



**SUDAN UNIVERSITY OF SCIENCE  
AND TECHNOLOGY**  
**COLLEGE OF GRADUATE STUDIES**



## **A Two Factors Authentication Method for Secure Password Transmission over Internet**

**طريقة تحقق ثنائية العوامل لتأمين إرسال كلمة المرور عبر الإنترنت**

A Thesis Submitted In Partial Fulfillment of the Requirement of  
M.Sc. in Computer Science

Prepared by:

Ibrahim Hussien Ibrahim Abdalla

Supervised by:

Dr. Faisal Mohammed Abdalla Ali

December 2017

## الاية

قال تعالى :

( وَبَشِّرِ الَّذِينَ آمَنُوا وَعَمِلُوا الصَّالِحَاتِ أَنَّ لَهُمْ جَنَّاتٍ تَجْرِي مِنْ تَحْتِهَا  
الْأَنْهَارُ كُلَّمَا رُزِقُوا مِنْهَا مِنْ ثَمَرَةٍ رِزْقًا قَالُوا هَذَا الَّذِي رُزِقْنَا مِنْ  
قَبْلُ وَأُتُوا بِهِ مُتَشَابِهًا وَلَهُمْ فِيهَا أَزْوَاجٌ مُطَهَّرَةٌ وَهُمْ فِيهَا خَالِدُونَ )

سورة البقرة ، الآية 25

## DEDICATION

I dedicate my thesis work to my family and friends. A special feeling of gratitude to **my loving parents**, Hussien Ibrahim and Batul Fadeel, whose words of encouragement and push for persistence ring in my ears.

I also dedicate this work and give special thanks to **my brothers and sisters** for being there for me throughout the entire master program. All of you have been my best cheerleaders.

I dedicate this dissertation to **my many friends** who have supported me throughout the process. I will always appreciate all they have done, for helping and hours of proofreading.

## **ABSTRACT**

The internet based applications are play a vital role in different sectors in last decade. The users need to gain access remotely to sensitive information over the internet which is considered as unsecure network due to several vulnerabilities which can be exploited by eavesdroppers to affect these sensitive data by several ways. Therefore the need of secure mechanism to authenticate users with obtaining availability, confidentiality and privacy is increased. There are some popular types of authentication, such as static password authentication which known as being insecure because majority of people use short and simple passwords. Public key certificates schemes which provide the necessary security. However, it requires heavy computational costs and is not suitable for low specification mobile devices. This study proposed a new method for user authentication over internet using hash function and one time password through E-mail as a second authentication factor. This method is implemented on MVC model. From implementation of this model some results can achieved such as: it is secure against password stolen attack, replay attack and man-in-the middle attack and it can be implemented in low specification devices. The proposed scheme can be implemented with less computation complexity for both client and server ends due to using SHA-512 instated of image steganography.

## المستخلص

تؤدي التطبيقات القائمة على الإنترنت دورا حيويا في مختلف القطاعات في العقد الاخير . يحتاج المستخدمون إلى الوصول عن بعد إلى معلومات حساسة عبر الإنترنت والتي تعتبر شبكة غير آمنة بسبب العديد من نقاط الضعف التي يمكن استغلالها من قبل المتتصتين للتأثير على هذه البيانات الحساسة بعدة طرق. لذلك تزداد الحاجة إلى آلية آمنة لمصادقة المستخدمين مع الإبقاء على التوافر والسرية والخصوصية. هناك بعض الأنواع الشائعة من المصادقة، مثل مصادقة كلمة المرور الثابتة ( Static Password ) والتي تعرف بأنها غير آمنة لأن غالبية المستخدمين يستخدمون كلمات مرور قصيرة وبسيطة. مخططات شهادات المفتاح العمومي ( Public Key Certificate ) والتي توفر الأمن اللازم، ومع ذلك، فإنها تتطلب تكاليف حسابية ثقيلة وغير مناسبة للأجهزة النقالة ذات المواصفات المنخفضة. اقترحت هذه الدراسة طريقة جديدة لمصادقة المستخدم عبر الإنترنت باستخدام الدالة (SHA-512) وكلمة مرور لمرة واحدة (One-Time-Password) من خلال البريد الإلكتروني كعامل ثانٍ للمصادقة. تم تنفيذ هذه الطريقة على نموذج (MVC). من تنفيذ هذا النموذج يمكن تحقيق بعض النتائج مثل: أن هذه الطريقة آمنة ضد أنواع الهجوم الحالية مثل : ( Stolen Password Attack )، ( Replay Attack ) و ( Man-in-the meddle Attack ) ويمكن تنفيذها على أجهزة ذات مواصفات منخفضة. كما يمكن تنفيذ المخطط المقترح بأقل درجة تعقيد على كل من العميل والخادم.

## TABLE OF CONTENTS

الاية	I
DEDICATION	II
ABSTRACT	III
المستخلص	IV
TABLE OF CONTENTS	V
LIST OF TABLES	VII
LIST OF FIGURES	VIII
LIST OF ABBREVIATIONS	IX
1. INTRODUCTION	- 1 -
1.1. Background	- 1 -
1.2. Problem Statement	- 1 -
1.3. Research Significance	- 2 -
1.4. Research Hypotheses	- 2 -
1.5. Research Objective	- 3 -
1.6. Research Scope	- 3 -
1.7. Research Methodology	- 3 -
1.8. Research Organization	- 4 -
2. LITERATURE REVIEW & RELATED WORKS	- 5 -
2.1 Introduction	- 5 -
2.2 Overview	- 5 -
2.3 Authentication	- 6 -
2.3.1 Static password Authentications	- 6 -
2.3.2 Security of Password Based Authentication	- 7 -
2.3.3 Public key certificates	- 7 -
2.3.4 One-time Password schemes	- 7 -
2.4 Cryptography	- 8 -
2.4.1 The type of operations used for transforming plaintext to ciphertext	- 8 -
2.4.2 The number of keys used	- 9 -
2.4.3 The way in which the plaintext is processed	- 9 -
2.4.4 Cryptographic Protocols	- 9 -
2.5 Cryptanalysis	- 10 -

2.5.1 Classical Cryptanalysis .....	- 10 -
2.5.2 Brute-Force Attack.....	- 10 -
2.5.3 Non-Brute-Force Attack (Cryptanalytic-Attack) .....	- 10 -
2.6 Implementation Attack.....	- 10 -
2.7 Social Engineering Attacks .....	- 11 -
2.8 Cryptographic Hash Function .....	- 11 -
2.8.1 SHA-256 .....	- 11 -
2.8.2 SHA-512 .....	- 12 -
2.8.3 SHA-384 .....	- 12 -
2.9 Steganography .....	- 12 -
2.9.1 Steganography Techniques.....	- 13 -
2.10 Model-View-Controller (MVC).....	- 14 -
2.11 Related Works.....	- 15 -
2.11.1 Passwords Management via Split-Key .....	- 15 -
2.11.2 Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography .....	- 15 -
2.11.3 A Tow Factor Authentication System with QR Codes for Web and Mobile Applications .....	- 16 -
2.11.4 A New Advanced User Authentication and Confidentiality Security Service .	- 16 -
2.11.5 User Authentication Using Smart Phone and One Time Password .....	- 17 -
3. METHODOLOGY .....	- 17 -
3.1 Introduction .....	- 17 -
3.2 Proposed Model .....	- 17 -
3.2.1 System Implementation Steps:.....	- 17 -
3.3 System Analysis.....	- 19 -
3.3.1 System Operations.....	- 19 -
3.3.2 System flowchart .....	- 20 -
3.3.3 Registration Sequence Diagram .....	- 21 -
3.3.4 Login Sequence Diagram .....	- 22 -
4. IMPLEMENTATION AND RESULTS.....	- 23 -
4.1 Introduction .....	- 23 -
4.2 System Hardware.....	- 23 -
4.3 System Interfaces .....	- 23 -

4.3.1 Sign Up Page .....	- 24 -
4.3.2 Login Page.....	- 25 -
4.3.3 Login Error Message .....	- 26 -
4.3.4 OTP code.....	- 27 -
4.3.5 OTP Page.....	- 28 -
4.3.6 OTP Error Message .....	- 29 -
4.4 Results.....	- 30 -
4.5 Discussion .....	- 30 -
4.6 Evaluation and Comparison.....	- 31 -
5 CONCLUSION AND RECOMMENDATIONS .....	- 32 -
5.1 Introduction .....	- 32 -
5.2 Conclusion.....	- 32 -
5.3 Recommendations.....	- 32 -
<b>References.....</b>	<b>- 33 -</b>

## LIST OF TABLES

<b>Table 4-1: Evaluation and Comparison .....</b>	<b>- 31 -</b>
---	---------------



