrates the system login page	29
4.6	illustrates invalid username or password	30
4.7	illustrates the entered one time password expire	30
4.8	illustrates the entered one time password Mismatch	31
4.9	illustrates the main screen of system administrator	31
4.10	illustrates the main operations for system administrator	32
4.11	illustrates viewing users by system administrator	32
4.12	illustrates user creation	33
4.13	illustrates view all customer accounts	33
4.14	illustrates create account	34

4.15	illustrates the main screen for customer	34
4.16	illustrates balance statement	35
4.17	illustrates the deposite operation	35
4.18	illustrates the withdraw operation	36
419	illustrates the balance transfer operation	37

Abbreviation Table

Abbreviation	**Description**
2FA	Two factor authentication
3DES	Triple Data Encryption Standard
AES	Advance Encryption Standard
DES	Data Encryption Standard
E-mail	Electronic Mail
IDE	Integrated Development Environment
IMEI	International Mobile Equipment Identity
iOS	iPhone Operating System
J2ME	Java 2 Micro Edition
MAC	Media Access Control
MMS	Multi Media Messaging Service
OTP	One time password
QR	Quick Response
TFA	Two factor authentication
UML	Unified Modeling Language

Chapter One

(INTRODUCTION)

1.1. INTRODUCTION

With the development of science and technology and means of storage and exchange of information in different ways, or so-called transfer of data across the network from site another site, became to look at the security of data and information is important; we need to provide protection for the information of the dangers that threaten them or attack them through the use of tools to protect information from internal or external threats. In addition to the procedures adopted to prevent access information into the hands of unauthorized persons through communications and to ensure the authenticity of these communications.

1.2 THE PROBLEM

In recent years, increased interest institutions and organizations in the security aspects of their networks and systems, and among these aspects to verify that the person requesting access to the system that he is the person who claims that he/she is, this process called Authentication, in most systems are using a password only to access the system for login process. Below are some problems and risks for the use of password in the user authentication process:

- Recently it became Breakthroughs systems, websites and personal accounts are a large and different ways, because of weak protection of those systems methods so it was necessary to find ways more secure to protect those systems.
- Passwords become easier to guess [1].
- Short passwords are easy to guess and crack [1].
- Equipment and software often has standard pre-configured passwords (default passwords) [2].
- Most people they have many account use same password for all these accounts [2].

1.3 SIGNIFICANCE

With the development of computer science progressed accordingly ways to hack, and different ways plus sensitivity of data; as a result, the greater the need to find solutions to overcome the weaknesses those hackers exploits it, we will give a proposal for two level user authentications to access the system.

1.4 HYPOTHESIS

- Using password only not enough for login process.
- Smart phone can be used to generate one time password.
- Smart phone in authentication process can be lower cost.
- Use a password just in the verification that can claim to significant financial losses, such as bank accounts and transactions.

1.5 OBJECTIVES

- Avoid the risks related to the use password.
- Limit the unauthorized access to accounts.
- Verification of the person requesting access to the system.
- Building authentication process with low cost.
- To take advantage of users smartphone's.

1.6 SCOPE

This research is limited to smart phones that have Android operating system and are used in applications and systems requiring a high level of verification, such as bank applications, and social accounts.

1.7 METHODOLGY

The methodology used in this research is to construct a verification application, which can be used as an interface login for sensitive systems such as banking systems and personal accounts.

The server machine is configured and deploy the bank website into it and configure smart phone by install the android application into it.

The smart phone connect to server through the internet or the company network where the client computer request the service in the server, and the server to provide the service after being verified through the application in the smart phone of the user and it generate and send a one time password to smart phone.

I will conduct and apply below steps to achieve proposed goal:

- Write application to represent as middle ware with android OS to authenticate and bypass authorize user to target server.
- Encryption channel between application (middle ware) and target server.
- User enter your username and password on android app installed in user smart phone, then get one time password appear in mobile.
- The user enter generated one time password in target web site if the one time password correct and valid then login successfully.

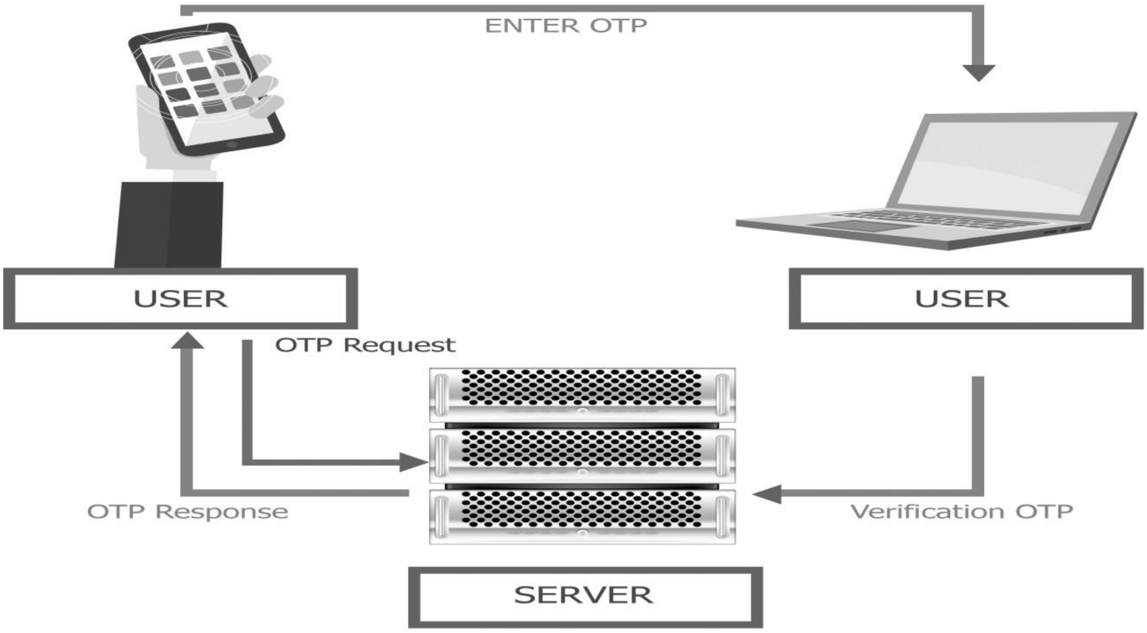


Figure (1.1) illustrates steps and system components

1.8 THESIS LAYOUT

Chapter one gives introduction about the project, defining the problem, objectives, methodology and scope. Chapter two represents Theoretical background and related work. Chapter three contains methodology. The chapter four contains implementation and result. Chapter five is contains conclusion and recommendations.

Chapter Two

(THEORETICAL BACKGROUND & RELATED WOERKS)

2.1 THEORETICAL BACKGROUND

The information and communication technology improvement significant impact in all areas of daily life, in the management of our personal lives and interact with others or in the management of institutions and activities dealing with customers. Despite the information and communication reduced many of the efforts daily transactions and facilitate the process of taking complex decisions, but that this technique could be accompanied by some of the real risks that the necessary security measures have been applied. Because of the rapid development of information technology and the growth in exchange for increasing the number of gaps security threats are discovered, the need to secure information and keep abreast of this development is a optimally goals the strategy seeks to achieve the advanced international institutions that deal with information technology. Knowing that, and in under difficult economic circumstances, a lot of work organizations around the world have sought to increase their investment in the development of information and personnel security technologies, so as to belief in representing as the foundation stone for the construction of its information secure system [3].

2.1.1 PASSWORD

Password is a set of secret characters or words utilized to gain access to a computer, web page, network resource, or data. Passwords help ensure that computers or data can only be accessed by those who have been granted the right to view or access them [4].

2.1.2 ONE TIME PASSWORD(OTP)

A One-Time Password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. An OTP is more secure than a fixed password, especially a user-created password, which might get prone to attacks after a certain period of time. OTPs may replace authentication login information or may be used in addition to it, to add another layer of security. OTP is password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs can either be time synchronized or be based on mathematical algorithms, time synchronized OTPs being the more famous type. A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and, through text-to-speech conversion, to any mobile or landline telephone, text messaging has a great potential to reach all consumers with a low total cost to implement [5].

2.1.3 CRYPTOGRAPHY

Discipline or techniques employed in protecting integrity or secrecy of electronic messages by converting them into unreadable (cipher text) form. Only the use of a secret key can convert the cipher text back into human readable (clear text) form. Cryptography software and/or hardware devices use mathematical formulas (algorithms) to change text from one form to another [6].

2.1.4 ENCRYPTION AND DECRYPTION

Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key. It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks [7].

2.1.5 DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES) is an outdated symmetric-key method of data encryption. DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. Once the go-to, symmetric-key algorithm for the encryption of electronic data, DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm. Originally designed by researchers at IBM in the early 1970s, DES was adopted by the U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data. It was the first encryption algorithm approved by the U.S. government for public disclosure [8].

2.1.6 TRIPLE DATA ENCRYPTION STANDARD ALGRITHM

Triple data encryption standard (DES) is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte [9].

2.1.7 ADVANCED ECNRYPTION STANDARD

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. The origins of AES date back to 1997 when the National Institute of Standards and Technology (NIST) announced that it needed a successor to the aging Data Encryption Standard (DES) which was becoming vulnerable to brute-force attacks [10].

2.1.8 AUTHENTICATION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Logically, authentication precedes authorization (although they may often seem to be combined). The two terms are often used synonymously but they are two different processes [11].

2.1.9 TWO FACTOR AUTHENTICATION

Two Factor Authentication, also known as 2FA, two step verification or TFA, is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand - such as a physical token. Using a username and password together with a piece of information that only the user knows makes it harder for potential intruders to gain access and steal that person's personal data or identity. Historically, two-factor authentication is not a new concept but its use has become far more prevalent with the digital age we now live in. As recently as February 2011 Google announced two factor authentications, online for their users, followed by MSN and Yahoo. Many people probably do not know this type of security process is called Two-Factor Authentication and likely do not even think about it when using hardware tokens, issued by their bank to use with their card and a Personal Identification Number when looking to complete Internet Banking transactions. Simply they are utilizing the benefits of this type of multi factor Authentication there are three common factors used for authentication:

- Something you know (such as a password)
- Something you have (such as a smart card)
- Something you are (such as a fingerprint or other biometric method)

Using a Two Factor Authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email, because the criminal would need more than just the users name and password details [12].

2.2 RELATED WORKS

Many of research studies have been performed in the area of authentication and authorization of user how request access to systems' in this research we will mention four related work.

The first related by Nilay Ylldmm, AsafVarol [13]. They proposed Android Based Mobile Application Development for Web Login Authentication Using Fingerprint Recognition Feature; this study uses the Samsung Galaxy S5 fingerprint recognition feature and IMEI number to generate single time passwords. Within a limited time frame, the secure passwords can be used to sign in/log in to online user accounts related to government, banking and education. The Android based Web Login Authentication application has been developed to use the mobile biometric feature login processes. The main purpose of the program is to produce a single use, time constrained password by fingerprint authentication that will be used along with user name and password for login to the related web site. The application consists of two parts. The first part is the web side and the second part is the Android application side, which generates the password. Initially, the user is presented with the login screen application and choose login with fingerprint option, if user not register; user can choose register finger print option. After the fingerprint verification step, the IMEI number will be queried in the database of the web site. Thus, the user can be exposed to two conditions:

- If the IMEI number is registered, the user will be redirected to the web site that produces single time passwords.
- If the IMEI number is not registered, the user will be directed to the registration page.

The IMEI number of the device is recorded by entering the user name and the password that are recorded to the database into the registration page. Thus, the device is defined. Users will be able to login only from defined mobile devices. Then, the user will be redirected to the page that generates the single time password. In the single time password generation page, the single time password is obtained. The user has to use the password for web site login within three minutes. After three minutes, it will be necessary to generate a new password. When the user enters the single time password along with his or her user name and password information, the user is directed to the relevant web site. The limitation of this study applicable for mobile phones support fingerprint, thus this device is very expensive to pay and fingerprint required soft fingers without injuries, which make difficult to apply in Sudan.

The second related work by Mete Eminagaoglu, Ece Cini, Gizem Sert, and Derya Zor [14] they proposed two factor authentication systems with QR codes for web and mobile application. This study has been implemented by developing a two factor identity verification system where the second factor is the user's mobile phone device and a pseudo randomly generation alphanumerical QR code which is used as the one time password token sent to the user via e-mail or MMS. The study use username and password mechanism for the first authentication step and the system generate QR code as one time password as second authentication step. The user verifies himself to the system by scanning QR code to the web camera manually. In the beginning the user enter username and password to the authentication server, if entry data correct; the system must send QR code automatically to user via of one the selective options; MMS or E-mail then the system checking, verifying and validating QR code. If the user displays the QR code's image to the web camera properly; the data encoded in the QR image is automatically sent to the server application and checking for verification and validation. If the scanned QR image by the camera is the correct QR code, then the second stage of the authentication process is finalized and the user is automatically directed to the authorized page in the application. If the scanned QR image by the camera is not verified by the server; the authentication process automatically fails and a warning message is displayed where the user is automatically directed to the first login page. The system record the last date and time of the last successful /unsuccessful user entry. The system store QR code up to five minute, after that QR code will be deleted. Password is store in database encrypted with AES Symmetric encryption. The login began the user fill username and password if correct QR code one time password send to mobile phone or E-mail and then scan it to web camera to verify. The limitation of this study use QR code that means required QR reader and web camera, then more cost and If the user selects E-mail approach to receive QR code that means internet needed thereby increasing the risk as well as may be delayed to arrive.

The third related work by Indu S, Sathya T.N, and Saravana Kumar V [15]. They proposed Stand Alone and SMS Based Approach for Authentication Using Mobile Phone In this study they develop a complete two factor authentication system using mobile phones. The system using a mobile phone as a software token for One Time Password generation. The OTP valid for a session and for a single use. The system consists of a server connected to a GSM modem and a mobile phone client running a J2ME application. Two modes of operation are available for the users based on their preference and constraints. The first is a stand-alone approach that is easy to use, secure, and cheap. The second approach is an SMS based approach that is also easy to use and secure, but more expensive. The stand-alone approach generates OTP without connecting the client to the server. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. In case the first approach fails to work, the password is rejected, or the client and server are out of sync, the mobile phone can request the OTP directly from the server without the need to generate the OTP locally on the mobile phone. In order for the server to verify the identity of the user, the mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone. The user will then have a given amount of time to use the

OTP before it expires. This approach will require both the client and server to pay for the telecommunication charges of sending the SMS message. The limitation of this study The SMS may be delay for some minute for arrive to phone that means the OTP may became expire and this study needs telecommunications charges that means must pay for them.

The fourth related work by, Ms. E.Kalaikavitha, Mrs. Juliana gnanaselvi [16]. They proposed secure login using encrypted one time password and mobile based login methodology, in this study they secure login to web server by generating one time password then encrypt it by advance encryption standard (AES). User no need to enter OTP manually, because of security reasons OTP is encrypted and sends to mobile by electronic mail (Email). User just read the mail for verification and type application password with that encrypted OTP and sends it to the system Web server is used to send mail to user. The limitation of this study use internet to send OTP by Email that means increase vulnerability of hacking and brute force of OTP as well as the Email may be delay because use internet that means the OTP may become expire.

Chapter Three

(METHODOLOGY)

3.1 INTRODUCTION

This chapter describes system platform and tool and software used to complete the system, and contain system description and graphically operations of system using the Unified Modeling Language.

3.2 SYSTEM COMPONENTS & PLATFORM

The system (server and client) works under windows operation system but the bank application (bank app) runs under android operating system on customer’s smartphone.

The server component contains the relation database (Microsoft Sql Server) as well as web server (Internet Information Services IIS) contains the bank website (asp.net programming language) to allow customer performs his/her daily operations.

The client component just contains web browser (Mozilla Firefox, internet explorer, Opera etc.).

The last component is android smartphone that contains android application build using eclipse IDE.

3.3 HOW OTPs ARE GENERATED AND DISTRIBUTED

OTP generation algorithms typically make use of pseudorandomness or randomness, making prediction of successor OTPs by an attacker difficult, and encryption the OTP, The generated OTPs valid only for a three minute of time.

3.4 HOW THE SYSTEM WORKS

The customer needs to access his/her account using bank website to do any operation, customer must perform following steps:

- The first step customer open android application in smartphone and enter username and password to request one time password.
- The android application use username and password plus smartphone serial number to generate Otp.
- Then the generated one time password appears in smartphone screen, the one-time password transfer to smartphone encrypted using AES algorithm, the life time of the generated one time password is three minutes after that it became expire.
- Customer open website and enter credential information (use another username/password pair that are different from username/password that are used to generate Otp) and one time password from smartphone.
- If this credential information are true and one time password matched and it not expired then system allow user to access his/her account, else message appear to user contain appropriate error message.
- The user must register the serial number of smartphone in system by system administrator to generate Otp, because if smartphone device not register Otp not generated.

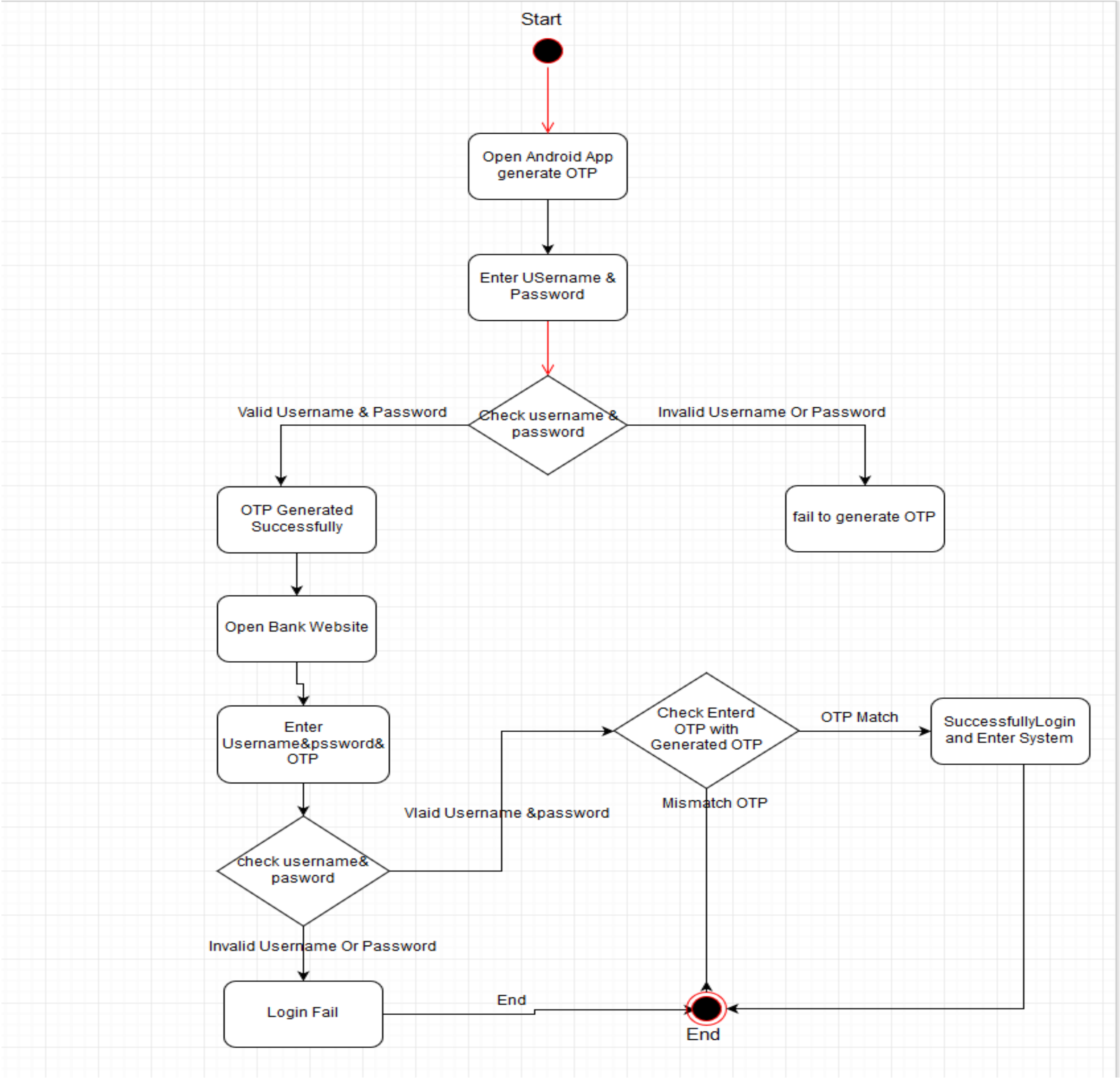

Start
Open Android App generate OTP
Enter USername & Password
Valid Username & Password
Check username & password
Invalid Username Or Password
OTP Generated Successfully
fail to generate OTP
Open Bank Website
Enter Username&pssword& OTP
Check Enterd OTP with Generated OTP
OTP Match
SuccessfullyLogin and Enter System
Vlaid Username &password
Mismatch OTP
check username& pasword
Invalid Username Or Password
Login Fail
End
End

Figure (3.1) illustrates the UML Activity Diagram

3.5 SYSTEM ENVIRONMENT

The system environment is bank website contains simplified virtual environment bellow:

- Deposite Operation.
- Withdraw Operation.
- Transformation To another account.
- Balance statement.

3.6 SYSTEM ANALYSIS

All the system operation describe below using Unified Modeling language (UML). UML is a standardized modeling language enabling developers to specify, visualize, construct and document artifacts of a software system. Thus, UML makes these artifacts scalable, secure and robust in execution. UML is an important aspect involved in object-oriented software development. It uses graphic notation to create visual models of software systems [14].

3.7 USE CASE DIAGRAM

- The customer performs login process.
- The customer performs bank operation (deposit, withdraw, balance statement and amount transfer).

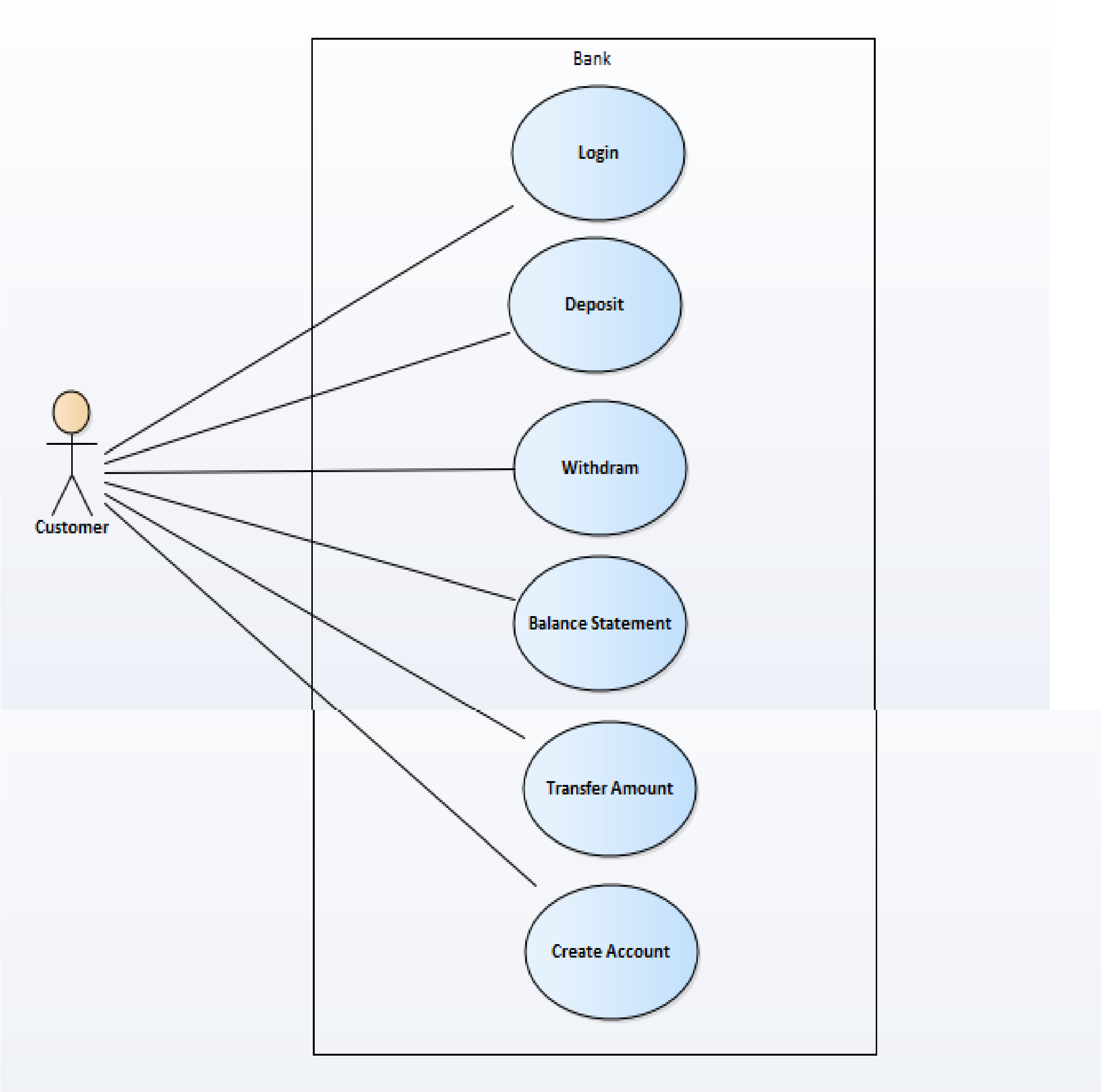


Figure (3.2) illustrates the operations that can be performed by the customer

3.8 SEQUENCE DIAGRAM

- The customer uses his/her phone to request one time password by enter username and password in android application.
- After one time password generated the customer use it plus his/her username and password n login operation.

- If previous credential information right and valid then customer allowed to enter bank application.