## LIST OF FIGURES

Figure 2.1 The Security Requirements Triad, source :[1] .....	- 5 -
Figure 2.2 steganography source :[2] .....	- 12 -
Figure 2.3 model-view-controller .....	- 14 -
Figure 3.1 : proposed model methodology .....	- 18 -
Figure 3.2: system operations .....	- 19 -
Figure 3.3: system flowchart .....	- 20 -
Figure 3.4: sign up sequence diagram .....	- 21 -
Figure 3.5: login sequence diagram .....	- 22 -
Figure 4.1: sign up form .....	- 24 -
Figure 4.2: login form .....	- 25 -
Figure 4.3: Login Error Message .....	- 26 -
Figure 4.4.: OTP code sent to E-mail .....	- 27 -
Figure 4.5: OTP Verification Form .....	- 28 -
Figure 4.6: OTP Error Message .....	- 29 -

## LIST OF ABBREVIATIONS

<i>Abbreviation</i>	<i>Description</i>
AES	Advance Encryption Standard
DCT	discrete cosine transformations
HTML	Hypertext Markup Language
LSB	Least-Significant Bit Modifications
MMS	Multimedia Messaging Service
MVC	Model-View-Controller
OTP	One Time Password
QR Codes	Quick Response Codes
SHA-512	Secure Hash Algorithm

# **CHAPTER I**

## **INTRODUCTION**

# 1. INTRODUCTION

## 1.1. Background

The internet based applications are play a vital role in different sectors in last decade. The users need to gain access remotely to sensitive information over the internet which is considered as unsecure network due to several vulnerabilities which can be exploited by eavesdroppers to affect these sensitive data by several ways such as modification, delaying, replying or replacing them by other incorrect information. To keep the privacy of the sensitive information which transmitted between client and server, it is necessary to authenticate the users before connection establish. The most popular authentication mechanism is password-based authentication.

Password-based authentication is one of the most commonly used authentication mechanisms over the Internet. The user presenting himself to the system by entering the user name and password. Most web applications rely on passwords in the process of authenticating users. For example, remote login, government organizations, private corporations, database management systems and cloud storage servers systems. However, the current Internet environment is vulnerable to various attacks. Due to these vulnerabilities the eavesdroppers can gain access to and disclose the sensitive information by unauthorized ways. So we need to protect passwords by providing secure password transmission over the internet.

## 1.2. Problem Statement

In[2] the authors proposed Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography, they used advanced encryption standard algorithm (AES) for encryption and Least Significant Bit algorithm (LSB) for steganography.

The computation complexity is quite high due to image data manipulation for both client and server ends.

The LSB's drawback is the existence of detectable artifacts in the form of pairs of values. While the AES has poor performance results since it requires more processing power[3].

Due to drawbacks of AES and LSB a secured model to overcome these weakness is required.

### **1.3. Research Significance**

The network and internet security become an important issue nowadays due to the increasing of online applications usage which is followed by increasing of vulnerabilities and attacks. There are huge amount of sensitive information exchange over the internet which may cause a big worthiness to people, companies and governments when these information are lost.

So providing secure user authentication between client and server over the internet is a significant issue due to open world digital eavesdroppers. Generally, password-based authentication is a most common approach in client/server environment. But the convenient password based authentication was became vulnerable to some attacks such as [4]: password guessing attack, replay attack and denial of service attack. So it is very important to find a secure authentication mechanisms.

### **1.4. Research Hypotheses**

- Storing the hashed image of password instead of plain password prevent password stolen attack.
- Two factor authentication can overcome replay attack and man-in-the middle attack.

## **1.5. Research Objective**

This research aim to develop new authentication method to secure the password during transmission over Internet to:

1. Overcome replay attack and man-in-the middle attack using two factor authentication.
2. Prevent password stolen attack by storing the hashed image of password instead of the actual password.

## **1.6. Research Scope**

In this research we proposed a secure and effective password-based user authentication system for client/server environment using SHA-512 cryptographic hash function to protect password against Password stolen attack, and OTP to overcome Man in the middle attack.

## **1.7. Research Methodology**

This study proposed a secure user authentication over untrusted network using hash function and E-mail verification as a second authentication factor.

In the client side, the user have to sign up by entering his username and password, Then the 512 hash code will generated as a result of SHA-512 hash function and we select the first 128-bits of hash code which was generated from password as a password hash image. The password hash image and username will send to the server to be Stored in database.

In login phase. User enters his credential data. SHA-512 hash function will called and a 128-bit of password's hash image will send with username to server. The server matching user credential with the previous saved, if they matched the server send a verification code to user's e-mail and redirect's

user to verification page. Then user enters the verification code. If it is correct the system allow user to login.

## **1.8. Research Organization**

This research has the following structure: Chapter I is an Introduction, Chapter II is about Literature Review and related works, Chapter III contains research methodology, Chapter IV including Results and discussion, and Chapter V is Conclusion, recommendations and references.

## **CHAPTER II**

# **LITERATURE REVIEW & RELATED WORKS**



## 2. LITERATURE REVIEW & RELATED WORKS

### 2.1 Introduction

This chapter provides some issues and definitions related to information security and user authentication mechanisms with some previous related studies.

### 2.2 Overview

*“Computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources”*. There is three key objectives of computer security[5]:

“Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information”[5].

*“Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity”*[5].

“Availability: Assuring timely and reliable access to and use of information”[5].

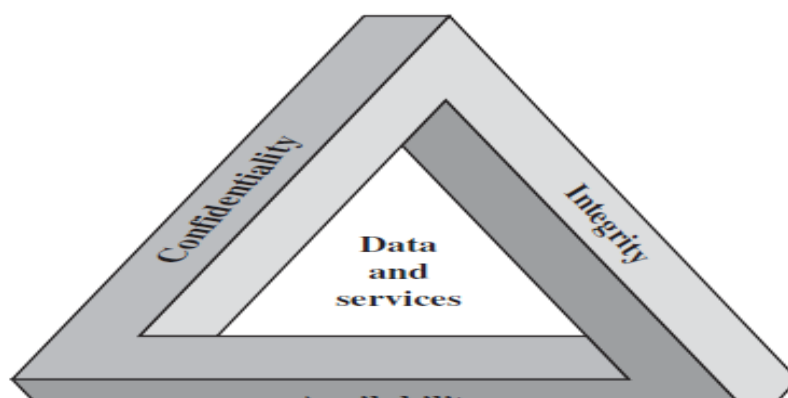


Figure 2.1 The Security Requirements Triad, source :[1]

## **2.3 Authentication**

Sometimes called (origin integrity), is the assurance that the communicating entity is the one that it claims to be.

Origin integrity include two concepts implicitly: Identity integrity: Ensure that data is belong to its source, and Data integrity: Prove that the data is reproduced from that source[6].

A good user authentication protocol which based on username and password must basically overcome the offline password guessing attack, the stolen verifier attack, and the DoS attack. some password-based authentication overcome stolen verifier attack by keeping verifiers, the hashed images of passwords, in the server's database instead of storing plain passwords. Denial-of-Service attack should prevented by strict integrity check[4].

There are three authentication schemes [7, 8]:

### **2.3.1 Static password Authentications**

Password-based authentication is one of the most commonly used authentication mechanisms over the Internet. The user presenting himself to the system by entering the user name and password. Most web applications rely on password in the process of authenticating users. For example, remote login, government organizations, private corporations, database management systems and cloud storage servers systems.

Static password authentication is considered insecure even when SSL / TLS is used, because of the shortness and simplicity of passwords used by most users.

### 2.3.2 Security of Password Based Authentication

Zhao, Zhu, and Z. Wang, provide a list of basic attacks that a password-based protocol needs to overcome. An ideal password-based protocol should be secure against these attacks[9]:

- **Eavesdropping:** means that the attacker monitors the communication channel between the parties.
- **Replay:** The attacker records messages he has observed and re-sends them at a later time.
- **Man-in-the-middle:** The attacker intercepts the messages sent between the parties, the client and the server, then replaces these with his own messages.
- **Impersonation:** Where the attacker impersonates one of the parties, either the client or the server to obtain some useful information.
- **Password-guessing:** The attacker tries to reach a relatively small dictionary of words that is likely to contain a secret password.
- **Partition attack:** In this type of attack, the attacker logs the previous connections, and then reduces the size of the dictionary by deleting those words that do not correspond to the recorded connections.

### 2.3.3 Public key certificates

*“Public key certificates schemes provide the necessary security. However, it requires heavy computational costs and is not suitable for low spec mobile devices”*[8].

### 2.3.4 One-time Password schemes

*“The computational costs of one-time Password schemes are lower than that of public-key certificate schemes”*[8].

## **2.4 Cryptography**

Cryptography is the most comprehensive term, which consists of two main parts. The first is encryption, which is the science that studies secret writing in order to conceal the true meaning of the message. The second part is Cryptanalysis, is the science or art of breaking those codes to reach the hidden meaning.