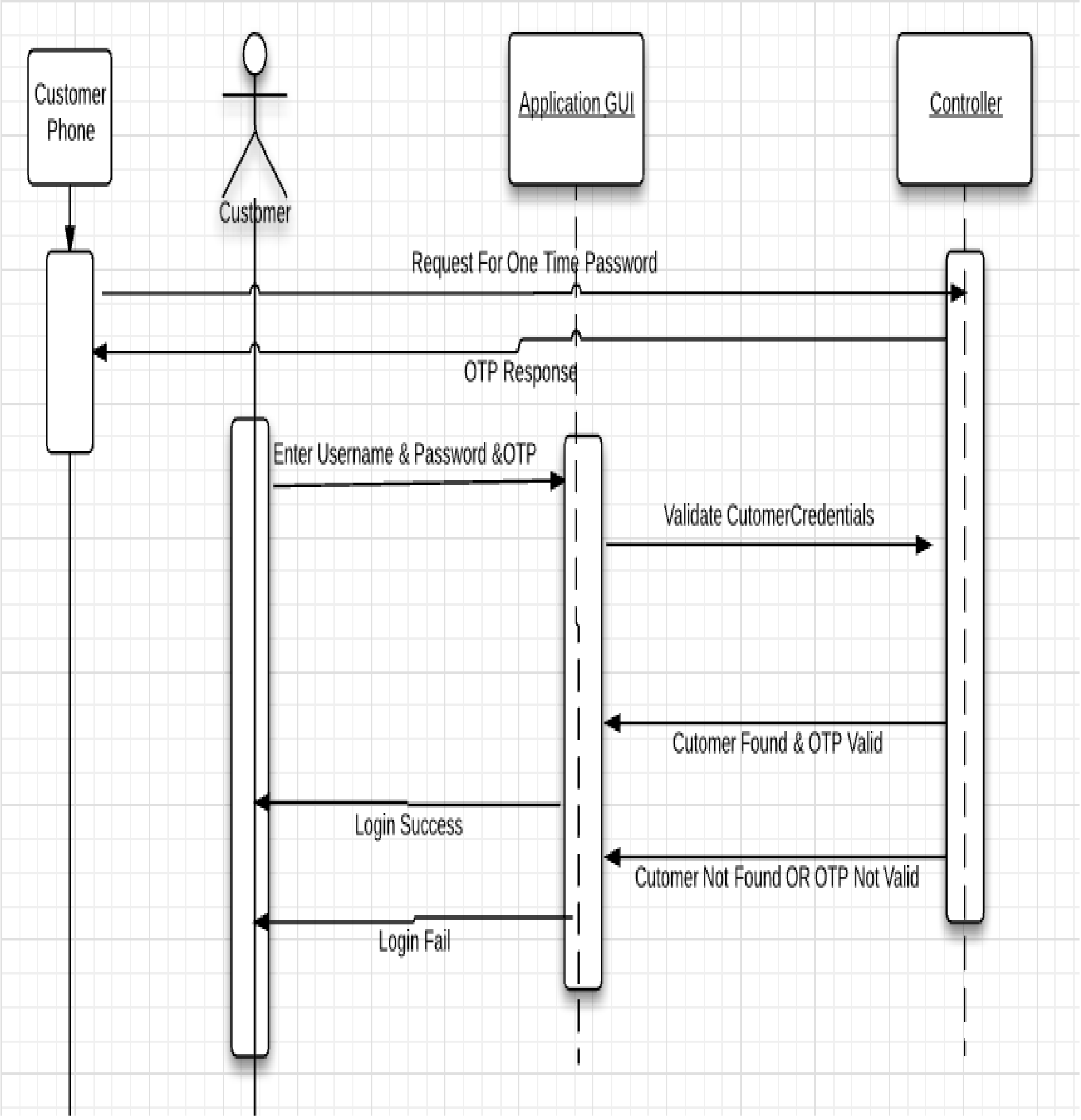

Customer Phone
Customer
Application GUI
Controller
Request For One Time Password
OTP Response
Enter Username & Password &OTP
Validate CutomerCredentials
Cutomer Found & OTP Valid
Login Success
Cutomer Not Found OR OTP Not Valid
Login Fail

Figure (3.3) illustrates the sequence diagram for Login operations that can be performed by the customer.

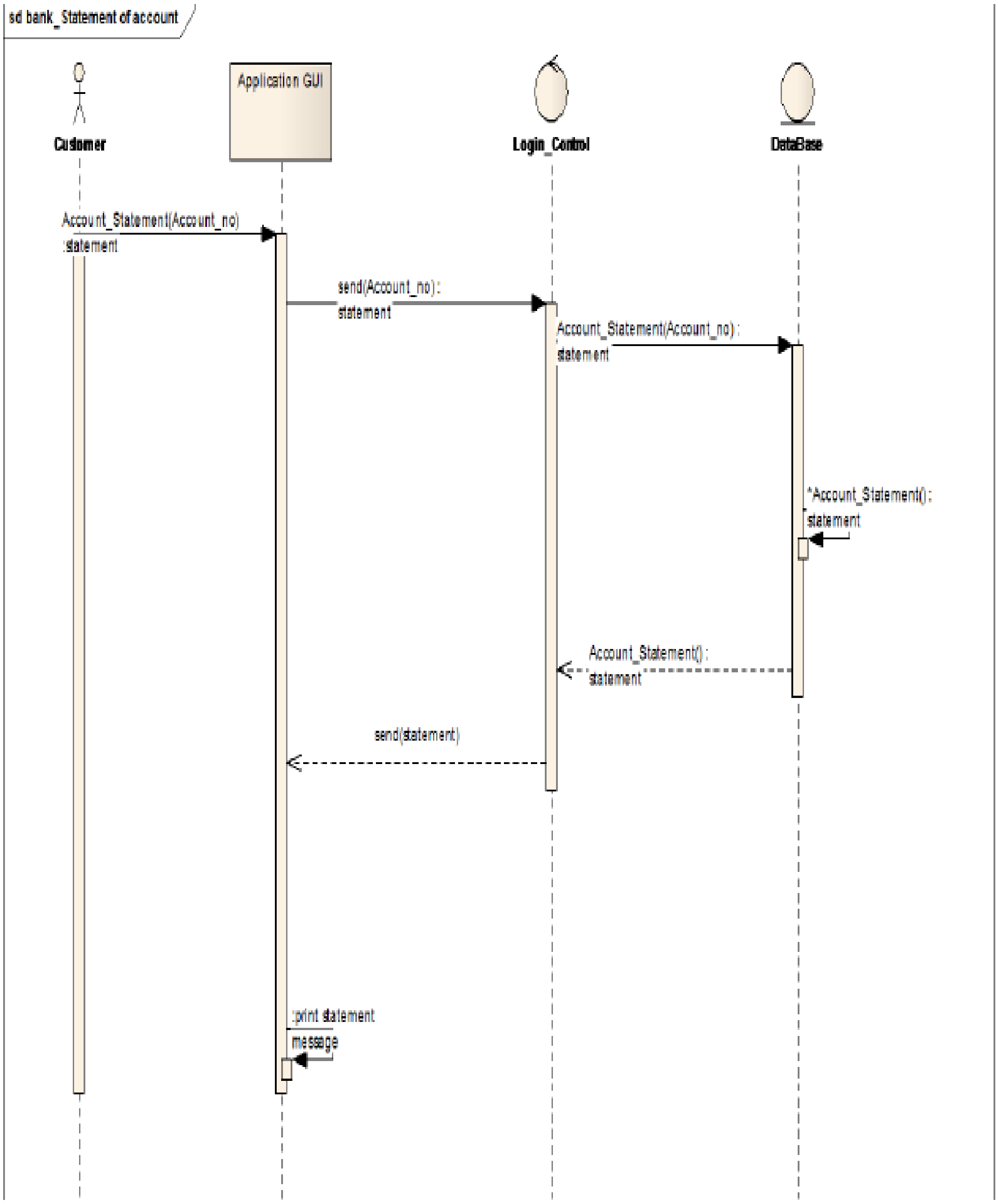
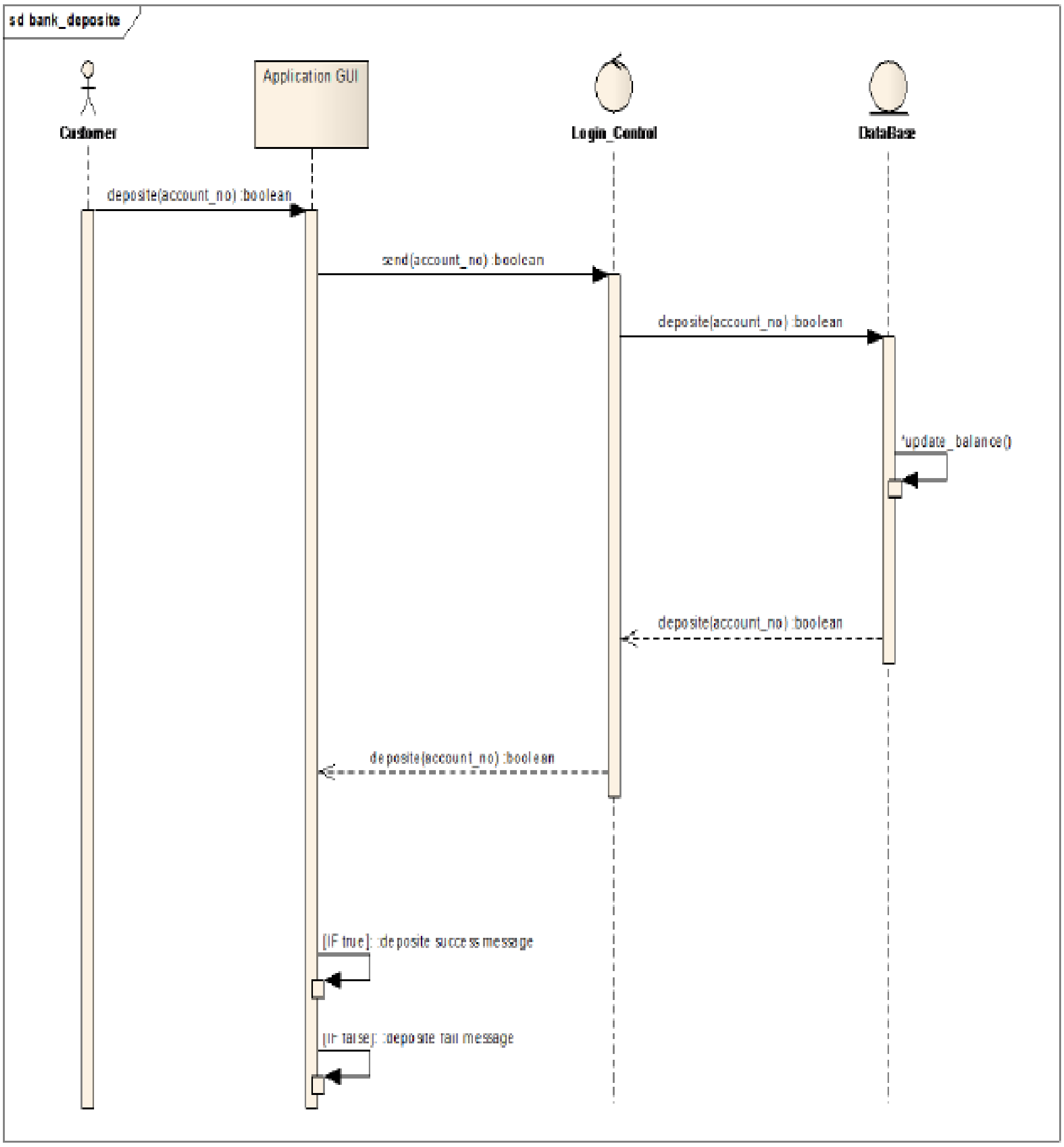
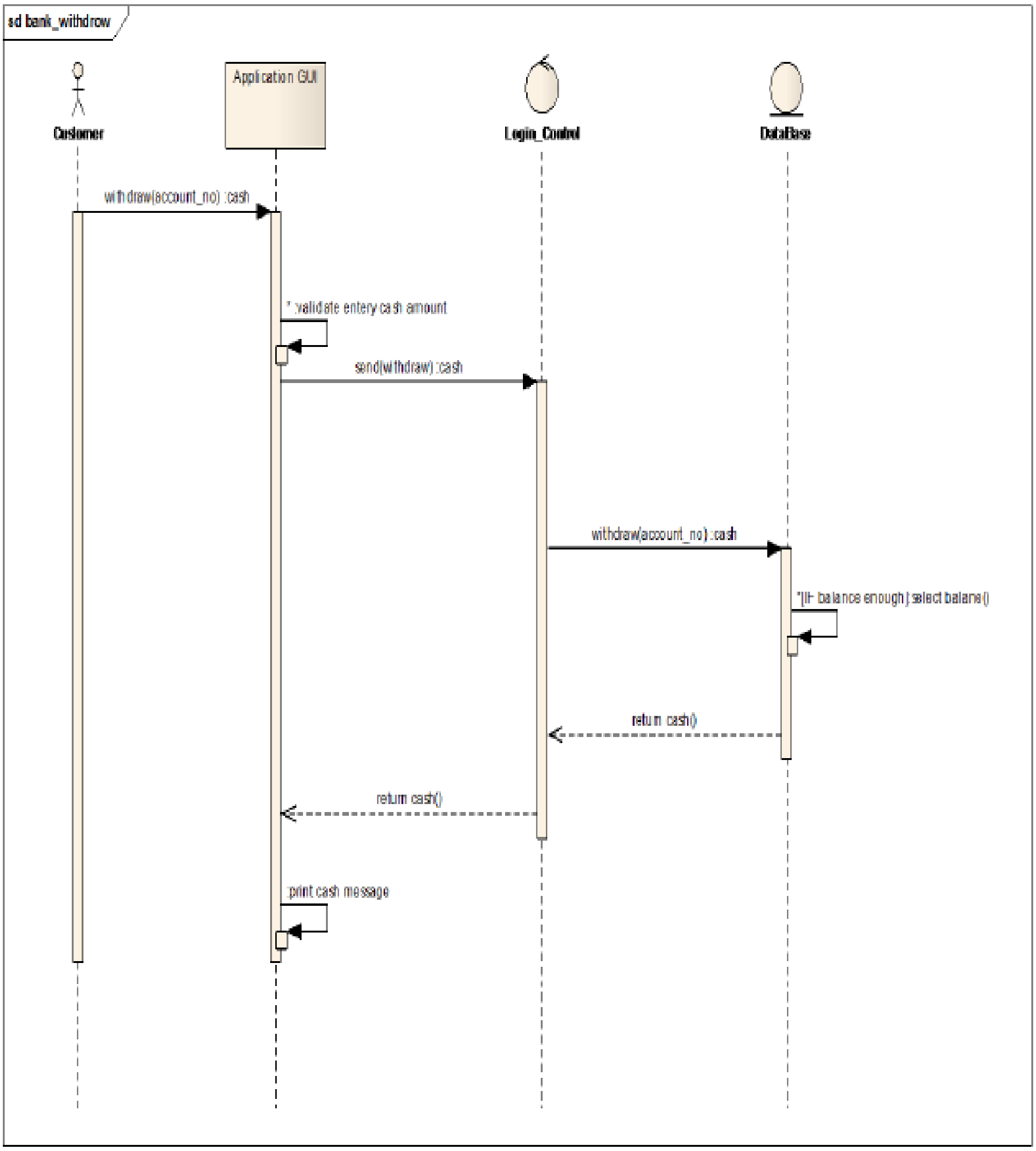

sd bank_ Statement of account
Customer
Application GUI
Login_Control
DataBase
Account_Statement(Account_no) :statement
send(Account_no) : statement
Account_Statement(Account_no) : statement
*Account_Statement() : statement
Account_Statement() : statement
send(statement)
:print statement message