Traditional encryption refers to the possibility of sending information between two parties in a distorted form so that unauthorized parties can't access them. Modern cryptography is scientific study of techniques to secure digital information, transactions and distributed computations. Cryptography deals with several problems such as message authentication and digital signature; it can be used as a protocol for secret key exchange[10].

Encryption systems can generally be divided on the basis of three independent criteria as follows[1]:

### **2.4.1 The type of operations used for transforming plaintext to ciphertext**

All encryption algorithms are based on two general principles:

#### **2.4.1.1 Substitution**

In this type, each element of plaintext is replaced with another one. Most popular ciphers of this type are: Caesar cipher and monoalphabetic substitution cipher.

#### **2.4.1.2 Transposition (Permutation)**

In this type of the classical ciphers, encryption is done by rearranging the order of plaintext elements. For example row transposition cipher.

## **2.4.2 The number of keys used**

### **2.4.2.1 Symmetric key**

Algorithms in which both sender and receiver use a common secret key to encrypt and decrypt messages. Most traditional cryptographic algorithms rely mainly on symmetric algorithm. This type is used to encrypt data and verify message integrity.

### **2.4.2.2 Asymmetric (public-key)**

In this type of cryptography, a user possesses a secret key as in symmetric cryptography with also a public key. Asymmetric algorithms can be used for applications such as digital signatures and key establishment, and also for classical data encryption.

## **2.4.3 The way in which the plaintext is processed**

### **2.4.3.1 A block cipher**

Ciphers which divide the plaintext into specific block size, the encryption and decryption processes deal with one block at a time. The ciphertext is produced as block too.

### **2.4.3.2 A stream cipher**

*“Processes the input elements continuously, producing output one element at a time, as it goes along”*[1].

## **2.4.4 Cryptographic Protocols**

Cryptographic protocols deal with the application of cryptographic algorithms. Asymmetric and symmetric algorithms are regarded as building blocks through which applications can be realized. The Transport Layer Security (TLS) scheme is an example of Cryptographic Protocols.

## **2.5 Cryptanalysis**

Cryptanalysis is the science and sometimes art of breaking cryptosystems. Or the process of trying to obtain plain text or encryption key.

### **2.5.1 Classical Cryptanalysis**

Is to recover the plaintext of a cipher-text or recover the secret key. There are two general types of attacks[1]: brute-force attack and non-brute-force attack.

### **2.5.2 Brute-Force Attack**

Is to try every key to decipher the cipher-text. On average, it need to try half of all possible keys, and the time needed is depend on size of key space.

### **2.5.3 Non-Brute-Force Attack (Cryptanalytic-Attack)**

We can classify this type of attack by how much information needed by attacker into: Cipher-text only attack, Known plaintext attack, Chosen plaintext attack and Chosen cipher-text attack.

## **2.6 Implementation Attack**

Side-channel analysis can be used to obtain a secret key, for instance, by measuring the electrical power consumption of a processor which operates on the secret key. The power trace can then be used to recover the key by applying signal processing techniques. In addition to power consumption, electromagnetic radiation or the runtime behavior of algorithms can give information about the secret key and are, thus, useful side channels. Note also that implementation attacks are mostly relevant against cryptosystems to which an attacker has physical access, such as smart cards. In most Internet-based attacks against remote systems, implementation attacks are usually not a concern[10].

## **2.7 Social Engineering Attacks**

Bribing, blackmailing, tricking or classical espionage can be used to obtain a secret key by involving humans. For instance, forcing someone to reveal his secret key. Another, less violent attack is to call people whom we want to attack on the phone, and impersonate their IT department of their company to ask them their passwords as software update requirement.

## **2.8 Cryptographic Hash Function**

*“Hash functions map messages of arbitrary length to a string of fixed length, called the ‘hash-value’ or ‘message digest’ ”[3].*

Nowadays modern world of e-mail, internet banking, online shopping, and other sensitive digital communications are increased and became substantial tools in our life.

Cryptography has become a vital tool for guaranteeing the secrecy of data transfers. Cryptographic hash functions operate as the main process of many common cryptographic methods, protocols, encryption algorithms and numerous random number generation algorithms.

*“In 2002, after SHA-1 security has been compromised, the National Institute of Standards and Technology (NIST) published a new Secure Hash Standard (SHA-2 family), which defined three new Secure Hash Algorithms SHA-256, SHA-384, and SHA-512”[3].*

### **2.8.1 SHA-256**

*“The SHA-256 compression function operates on a 512-bit message block and a 256-bit intermediate hash value. It is essentially a 256-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key”[3].*

## 2.8.2 SHA-512

The SHA-512 compression function operates on a 1024-bit message block and a 512-bit intermediate hash value. It is essentially a 512-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key.

## 2.8.3 SHA-384

SHA-384 is defined in the exact same manner as SHA-512 while the final 384-bit hash is obtained by truncating the SHA-512-based hash output to its left-most 384 bits.

## 2.9 Steganography

Steganography, coming from the Greek words stegos, meaning roof or covered and graphia which means writing.

Steganography is a science of hide the existence of a secret message in side digital media such as text, audio, image and video.

Steganography and cryptography are closely related but in some cases, sending an encrypted message will arouse suspicion while steganogram will not do so[5].

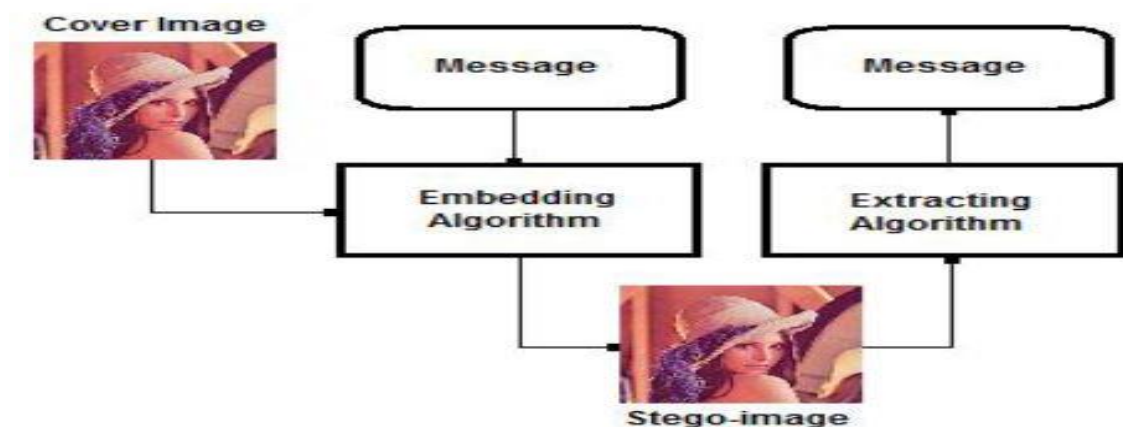


Figure 2.2 steganography source :[2]



## **2.9.1 Steganography Techniques**

Encryption techniques can be broadly divided as follows[11]:

### **2.9.1.1 Least-Significant Bit Modifications (LSB)**

The most widely used technique to hide data, is the usage of the LSB. When using a 24-bit color image, a least significant bit of each of the red, green and blue color components can be replaced by a bit of secret message, so a total of 3 bits can be stored in each pixel.

Disadvantages of using LSB are that it requires a quite large cover image to create a usable amount of hiding space. Secondly when compressing an image concealing a secret message using a lossy compression algorithm. The hidden message will be effected and is lost after the transformation.

### **2.9.1.2 Masking and Filtering**

Masking and filtering techniques, commonly restricted to 24-bits or grayscale images. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the brightness of parts of the image.

### **2.9.1.3 Transformations**

A more complex techniques of image steganography which use and modify the discrete cosine transformations (DCT) of image.

Discrete cosine transformations (DCT), are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image, into 64 DCT coefficients each.

## 2.10 Model-View-Controller (MVC)

Isolating the functional units from each other when building interactive applications helps programmers develop software modules that are easy to understand and modify without having to know all the details of other modules.

Model-View-Controller, Is an architectural web design pattern that separates an application into three main logical components: The Model component corresponds to all the data-related logic that the user works with. The View component is used for all the UI logic of the application. Controllers act as an interface between Model and View components to process all the business logic and incoming requests, manipulate data using the Model component and interact with the Views to render the final output[12].