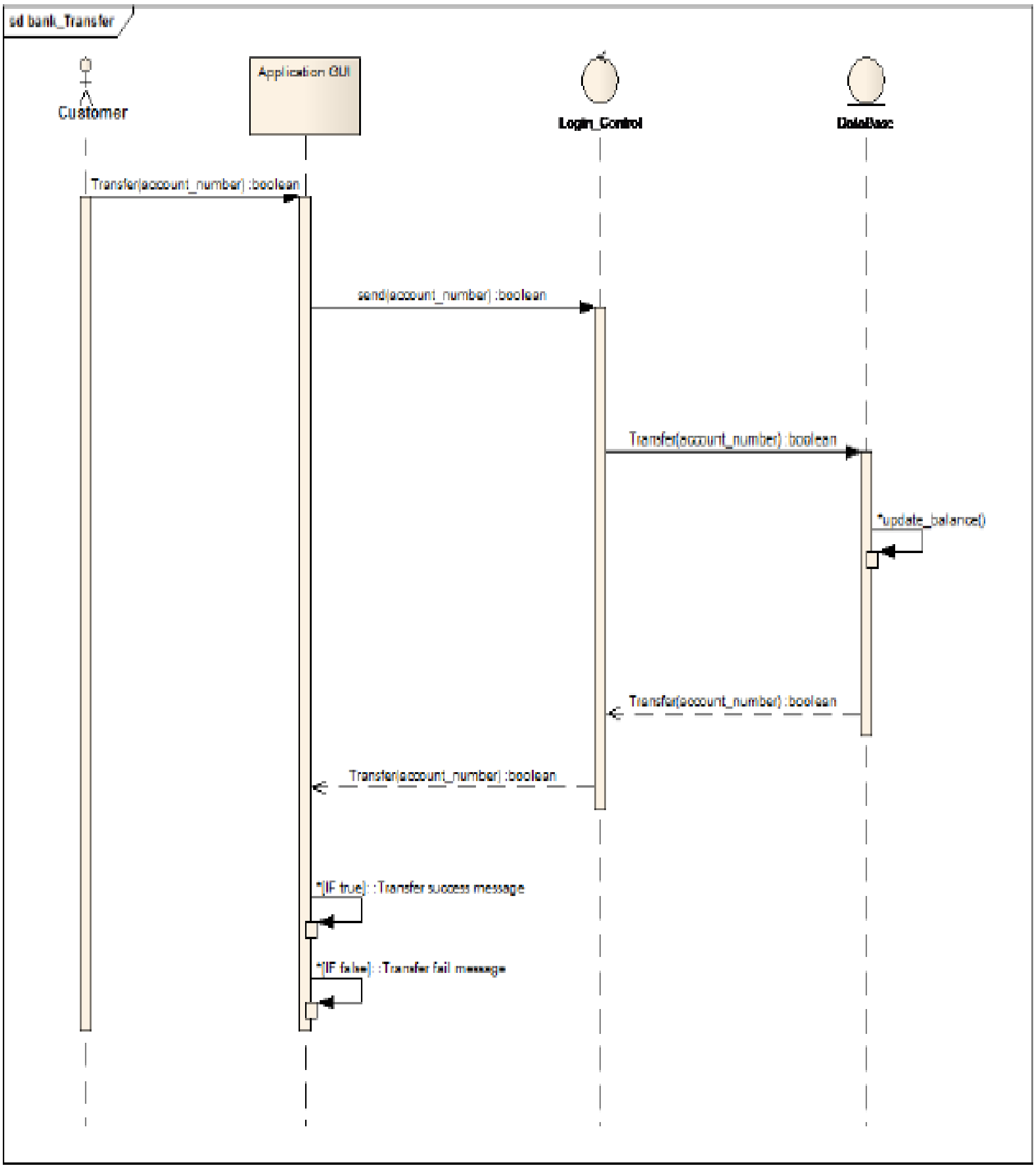
Figure (3.4) illustrates the sequence diagram for balance statement operations.


sd bank_deposite
Customer
Application GUI
Login_Control
DataBase
deposite(account_no) :boolean
send(account_no) :boolean
deposite(account_no) :boolean
*update_balance()
deposite(account_no) :boolean
deposite(account_no) :boolean
[IF true]: :deposite success message
[IF false]: :deposite fail message

- Figure (3.5) illustrates the sequence diagram for deposit operations; the customer enters the amount that wants to be deposit in his/her account.



- Figure (3.6) illustrates the sequence diagram for withdraw operations, the customer enter amount that to be withdraw from account.


sd bank_Transfer
Customer
Application GUI
Login_Control
DataBase
Transfer(account_number) :boolean
send(account_number) :boolean
Transfer(account_number) :boolean
*update_balance()
Transfer(account_number) :boolean
Transfer(account_number) :boolean
*[IF true] : :Transfer success message
*[IF false] : :Transfer fail message

- Figure (3.7) illustrates the sequence diagram for balance transfer to another account operation; the customer enters the amount that wants to be transfer and another account.

3.9 Deployment Diagram for System Components

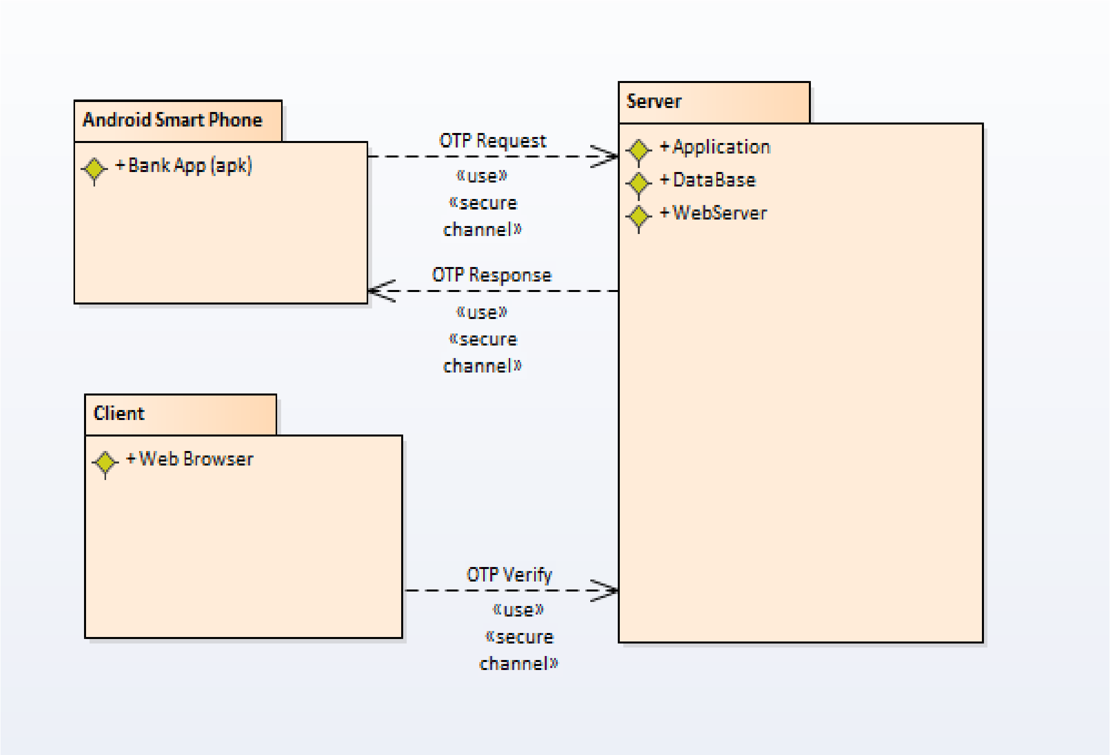


Figure (3.8) illustrates the Deployment Components

Chapter

FOUR

(IMPLEMENTATION)

4.1 INTRIDUCTION

The proposed model in this research has been developed as the system. The system has been implemented and tested. In this chapter show each screen in the system and discuss how it works.

4.2 SYSTEM SCREENS

4.2.1 REQUEST FOR ONE TIME PASSWIRD SCREEN

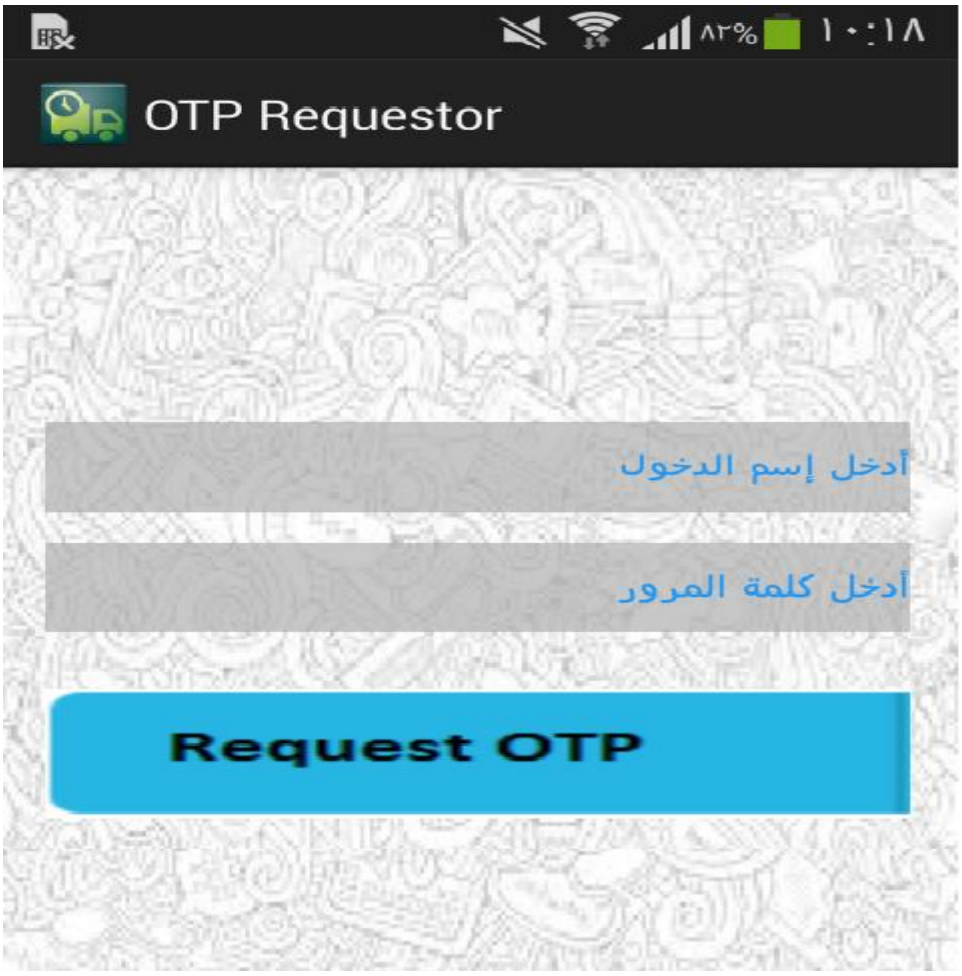
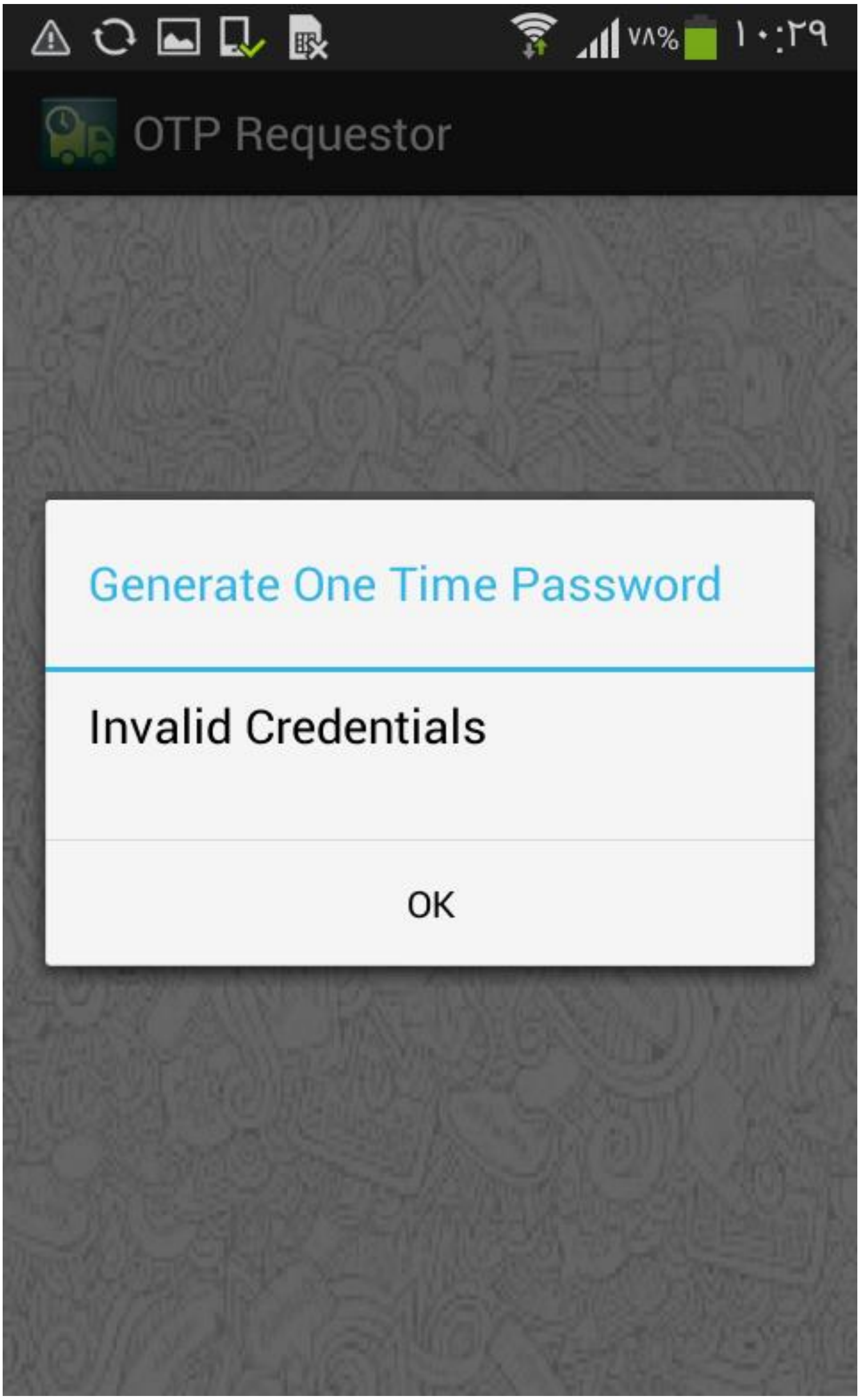


Figure (4.1) illustrates the system login page

This Figure illustrates the main screen in android app for request OTP, the user enters username and password if true Figure (4.4) appears if username or password not found or invalid Figure (4.2) appears.