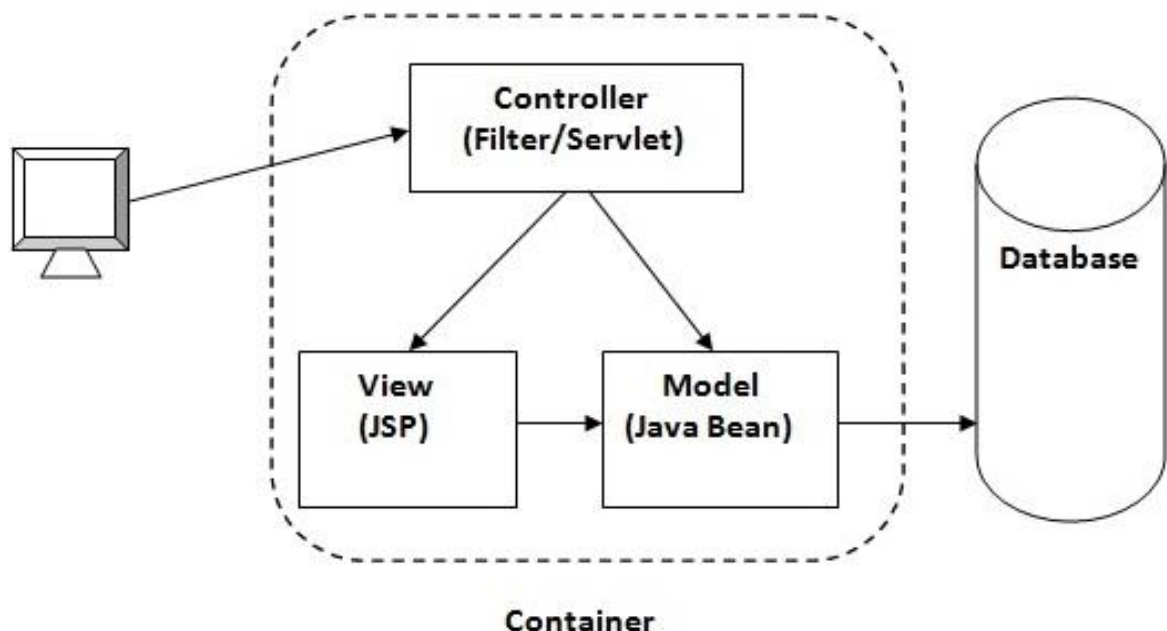


Figure 2.3 model-view-controller

## **2.11 Related Works**

### **2.11.1 Passwords Management via Split-Key**

Kenneth Giuliani, V. Kumar Murty and Guangwu Xu, proposed scheme combining three components which are user, server and web service, the password saved encrypted in the server. The encryption and decryption key is splits into two shares, one for user and the other saved in the server. User share is derived from passphrase selected by user, and the Server share derived from user share and encryption key. The user and server authenticate each other than the server send user log in data (user-ID and encrypted password) and server share to the user. Then the user decrypts the encrypted password and sent it with user-ID to the service. The encryption and decryption performed in the user side only. SHA-512 Hash function and AES Encryption algorithm are used. Unfortunately the password is sends to the web service as clear text, so it can be compromised by eavesdroppers[13].

### **2.11.2 Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography**

Mehdi Hossain and others, proposed a model which encrypts the password in client side using AES encryption algorithm. The encrypted password then embedded in an image using Least Significant Bit (LSB) steganographic algorithm. The image sent to the server over the internet. Then the server extracts the encrypted password from the image and decrypts the encrypted password. Further the server verifying of the actual password with one which stored in database.

But the computation complexity is quite high due to image data manipulation for both client and server ends and password was stored as clear text without encryption[2].

### **2.11.3 A Two Factor Authentication System with QR Codes for Web and Mobile Applications**

The model has been implemented by developing a two-factor identity verification system where the first factor is user credentials (username and password), and the second factor is the user smart / mobile phone device and a pseudo-random generated alphanumeric QR code which used as one time password token sent to the user via e-mail or MMS. Then the user have to scanning the QR code on web camera manually. The system should check, verify and validate the QR code[14].

It will be observed that the model requires mobile device and web camera. And there are time and space consuming due to image manipulation.

### **2.11.4 A New Advanced User Authentication and Confidentiality Security Service**

This paper introduces a new way of user authentication, which is done through two factor authentication system. First factor is graphical user name. Second factor is voice password. In User authentication through graphical user name, System will provide a series of pictures. Three pictures are randomly selected by the user with some sequence. These three pictures will act like a user name. System will accumulate the 1 byte unique binary number of each picture and save it as a pattern. System will save the pattern in the database for future login. To login the user has to select previously chosen pictures sequentially. The system will match the pattern with previously saved pattern. User authentication through voice password. System will provide a button to record the voice. User has to click on the button & say something. System will record the voice and sample the sound in digital format (binary form). System will save the binary number in the database which will act as password. In User login. System will provide a button to record the voice. User has to click on the button and say the previously

recorded words. System will capture the sound. Then system will sample the sound and digitized it in binary form. Then system will match both the binary pattern[15].

In this paper, multimedia objects are used for authentication which cause time and space consuming. Using sound as a second factor is difficult if there is interference.

### **2.11.5 User Authentication Using Smart Phone and One Time Password**

Author proposed a model for user authentication using smartphone. The smartphone must have special application installed on it, this application connected to server, the user open android application in his smartphone and enter username and password to request one time password (OTP) from server. The OTP will send from server to smartphone in encrypted form using AES encryption algorithm with three minutes life time before it become expired. Then user enter new username and password with generated OTP into website to access his account. If the username, password and OTP are matched and the OTP not expired he will gain access otherwise he will not[16].

There are some notes; first of all, the whole users must have smartphones with special application. Secondly, user needs two pair of username and password, one for android application and the other for website. In the login user enters username, password and OTP together which make this scheme vulnerable to reply attack within three minutes.

## **CHAPTER III**

### **METHODOLOGY**

## **3. METHODOLOGY**

### **3.1 Introduction**

This chapter describes research methodology and system components and it shows how the system works using unified modeling languages.

### **3.2 Proposed Model**

This model will be implemented in file store service which is a website that provides ability of uploading and downloading files. Model-View-Controller architecture is used to implement this model.

#### **3.2.1 System Implementation Steps:**

1. Firstly, user has to create an account with username, password and e-mail.
2. The system generates a hash code of password from actual password using SHA-512 cryptographic hash function.
3. Only 128-bits of 512bits of hash code will be used as a hashed image of password.
4. The username, password hashed image and e-mail will be sent to the server to be stored in database.
5. In login phase, user enters his credential data. SHA-512 hash function will be called and a 128-bit of password's hashed image will be sent with username to server.
6. The server matches user credentials with the previously saved, if they match then,
7. The server generates a random number using system time as a seed, which is then used to generate 128-bits hash code that is considered as verification code. This code will be expired either after 5 minutes

(verification code lifetime) of its generation or after authentication (it is available to use only onetime during its lifetime).

8. The verification code then will send to user's e-mail.
9. Then user enters the verification code. If it is correct and never used during its lifetime the system allow user to login.

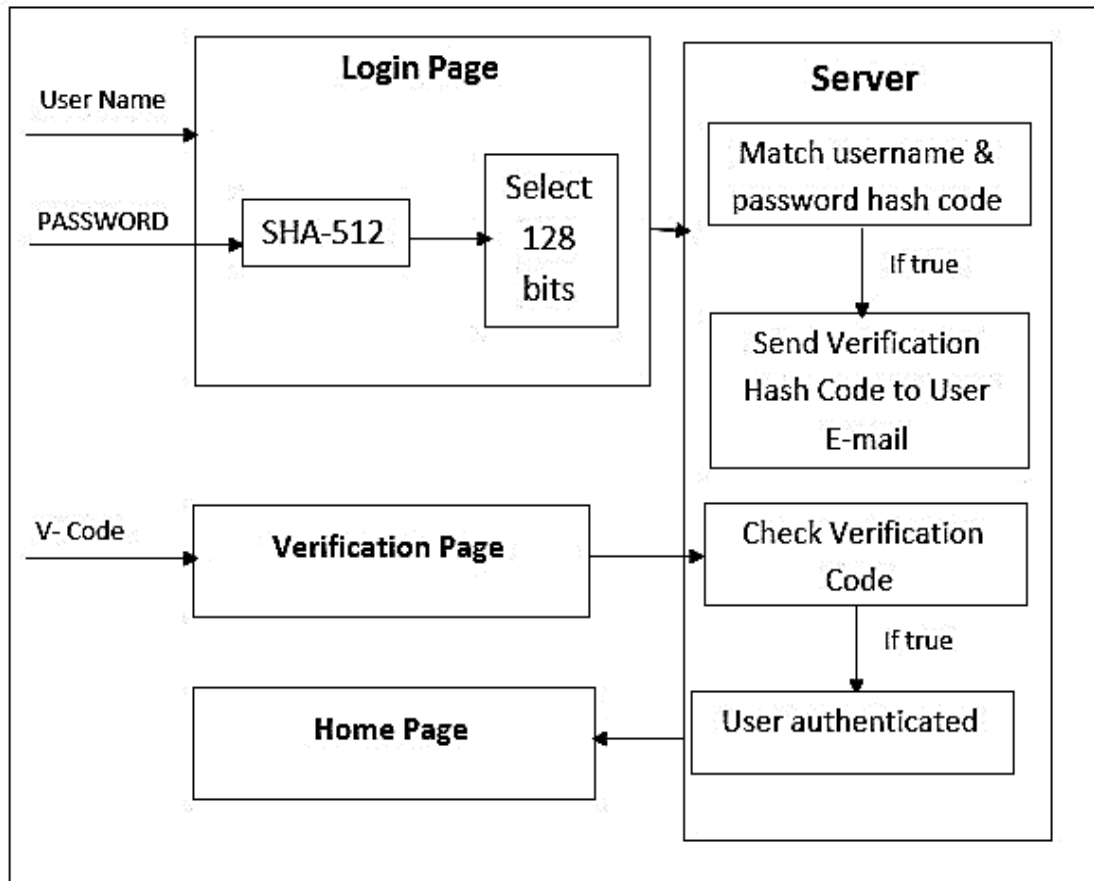


Figure 3.1 : proposed model methodology

The above Figure illustrate the main operations of the proposed models which consist of some operations, password hashed image generation, user credential matching and verification.



### 3.3 System Analysis

#### 3.3.1 System Operations

The main file store web site operations which can be performed by user in this system can show in figure (3.2) below.

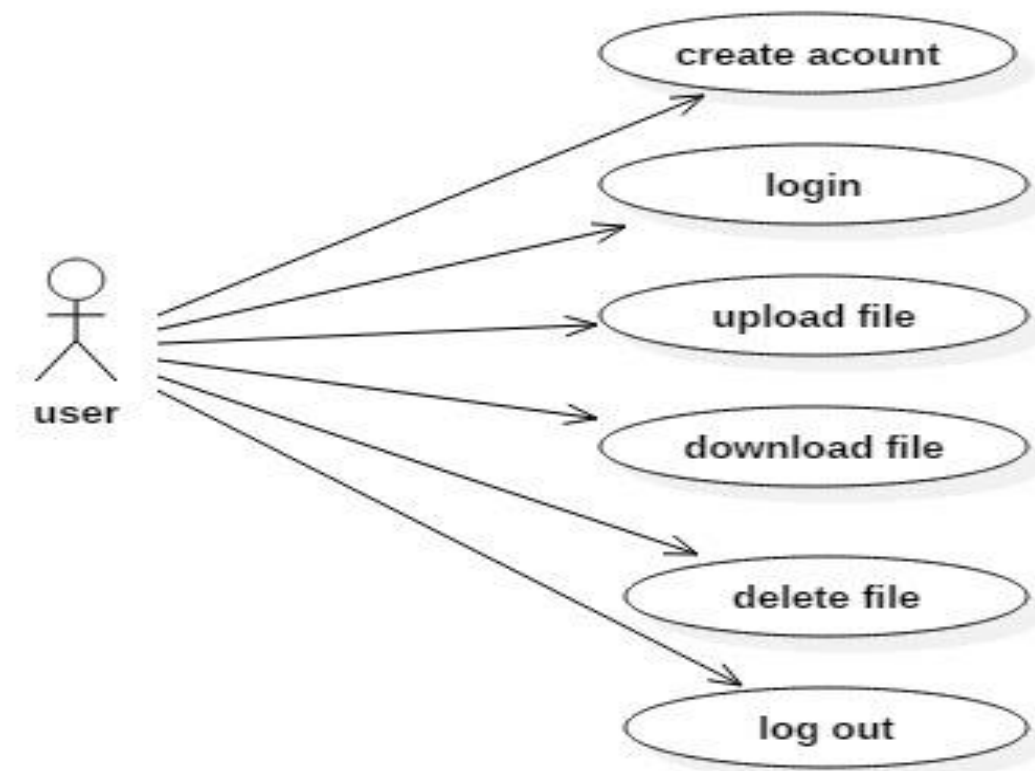


Figure 3.2: system operations

The user is able to create an account, login, upload files, download files, delete file and logging out as in figure (3.2).

### 3.3.2 System flowchart

Figure (3.3) represent system processes in flowchart.

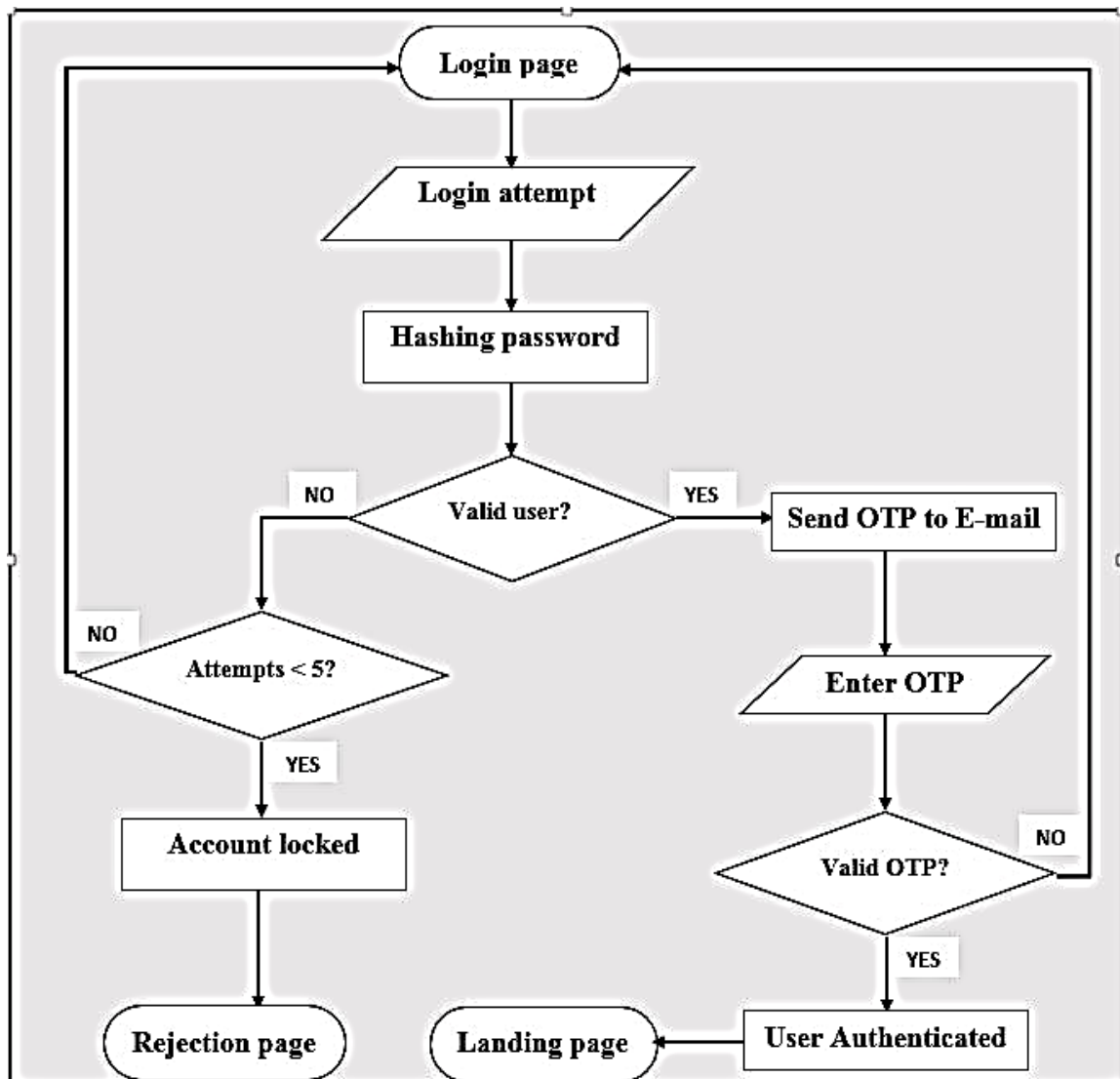


Figure 3.3: system flowchart

When user attempt to login, a hash image of the password will be generated. Then the validity of user account is checked as in figure (3.3). If user account is valid, then user have to enter the one time password (OTP). If OTP is valid, user considered authorized or he must attempt to login again. User account will lock after five attempts.

### 3.3.3 Registration Sequence Diagram

Figure (3.4) illustrate the first operation in this model which is registration or creating an account.