This Figure illustrates the user enter wrong username or password to generate OTP.

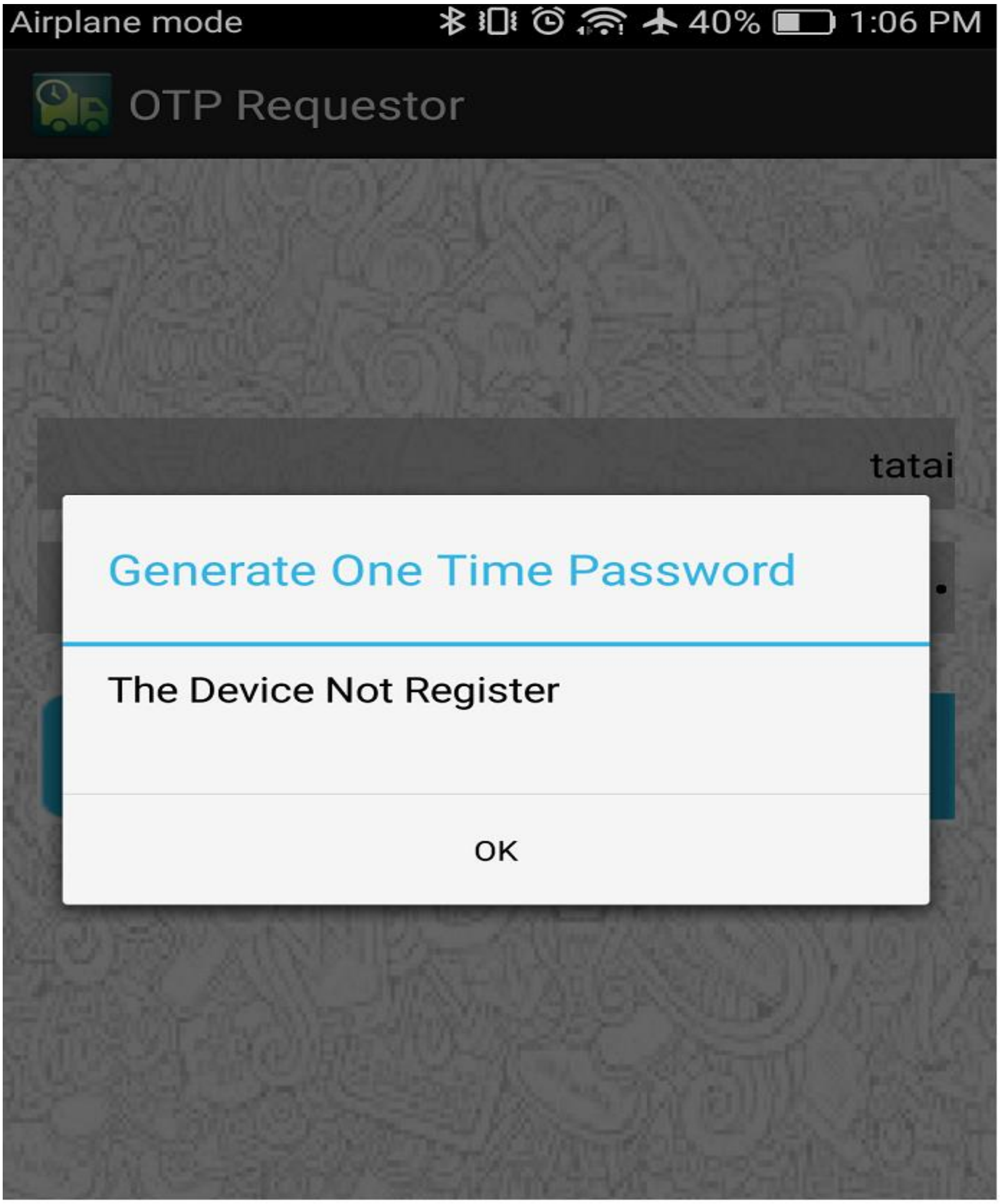


Generate One Time Password

Invalid Credentials

Figure (4.2) illustrates the system login page

This Figure illustrates the user enter wrong username or password to generate OTP.



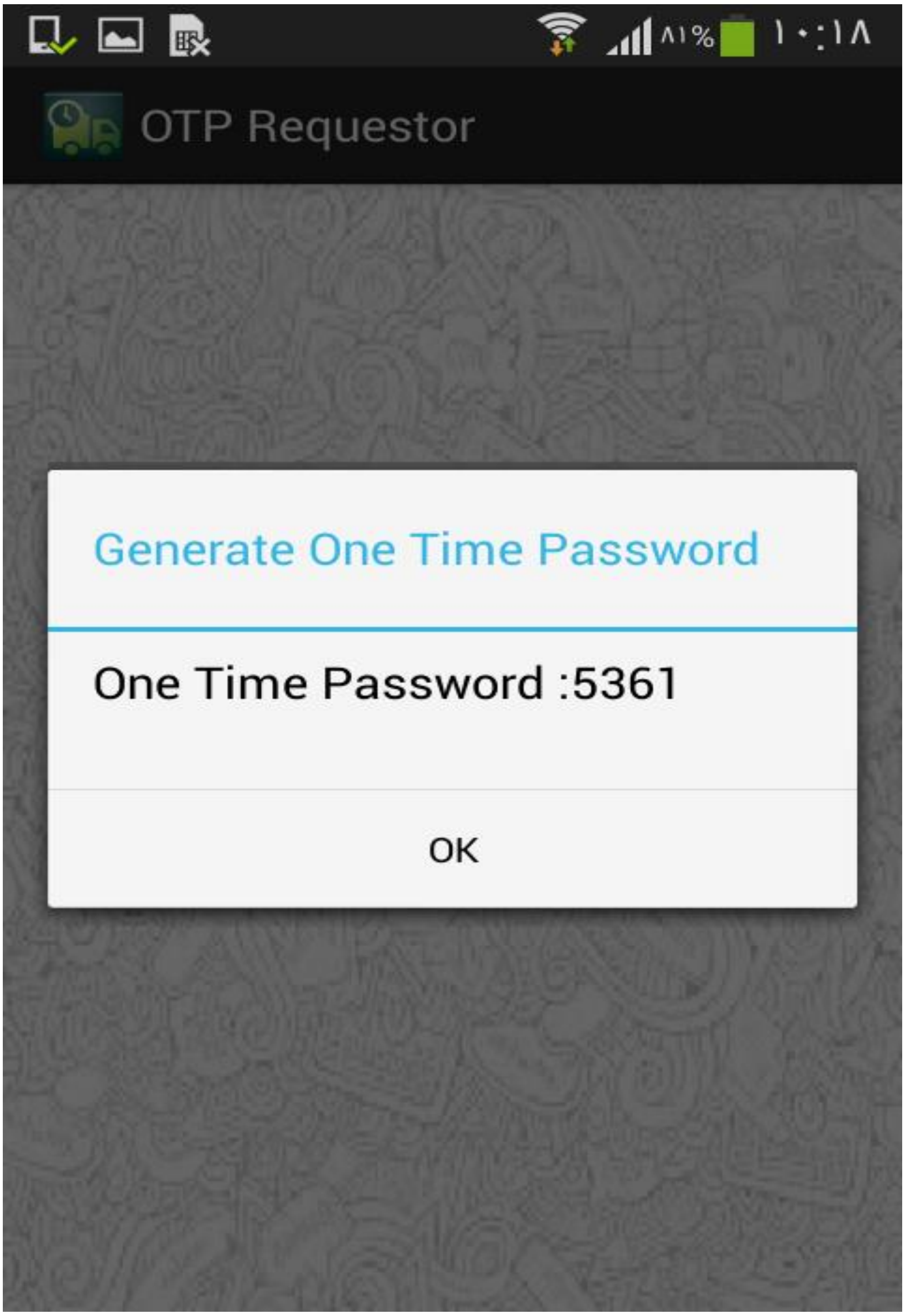
tatai

Generate One Time Password

The Device Not Register

Figure (4.3) illustrates the serial number of smartphone not register

This Figure illustrates the serial number of smartphone not register in system.



OTP Requestor

Generate One Time Password

One Time Password :5361

Figure (4.4) illustrates the system login page

This Figure illustrates the generating of OTP success and user use this OTP to login in website.

4.2.2 THE LOGIN SCREEN FOR WEBSITE

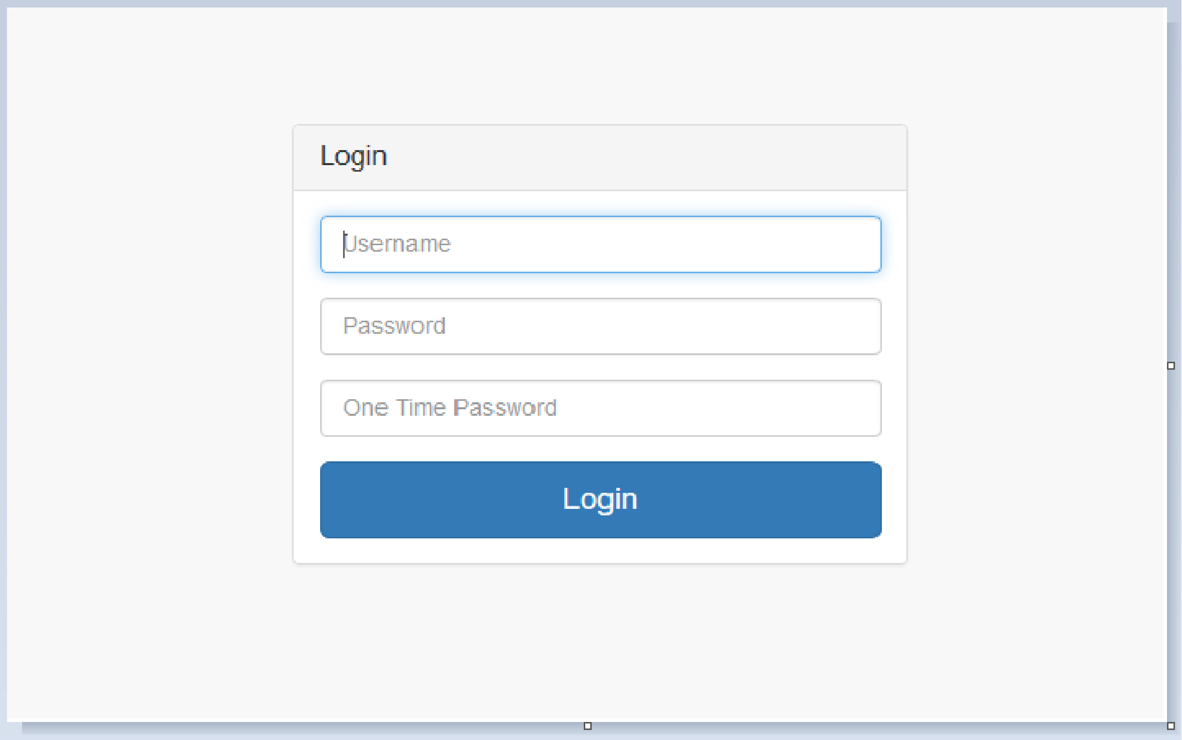
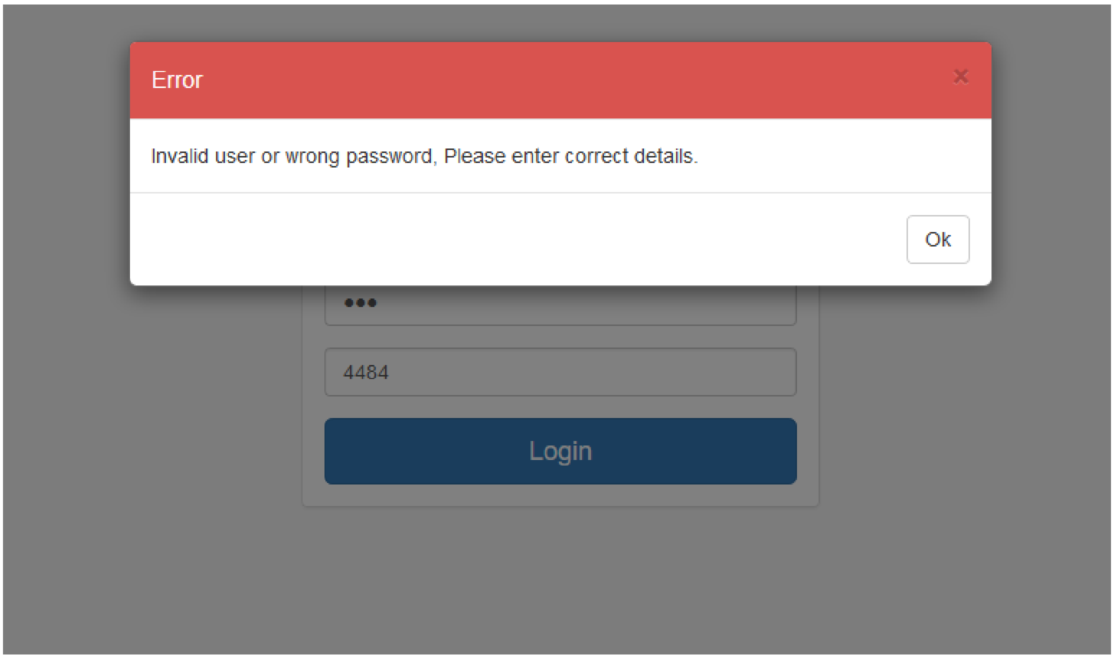


Figure (4.5) illustrates the system login page

In this screen the user enters his/her username, password and one time password, and then the system checks this entered information as well as check validity of OTP. If username or password not correct Figure (4.5) appears else if OTP expire Figure (4.6) appears and if OTP correct but it became expire Figure (4.7) appears. If above information correct then the system open appropriate screen if user is customer Figure (4.14) appears but if user is system administrator Figure (4.8) appears.