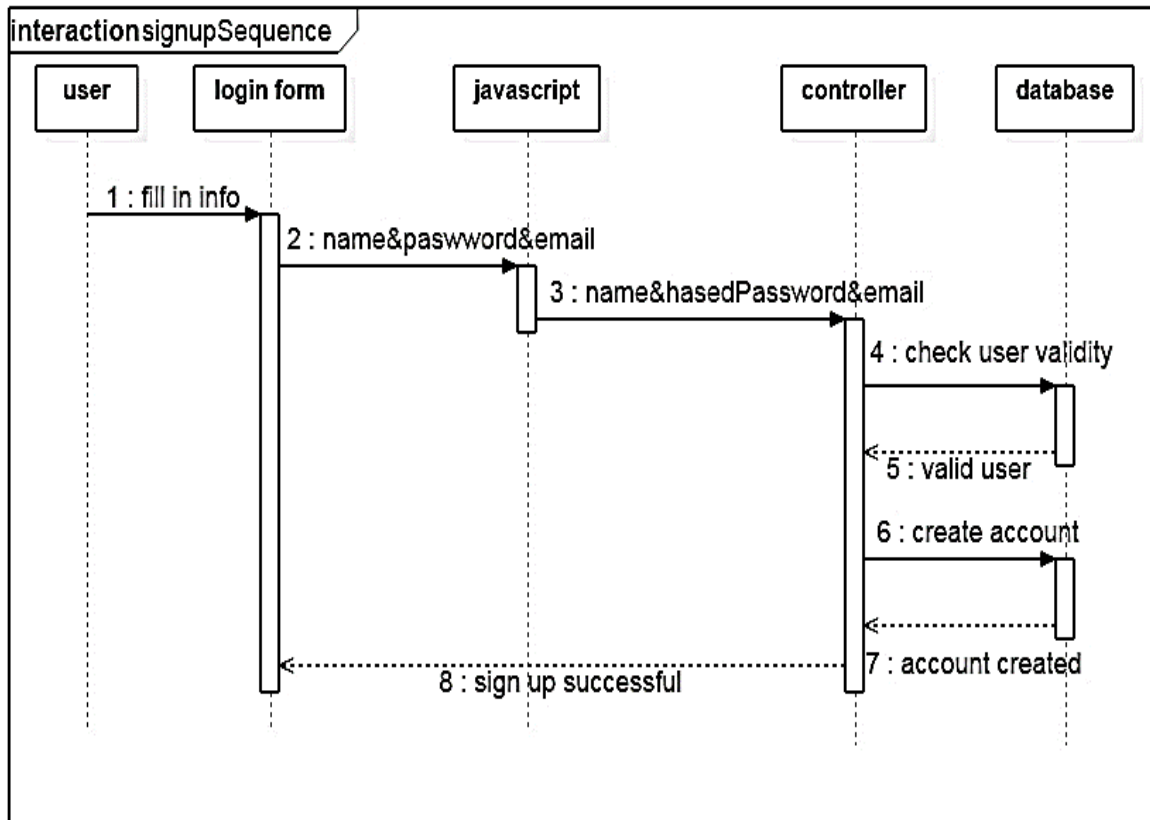


Figure 3.4: sign up sequence diagram

Figure (3.4) shows the interactions between user and the system components in registration sequence operation. In step one user enter his username, password and his e-mail which are send to step two where the hash code of password will generated. In step three username, hash code of password and e-mail are send to the controller which checks the availability of the username in step four. If the user is available then the user data are saved into data base and his account will be created in step five. Then a message sent to user such as in step six.

### 3.3.4 Login Sequence Diagram

After registration, the user have to login to system using his username and password. Then the system will authenticate him as below in figure (3.5):

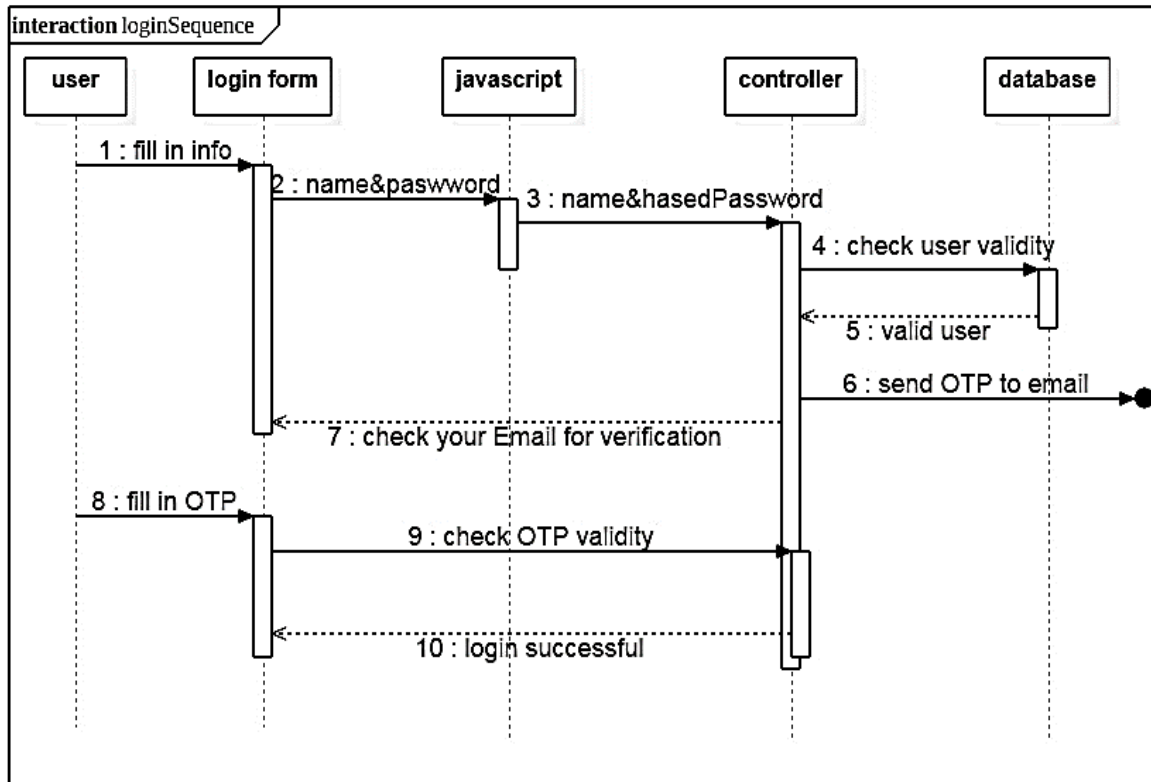


Figure 3.5: login sequence diagram

Steps one, two and three in figure (3.5) are similar to the three first steps in figure (3.4). In step four the controller matching the given user data with which stored in database user authenticity. Step five show if the authenticated or not, if he is authenticated an OTP will generated and sent to user e-mail in step six and a message send back to user to check his e-mail. In step nine the check the validity of OTP which entered by user in step eight. The last step show if the login operation is succeeded or not.

## **CHAPTER IV**

# **IMPLEMENTATION AND RESULTS**

## **4. IMPLEMENTATION AND RESULTS**

### **4.1 Introduction**

This chapter shows the proposed model which were described in the previous chapter. The proposed model has been implemented within a Model-View-controller (MVC) web based architecture where the view is developed in HTML and JavaScript scripting language, while the model and controller are developed in java programming language, then user data were stored in MySQL database. SHA-512 one-way hash function is used to secure the password.

### **4.2 System Hardware**

The hardware platform on client side is a user's device with internet browser within it. In the server side, the hardware platform is a web server.

### **4.3 System Interfaces**

This section shows the main screens and system messages which represent the core phases of user authentication operations and the interactions between System components.

### 4.3.1 Sign Up Page

To get benefits of this system, first of all user must create an account and fill in some information as appear in figure (4.1).



The image shows a sign-up form with a light green background. At the top, the text "SIGN UP" is written in large, bold, orange letters. Below this, there are four white input fields with rounded corners, each containing a placeholder label: "FULL NAME", "USER NAME", "PASSWORD", and "E-MAIL". At the bottom of the form, there is a prominent orange button with the text "SIGN UP" in white, bold letters.

Figure 4.1: sign up form

In this page, user must enter his full-name, user-name, password and E-mail to create new account as showed in figure (4.1). After fill in all of these field user will click on sign-up button which is called a JavaScript function to generate the hashed image of the password. This hashed image will saved in database instead of the actual password. The actual password never stores in database so it can't be retrieved from system. Then JavaScript function will send the user credentials to server after replace password with its hashed image to get saved in database to be ready to use later in user Authentication.

### 4.3.2 Login Page

After signing up, user need to sign in to access and use the system features. Figure (4.2) shows the login form.



Figure 4.2: login form

As in figure (4.2), the first field for username and the second one for password. When user fill in these fields and click on login button a password hash code will be generated and sent with username to server. The system will check the validity if the user is authenticated, one time password (OTP) send to user E-mail. Then system redirect user to the OTP page that represent in figure (4.5) with a message to user to check his E-mail, if user credentials are incorrect error message will appear such as in figure (4.6).



### 4.3.3 Login Error Message

When user enter incorrect username or password, an error message will retrieved as in figure (4.3).



Figure 4.3: Login Error Message

Figure (4.3), show a message when username or password which entered by user are incorrect.

#### 4.3.4 OTP code

When username and password which are entered by user in figure (4.2) are matched with which Stored in database, the OTP will be generate and send to user e-mail as in figure (4.4):

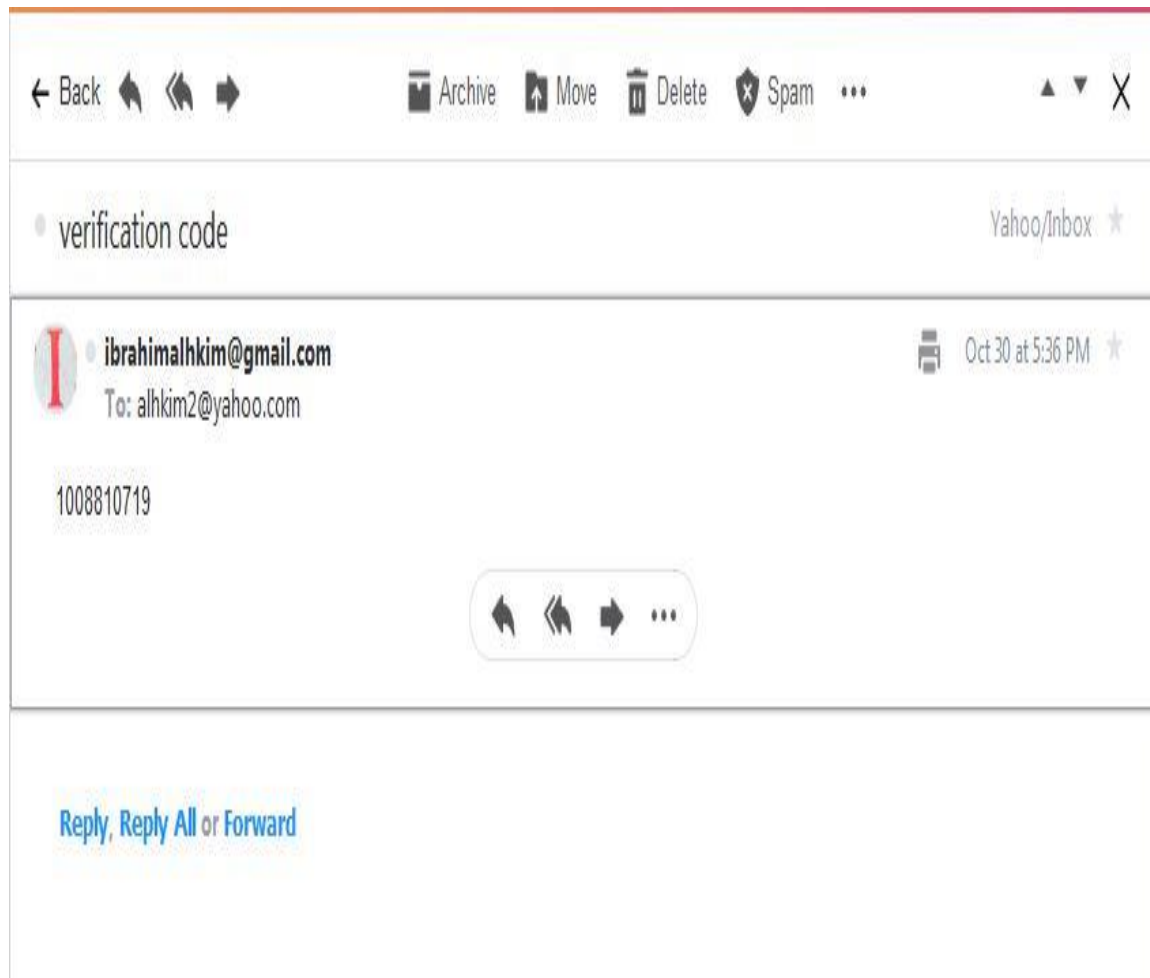


Figure 44.: OTP code sent to E-mail

Figure (4.4), illustrate OTP in user e-mail which consist of ten digits. This OTP will be used as a second factor authentication.

### 4.3.5 OTP Page

Figure (4.5), provide a field for OTP verification code which was received in user email.

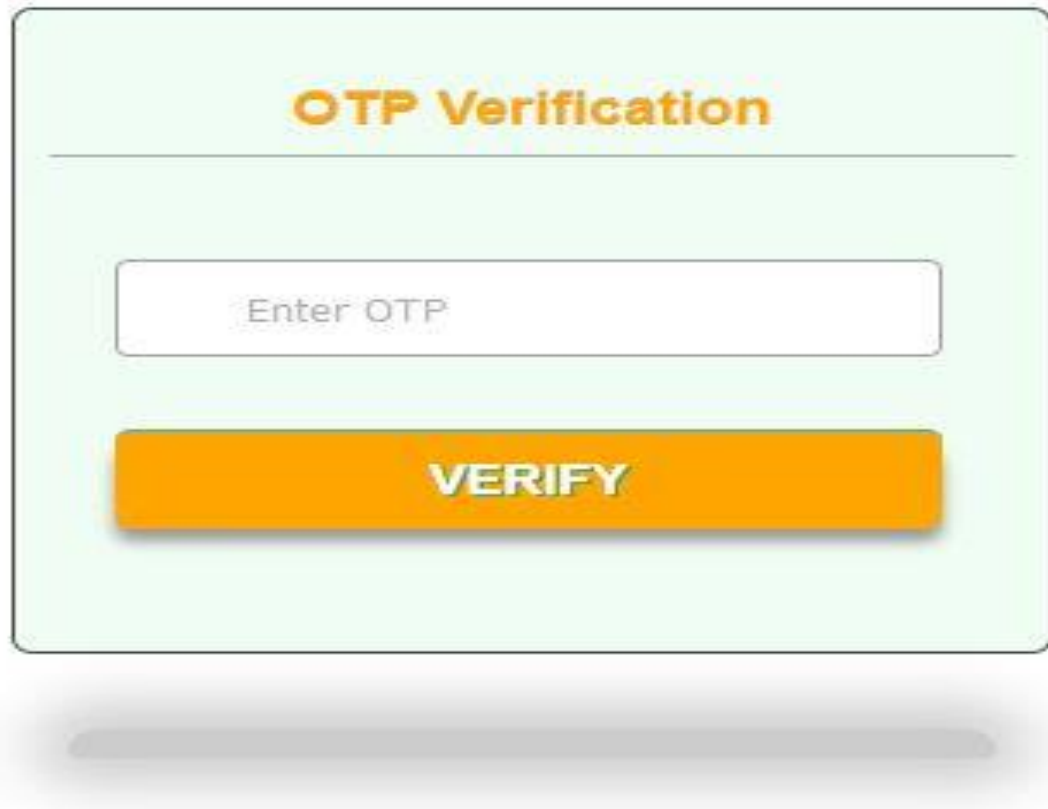
The image shows a mobile-style OTP verification form. At the top, the title "OTP Verification" is displayed in orange text. Below the title is a horizontal line. Underneath the line is a white text input field with the placeholder text "Enter OTP". Below the input field is a large, orange, rounded rectangular button with the word "VERIFY" written in white, bold, uppercase letters. The entire form is set against a light green background and is presented as if on a mobile device screen with a shadow below it.

Figure 4.5: OTP Verification Form

The user must copy the OTP from e-mail and paste it in field as in figure (4.5), then when user click on verify button , the system check if the OTP code is matched with which one were sent to user email and it's not expired, then the user can gain access to system. Or if the OTP is incorrect or it's expired the user will redirected to login page and an error message will popped up as in figure (4.6).

### 4.3.6 OTP Error Message

When the OTP is incorrect or expired, an error message will be retrieved as in figure (4.6).