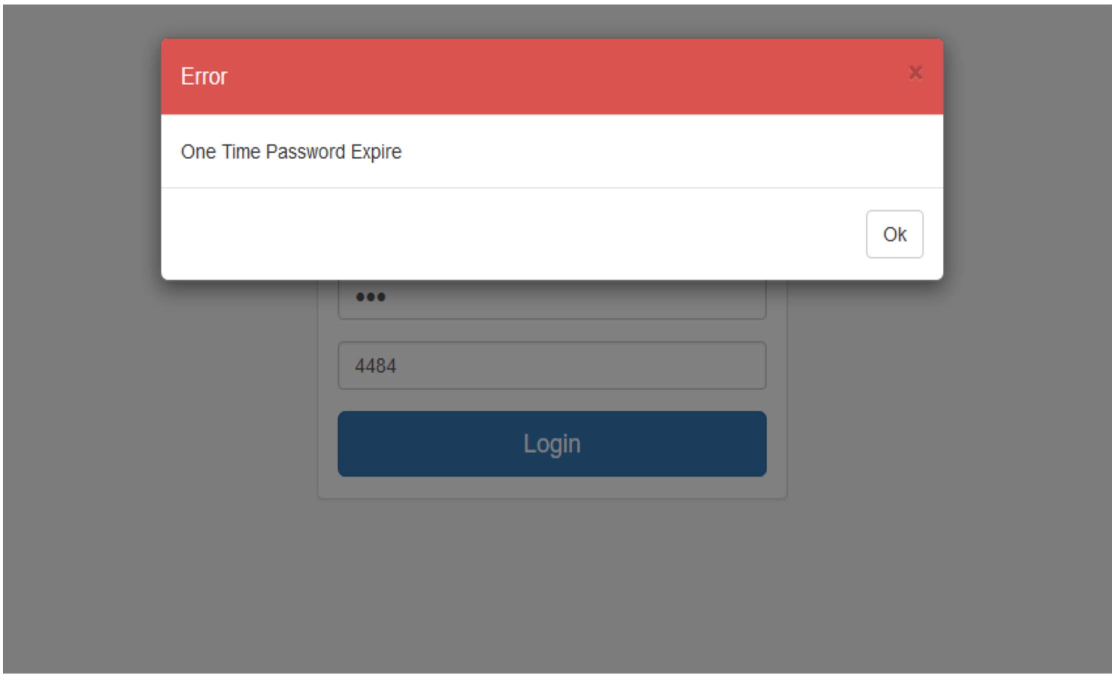
Error

×

Invalid user or wrong password, Please enter correct details.

Figure (4.6) illustrates invalid username or password

This screen illustrates the user enter wrong username or password for login information.



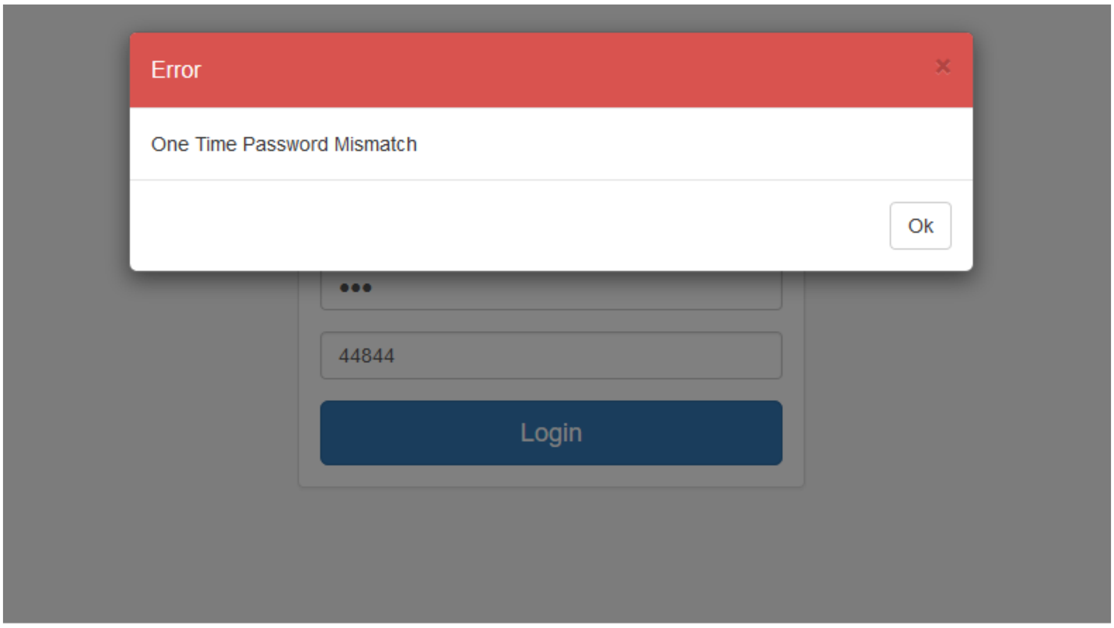
Error

×

One Time Password Expire

Figure (4.7) illustrates the entered one time password expire

This screen illustrates the entered one time password was is correct but became expire.



Error

One Time Password Mismatch

Figure (4.8) illustrates the entered one time password Mismatch

This screen illustrates the entered one time password mismatch against the one time password generated by user's smartphone.

4.2.3 THE MAIN SCREEN FOR ADMINISTRATOR

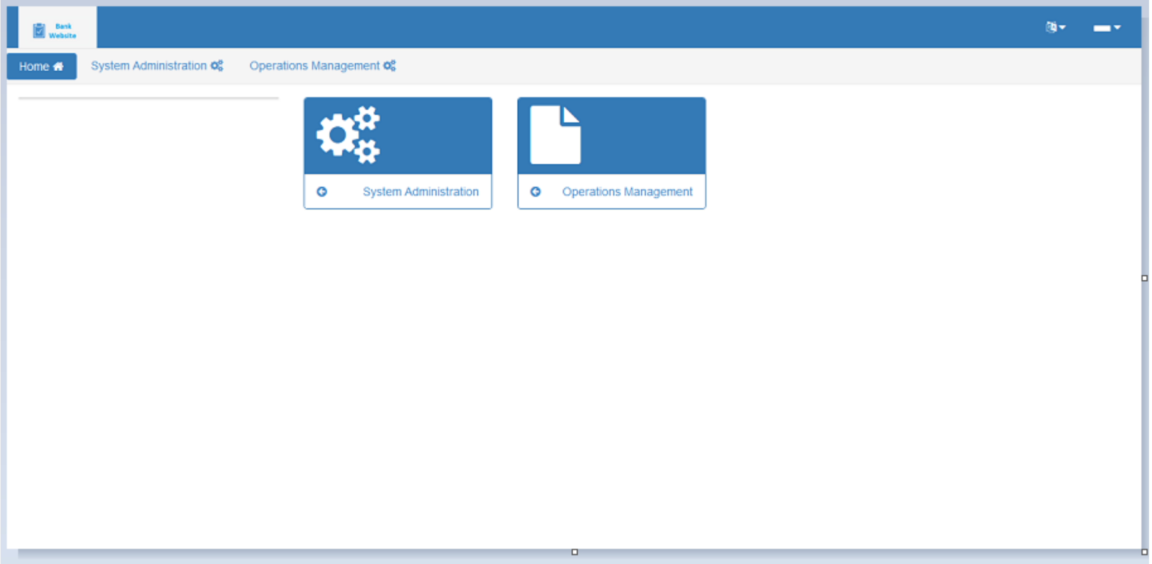


Figure (4.9) illustrates the main screen of system administrator

This screen illustrates the main screen for system administrator.

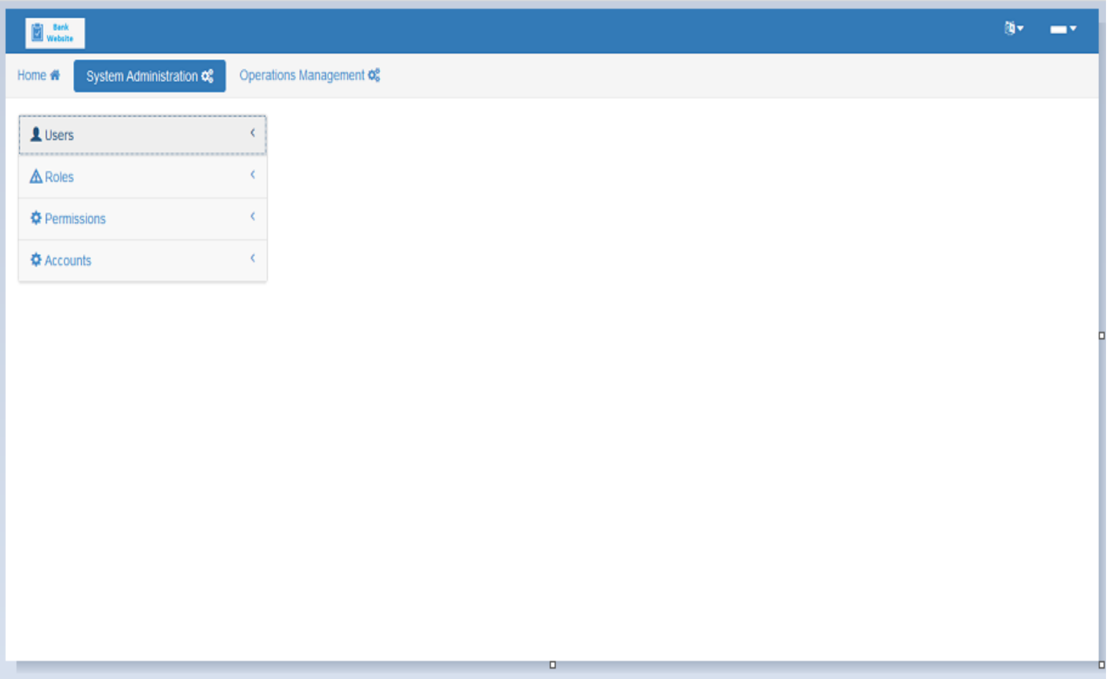
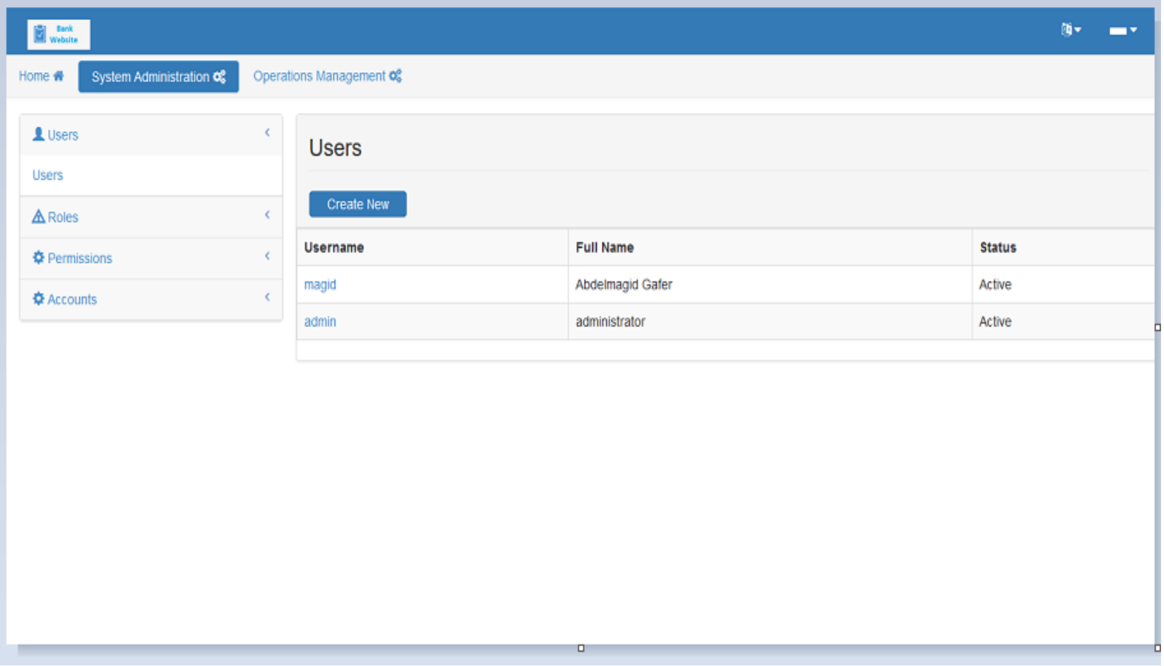


Figure (4.10) illustrates the main operations for system administrator

This screen illustrates the main operation for user management for system administrator.

4.2.4 USRES AND ACCOUNTS MANAGEMENT SCREEN



Users

Username	Full Name	Status
magid	Abdelmagid Gafer	Active
admin	administrator	Active

Figure (4.11) illustrates viewing users by system administrator

This screen illustrates the listing of all users by system administrator.

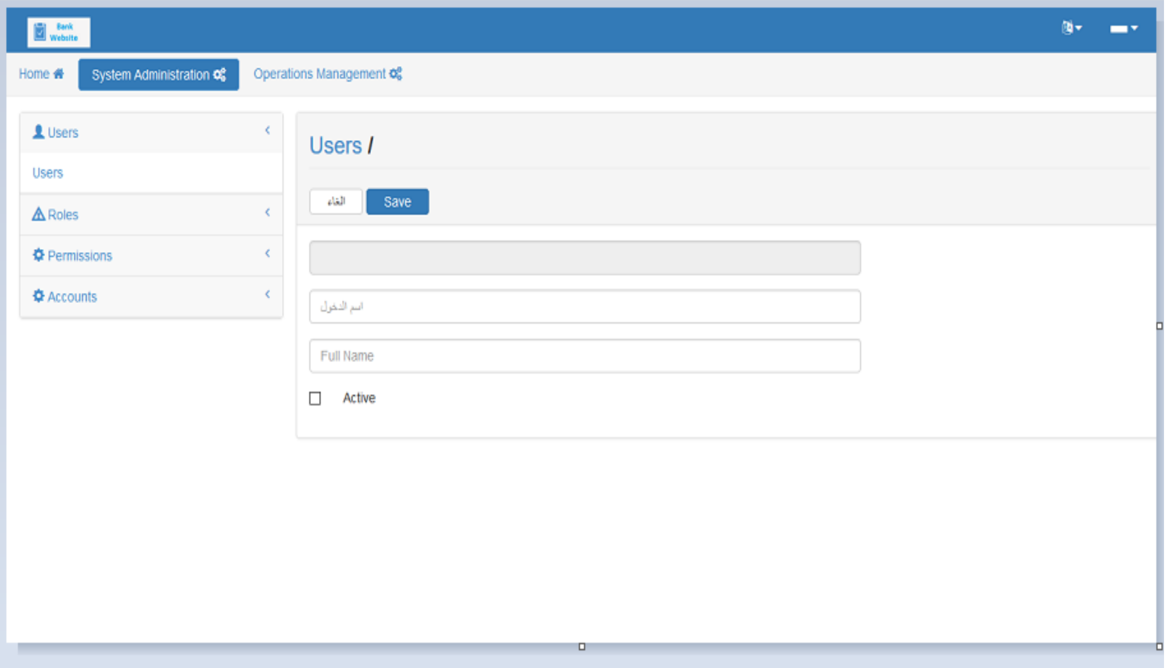
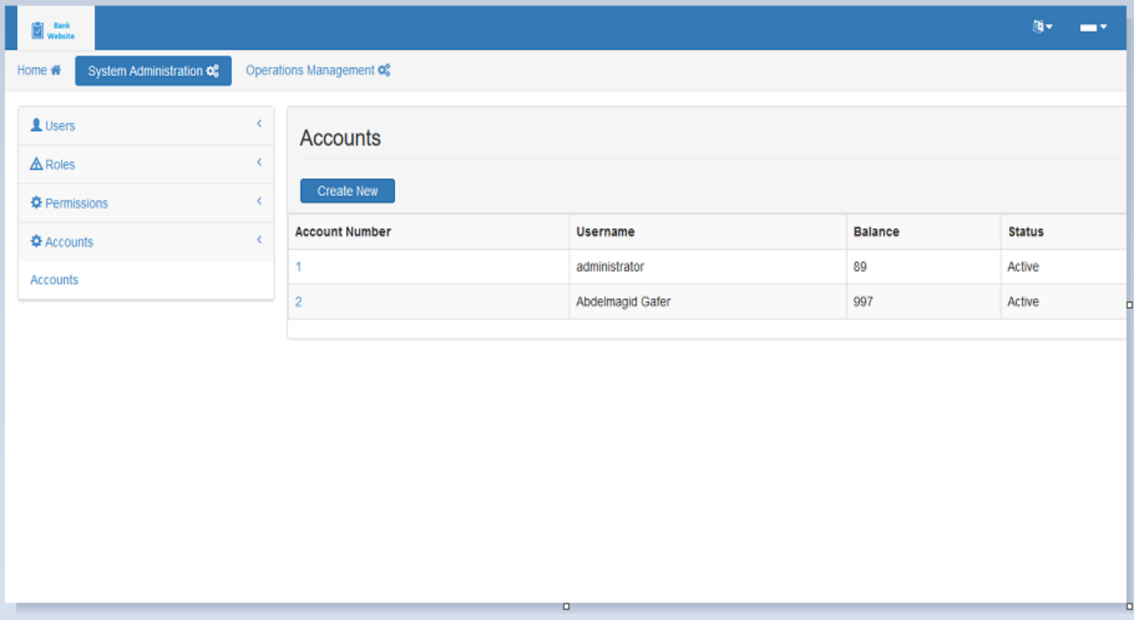


Figure (4.12) illustrates user creation

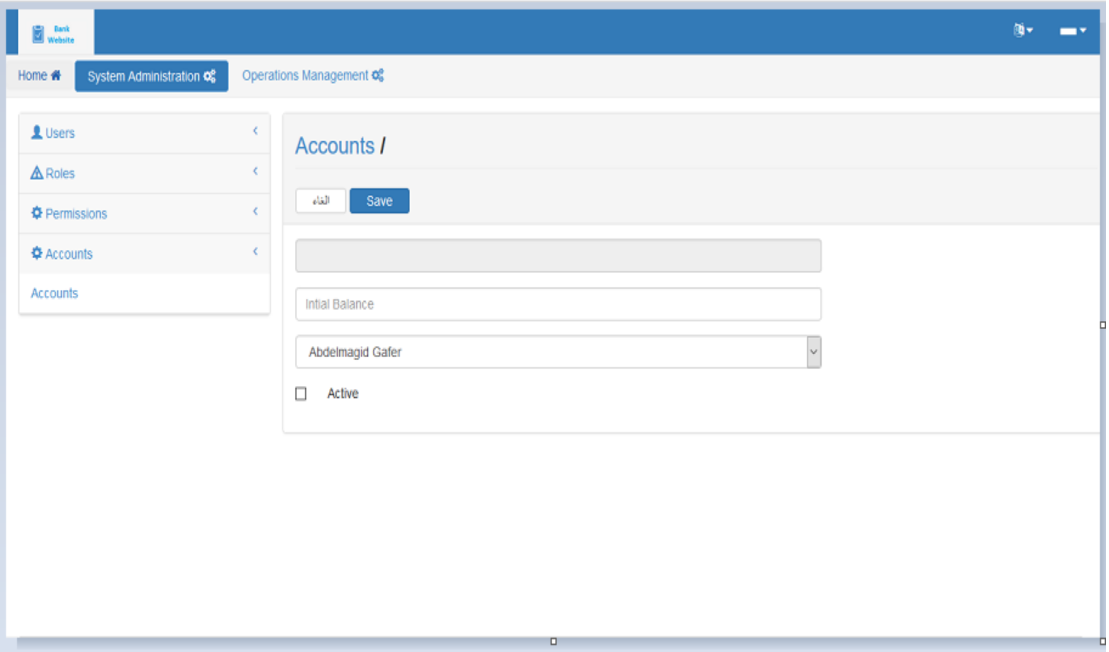
This screen illustrates create new user by system administrator. The administrator fills username and full name for customer



Account Number	Username	Balance	Status
1	administrator	89	Active
2	Abdelmagid Gafer	997	Active

Figure (4.13) illustrates view all customer accounts

This screen illustrates the listing of all customer accounts by system administrator.



Accounts /

Intial Balance

Abdelmagid Gafer

□ Active

Figure (4.14) illustrates create account

This screen illustrates create new account and assign this account to customer, the administrator enter initial balance for this account.

4.2.5 THE MAIN SCREEN FOR CUSTOMER

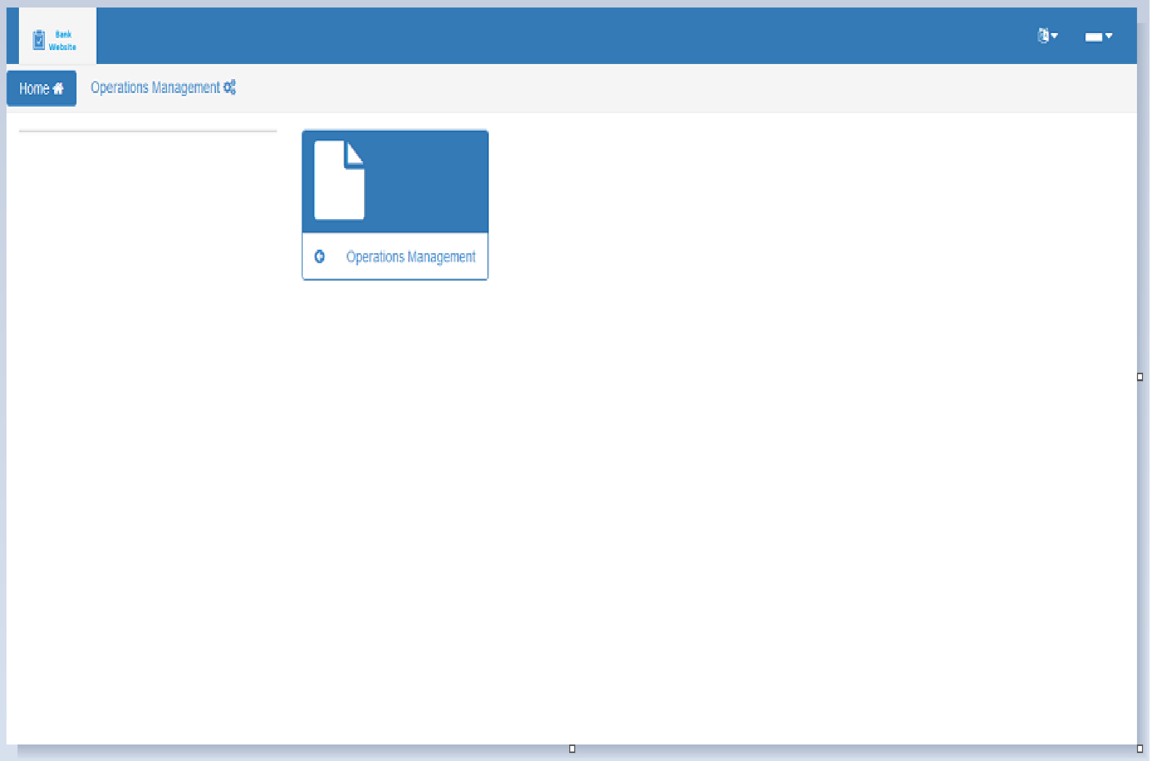
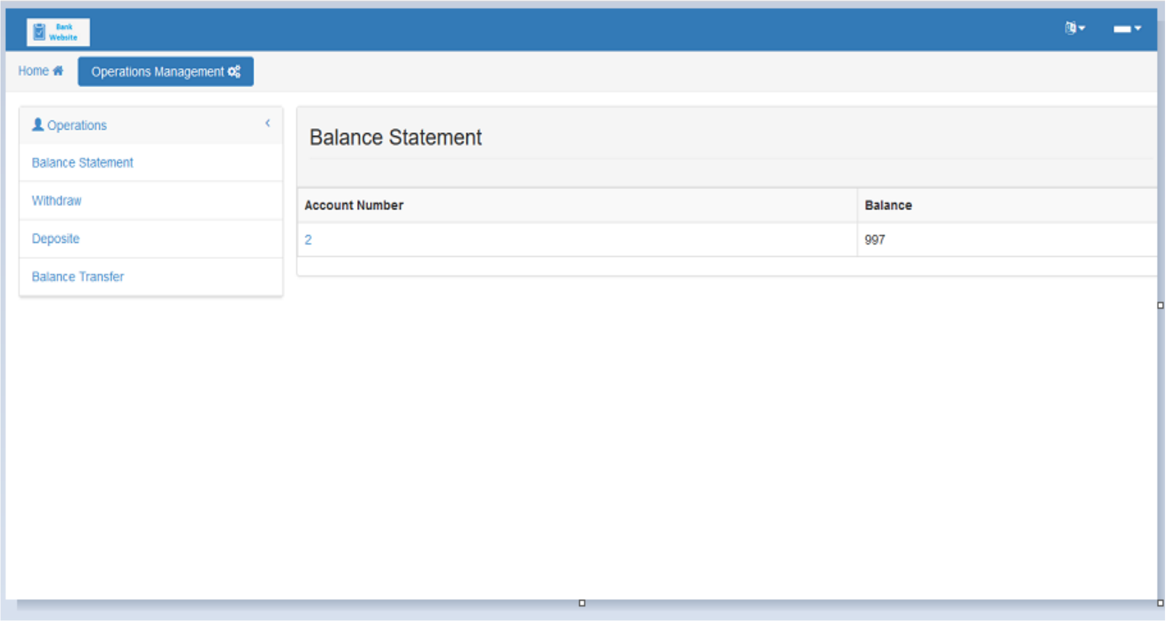


Figure (4.15) illustrates the main screen for customer

4.2.6 BALANCE STATEMENT SCREEN



Account Number	Balance
2	997

Figure (4.16) illustrates balance statement

This screen illustrates view the balance for the customer.