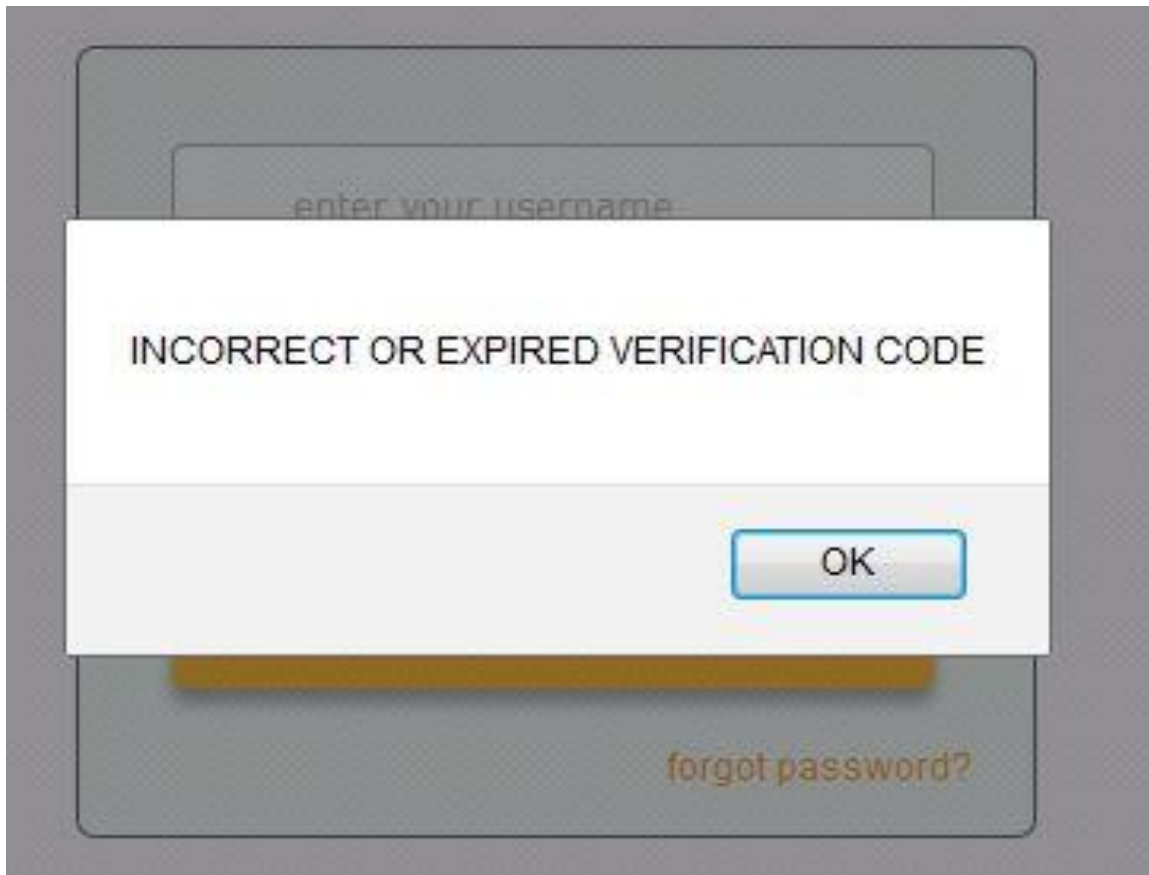


Figure 4.6: OTP Error Message

The message in figure (4.6), appears due to three reasons, either OTP is incorrect, expired or invalid.

#### **4.4 Results**

From the implementation of the proposed model, some results can be observed:

1. The method is secure against password stolen attack, replay attack and man-in-the middle attack.
2. This method can be implemented in low specification devices.
3. Easy to implement with no additional software or certificates requirement in client side.
4. Easy to use with less probability of error verification code entering (copy & past).
5. High performance and less processing power comparing with using AES algorithm.
6. Less computation complexity for both client and server ends due to using SHA-512 instated of image steganography.

#### **4.5 Discussion**

1. It is difficult to guess the password or because of using cryptographic hash function which generate specific length hash code from different input length.
2. There are two probabilities of Replay attack, the first when attacker replay username and password. In this case, the OTP code will be sent to user e-mail so attacker can't access it. Or the attacker may replay the OTP code which it will be expire after first use or the end of its lifetime.

## 4.6 Evaluation and Comparison

The next table show the comparison the proposed model to models which discussed as related works in chapter II.

**Table 4-1: Evaluation and Comparison**

Model name	Techniques	Results	Open issues
User Authentication Using Smart Phone and One Time Password[16]	<ul style="list-style-type: none"> <li>- AES Encryption algorithm</li> <li>- One Time Password</li> </ul>	<ul style="list-style-type: none"> <li>- The encryption and decryption performed in the user side only</li> </ul>	<ul style="list-style-type: none"> <li>- Mobile with android app is required.</li> <li>- Vulnerable to replay attack within three minutes.</li> <li>- Using couple of usernames and passwords.</li> </ul>
Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography[2]	<ul style="list-style-type: none"> <li>- AES encryption algorithm</li> <li>- Least Significant Bit (LSB) steganographic algorithm.</li> </ul>	<ul style="list-style-type: none"> <li>- Secure Password Transmission with high computation complexity</li> </ul>	<ul style="list-style-type: none"> <li>- High computational Complexity cause of cryptography and steganography</li> <li>- Vulnerable to password stolen attack</li> </ul>
A Tow Factor Authentication System with QR Codes for Web and Mobile Applications[14]	<ul style="list-style-type: none"> <li>- QR code used as one time password.</li> </ul>	<ul style="list-style-type: none"> <li>- Provide secure password transmission.</li> </ul>	<ul style="list-style-type: none"> <li>- Requires mobile device and web camera.</li> <li>- Complex due to image manipulation.</li> <li>- Hard to use cause of using mobile and web camera to read OTP</li> </ul>
A New Advanced User Authentication and Confidentiality Security Service[15]	<ul style="list-style-type: none"> <li>- Graphical user name.</li> <li>- Voice password.</li> </ul>	<ul style="list-style-type: none"> <li>- Password is secured during transmission.</li> </ul>	<ul style="list-style-type: none"> <li>- More Complex due to image manipulation and voice recognition</li> <li>- Using sound as a second factor is difficult if there is an interference.</li> </ul>
The proposed model	<ul style="list-style-type: none"> <li>- SHA-512 hash function.</li> <li>- OTP.</li> </ul>	<ul style="list-style-type: none"> <li>- Secure against replay attack.</li> <li>- Suitable to low specification devices.</li> <li>- Password stored encrypted.</li> </ul>	<ul style="list-style-type: none"> <li>- Actual password can't retrieved when it forgot</li> </ul>

## **CHAPTER V**

### **CONCLUSION AND RECOMMENDATIONS**

## **5 CONCLUSION AND RECOMMENDATIONS**

### **5.1 Introduction**

This chapter shows research conclusion and recommendations.

### **5.2 Conclusion**

The existing schemes are vulnerable to some attacks. In this research, a new secure user authentication scheme is proposed against the password guessing attack, replay attack and key logger attack. Moreover, the proposed scheme can compute faster because it is based only on a one-way hash function. We can apply the proposed scheme to low specification devices.

### **5.3 Recommendations**

This model show how two factor authentication provide security against several password attacks. The verification code which would send to user email is core of this model. So a good manage of email password is recommended.

The password won't be saved anywhere, so when the user forgot his password he will can't access the system any more. Then researcher recommend that it necessary to find a mechanism to deal withss this issue.



## **REFERENCES**

## References

- [1] W. Stallings, *Network security essentials: applications and standards*. Pearson Education India, 2007.
- [2] M. Hussain, A. W. A. Wahab, I. Batool, and M. Arif, "Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography," *vol*, vol. 9, pp. 179-188, 2015.
- [3] R. P. McEvoy, F. M. Crowe, C. C. Murphy, and W. P. Marnane, "Optimisation of the SHA-2 family of hash functions on FPGAs," in *Emerging VLSI Technologies and Architectures, 2006. IEEE Computer Society Annual Symposium on*, 2006, p. 6 pp.: IEEE.
- [4] B. T. Hsieh, H. M. Sun, and T. Hwang, "On the security of some password authentication protocols," *Informatica*, vol. 14, no. 2, pp. 195-204, 2003.
- [5] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.
- [6] E. Talbot, S. Peisert, and M. Bishop, "Principles of Authentication," 2014.
- [7] R. Isawa and M. Morii, "One-Time Password Authentication Scheme to Solve Stolen Verifier Problem," in *Proc. of Forum on Information Technology*, 2011.
- [8] C.-M. Chen and W.-C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Transactions on communications*, vol. 85, no. 11, pp. 2519-2521, 2002.
- [9] Z. Zhao and Z. Wang, "Security analysis of a password-based authentication protocol proposed to IEEE 1363," *arXiv preprint arXiv:1207.5442*, 2012.
- [10] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

- [11] R. Krenn, "Steganography and steganalysis," ed: January, 2004.
- [12] G. E. Krasner and S. T. Pope, "A description of the model-view-controller user interface paradigm in the smalltalk-80 system," *Journal of object oriented programming*, vol. 1, no. 3, pp. 26-49, 1988.
- [13] K. Giuliani, V. K. Murty, and G. Xu, "Passwords Management via Split-Key," *Journal of Information Security*, vol. 7, no. 03, p. 206, 2016.
- [14] M. Eminagaoglu, E. Cini, G. Sert, and D. Zor, "A Two-Factor Authentication System with QR Codes for Web and Mobile Applications," in *Emerging Security Technologies (EST), 2014 Fifth International Conference on*, 2014, pp. 105-112: IEEE.
- [15] S. Majumder, S. Chakraborty, and S. Das, "A New Advanced User Authentication and Confidentiality Security Service," *arXiv preprint arXiv:1406.4748*, 2014.
- [16] A. G. A. Tatai, "USER AUTHENTICATION USING SMART PHONE AND ONE TIME PASSWORD," Sudan University of Science and Technology, 2017.