4.2.7 DEPOSITE SCREEN

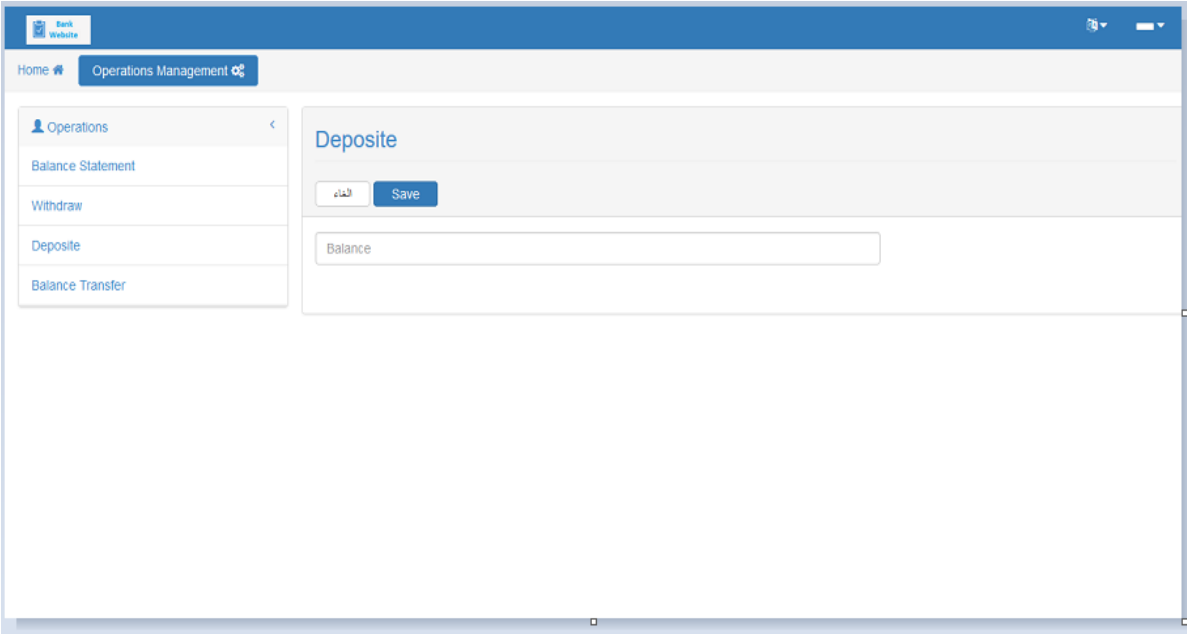


Figure (4.17) illustrates the deposite operation

This screen illustrates the deposite operation by customer. In this screen the customer enter the amount for balance that who wants to Deposited.

4.2.8 WITHDRAW SCREEN

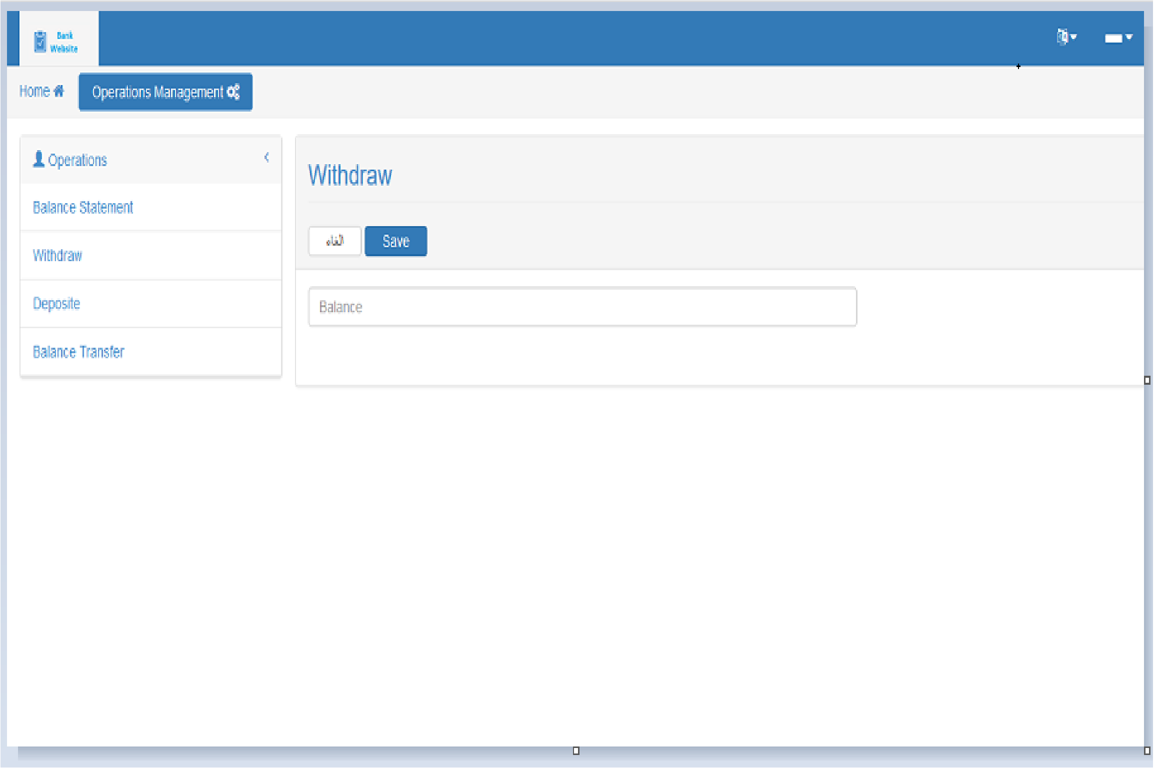


Figure (4.18) illustrates the withdraw operation

This screen illustrates the withdraw operation by customer. In this screen the customer enter the amount for balance that who want to be withdrawn.

4.2.9BALANCE TRANSFER SCREEN

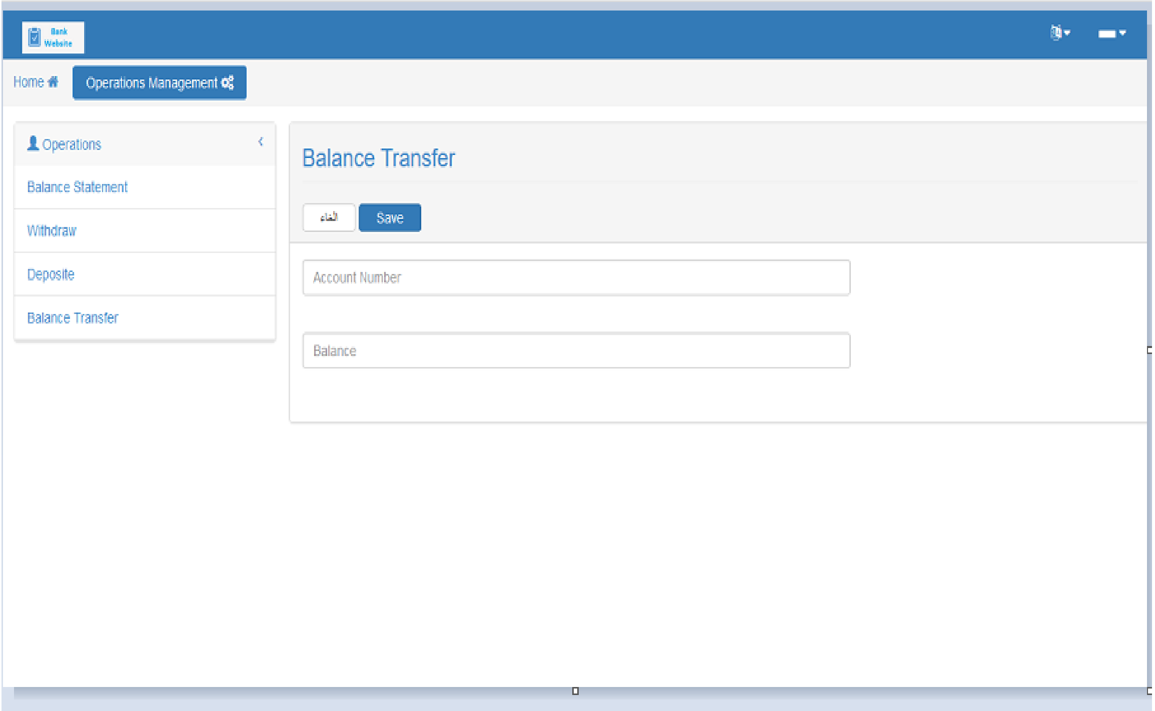


Figure (4.19) illustrates the balance transfer operation

This screen illustrates the transfer balance from his/her account to another account. In this operation the customer enter the amount for balance that who want to transfer and another account number.

4.3 RESULTS

After the design and developing the application for user authentication using one time password and android application as OTP generation, while testing complete get below result:

- User can be authenticated using smart phone (android app) and one time password.
- Decrease the unauthorized login to system.
- This application can be gate authentication to enter the sensitive system (bank website, airline reservation, etc.).

- Low cost to implement.
- Easily adaptable into multiple systems.
- The OTP is valid for only one login session.
- OTP is unique to each key, and every generation is unique from any other.
- OTP became expire after three minute.
- The android application not work in the device not registers in system, because the android application takes smartphone serial number to generate Otp.

4.4 DISCUSSION AND ANALYSIS

Recently, one time password has come under heavy attack, especially by man in the middle attack or brute force attack. In this system, we analyze and discuss this attack against the system.

4.4.1 MAN IN THE MIDDLE ATTACK

A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The system prevents man-in-the-middle attack because the user information used to generate Otp different from user information used to sign in website. Each user has username/password for android app and other username/password for website.

4.4.2 BRUTE FORCE ATTACK

A brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

The system blocks brute force attacks against generated one time password by using advance encryption standard algorithm (AES) to encrypt it, Because the brutal attack needs a period of time to test all the possibilities the one time password became not valid because it valid for three minutes and the AES algorithm need to more time to break it.

4.4.3 STEAL OR LOSE USER’S SMART PHONE

If user loses or steals smart phone the attacker not be able to generate one time password because need username and password to generate it after that user can suspend the account by system administrator.

Chapter

FIVE

(CONCLUSIONS & RECOMMENDATIONS)

5.1 CONCLUSIONS

Authentication is the process of verifying a user's identity when the user is requesting services from any secure IT system. By far, the most popular authentication is a basic username/password based method that is commonly considered to be a weak technique of authentication.

A more secure method is the multi-factor authentication that verifies not only the username/password pair, but also requires a second or third unique physical or biological factor.

technical application is been developed that provides a high level of protection through the use of a two factor authentication mechanism via one time password technology, where the first factor is the user name and password, and the second factor is the generated one time password by smart phone.

Finally because the importance of information security issue which is one of the parts of power in the system, it is through this research has been to provide login interface with one time password that can be used in sensitive systems.

5.2 RECOMMENDATIONS

- Generate one time password in offline mode.
- Develop the application for IPhone device (iOS) operating system.
- Ability to generate one time password in offline mode (no connectivity between smart phone and server).

Reference

[1] Acunetix, “Weak Password Vulnerabilities”, https://www.acunetix.com /blog/articles/weak-password-vulnerabilitycommon-think/,20-03-2017 2:56 PM.

[2] Stephen Northcutt, “Risks of Default Passwords on the Internet”, https://www.sans.edu/cyber-research/security-laboratory/article/default-psswd, 20-03-2017 3:00 PM.

[3] Khalid Bin Sulaiman Alghathbar, “the basics of information security”, http://coeia.ksu.edu.sa, 28-11-2016 5:16 PM.

[4] Andrea Stein, “Password”, http://itstillworks.com/password-hacking-7273695.html, 27-12-2016 12:20 AM.

[5] John Jacob , Kavya Jha , PaarthKotak , Shubha Puthran , “Mobile Attendance using Near Field Communication and One-Time Password”,2015.

[6] Vangie Beal, “Cryptography”, http://www.webopedia.com/TERM/ C/cryptography.html, 27-12-2016 1:20 AM.

[7] Marumari, “Data Encryption and Decryption”, https://developer.mozilla. org/enUS/docs/Archive/Security/Encryption_and_Decryption, 28-11-2016 5:25 PM.

[8] Margaret Rouse, “Data Encryption Standard (DES)”, searchsecurity. techtarget.com/definition/Data-Encryption-Standard, 27-12-2016 2:56 AM.

[9] Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications, 2013.

[10] Margaret Rouse, “Advanced Encryption Standard (AES)”, http:// searchsecurity. techtarget.com/definition/Advanced-Encryption-Standard, 27-12-2016 2:55 PM.

[11] Margaret Rouse, “Authentication”, http://searchsecurity.techtarget. com/definition/authentication, 20-03-2017 4:55 PM.

[12] Tony Bradley, ”What is Two Factor Authentication”, https://www.life wire.com/ what-is-two-factor-authentication-2487538”, 28-11-2016 5:27 PM.

[13] Nilay Ylldmm, AsafVarol, “Android Based Mobile Application Development for Web Login Authentication Using Fingerprint Recognition

Feature”, 2015 23nd Signal Processing and Communications Applications Conference (SIU), 2015.

[14] Mete Eminagaoglu, Ece Cini, Gizem Sert, Derya Zor, “Two Factor Authentication System with QR Codes for Web and Mobile Application”, 2014 Fifth International Conference on Emerging Security Technologies, 2014.

[15] Indu S, Sathya T.N, and Saravana Kumar V, “a stand-alone and sms-based approach for authentication using mobile phone”, 2013 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[16] E.Kalaikavitha, Mrs. Juliana gnanaselvi, “secure login using encrypted one time password and mobile based login methodology”, International Journal of Engineering and Science, 2013.