

بسم الله الرحمن الرحيم



Sudan University of Science & Technology
College of Graduate Studies

Use of A multi Factor Authentication System For Banking Application

إستخدام نظام تحقق متعدد العوامل لتطبيقات البنوك

Thesis Submitted in Partial Fulfillment of the Requirements of the
Master's Degree in Computer Science

By:
Hazim Abdurrahman Mohammed

Supervisor:
Dr. Faisal Mohammed Abdalla

Oct 2020

الآية

(وَقُلْ أَعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ
إِلَىٰ عِلْمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ)

(التوبة : 105)

صدق الله العظيم

DEDICATION

This thesis is dedicated

To my late father, the reason what I become today

To my dear mother, thanks for your great support and continuous care

*To my sisters, my brothers, my late little brother I am really grateful to
all of you*

You have been my inspiration, and my soul mates

ACKNOWLEDMENT

Firstly, I would like to express my sincere gratitude to my advisor Dr. Faisal Mohammed Abdalla for the continuous support of my M.Sc study: A multi Factor Authentication System For Banking Application, and for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my M.Sc study.

Abstract

Especially in light of the great development that the financial technology industry has witnessed during the recent period, and the enhancement of the level of services provided to customers through new innovative channels, far from the traditional banks used to provide banking services, This increased the chances of them being attacked by hackers to find out the weaknesses that can be used in order to eavesdrop to affect sensitive data in several ways, and this is one of the challenges facing banks and financial sectors in general. Therefore, a secure mechanism for authentication between the bank and their customers must be found to provide confidentiality and privacy. There are some common types of authentication, such as Static Password Authentication which are known to be unsafe because the majority of people use short and simple passwords.

This study proposed to authenticate the user over the Internet using a multi-factor verification system to reduce the hacking and theft of sensitive client data.

المستخلص

إن التطور الكبير الذي شهدته صناعة التقنيات المالية خلال الفترة الأخيرة، وتعزيز مستوى الخدمات المقدمة للعملاء من خلال قنوات جديدة مبتكرة، بعيداً عن التقليدية التي اعتادت عليها المصارف لتقديم الخدمات المصرفية، ما زاد من فرص تعرضها للهجمات من قبل المخترقين لمعرفة نقاط الضعف التي يمكن استغلالها من أجل التنصت للتأثير على البيانات الحساسة بعدة طرق ، و هذه من التحديات التي تواجه البنوك والقطاعات المالية بشكل عام.

لهذا يجب الوصول إلى آلية آمنة للمصادقة بين البنك و عملائهم لتوفير السرية والخصوصية.

هناك بعض الأنواع الشائعة من المصادقة ، مثل مصادقة كلمة المرور الثابتة والتي تُعرف بأنها غير آمنة لأن غالبية الأشخاص يستخدمون كلمات مرور قصيرة وبسيطة.

اقترحت هذه الدراسة لمصادقة المستخدم عبر الإنترنت باستخدام نظام تحقق متعدد العوامل للحد من عمليات الإختراق و سرقة البيانات الحساسة للعميل

Table of contents

TOPIC	PAGE NO
الأية	I
DEDICATION	II
ACKNOWLEDGEMENT	III
ABSTRACT	IV
المستخلص	V
TABLE OF CONTENTS	VI
LIST OF TABLES	VIII
LIST OF FIGURES	IX
LIST OF ABBREVIATIONS	X
CHAPTER ONE INTRODUCTION	
1.1 INTRODUCTION	1
1.2 PHISHING ATTACKS	2
1.3 PROBLEM STATEMENT	5
1.4 OBJECTIVE OF THE THESIS	5
1.5 RESEARCH HYPOTHESES	5
1.6 SIGNIFICANCE OF THE RESEARCH	6
1.7 RESEARCH SCOPE	6
1.8 METHODOLOGY	7
1.9 THESIS ORGANIZATION	7
CHAPTER TWO LITERATURE REVIEW & RELATED WORKS	
2.1 INTRODUCTION	8
2.2 SECURITY SERVICES	8
2.3 TYPES OF SECURITY SERVICES	8
2.3.1 AUTHENTICATION	9
2.3.2 PASSWORD	10
2.3.3 STRENGTH OF PASSWORD AUTHENTICATION	10
2.3.4 VULNERABILITIES OF PASSWORD RETRYING	10
2.4 CRYPTOGRAPHY	11
2.4.1 MODERN CRYPTOGRAPHY CONCERNS	12
2.4.2 THREE TYPES OF CRYPTOGRAPHIC TECHNIQUES USED IN GENERAL	12
2.5 FACTOR AUTHENTICATION	13
2.5.1 TWO-FACTOR AUTHENTICATION	14

2.5.2 MULTI-FACTOR AUTHENTICATION	15
2.6 HASH FUNCTION	17
2.7 BIOMETRICS	17
2.8 RELATED WORK	20
2.8.1 TECHNIQUES FOR DETECTING ZERO DAY PHISHING WEBSITES	20
2.8.2 PHISHING WITHIN E-COMMERCE	20
2.8.3 SEPARABLE IDENTITY-BASED RINGSIGNATURE	21
2.8.4 ONE-TIME PASSWORD AUTHENTICATION	22
CHAPTER THREE THE METHODOLOGY	
3.1 INTRODUCTION	24
3.2 DIGITAL SIGNATURE	24
3.3 TECHNOLOGIES AND REQUIREMENTS	25
CHAPTER FOUR DESIGN AND IMPLEMENTATION	
4.1 ACTIVEXPERTS SMS AND MMS COMPONENT 5.1	27
4.2 PROGRAMMING PROCESS	27
4.3 PROGRAMMING MAINTENANCE	28
4.4 IMPLEMENTATION	29
4.4.1 INDEX.PHP	29
4.4.2 REGISTER.HTML	30
4.4.3 REGFORM.PHP	31
4.4.4 LOGIN_HOME.PHP	31
4.5 SYSTEM TEST AND RESULT	33
CHAPTER FIVE CONCLUSION AND RECOMMENDATION	
5.1 CONCLUSION	36
5.2 FUTURE WORK	36
REFERENCES	37

List Of Tables

Table No.	Table Title	Page No.
4.5.1	Case1	34
4.5.2	Case 2	35

List Of Figures

Figure No.	Table Title	Page No.
3.4	Login Diagram	26
4.1	Home Page	29
4.2	Register page	30
4.3	Login page	32

List Of Abbreviations

2WAMS - 2 Way Mobile Authentication Systems

SMS - Short Messaging Service

PHP - Personal Home Pages

HTML- Hypertext Markup Language

SQL - Structured Query Language

SIM - Subscriber Identity Module

DSA - Digital Signature Algorithm

DSS - Digital Signature Standard

CHAPTER ONE

Introduction

1.1. Introduction

While the Internet has brought unprecedented convenience to many people for managing their finances and investments, it also provides opportunities for conducting fraud on a massive scale with little cost to the fraudsters. Fraudsters can manipulate users instead of hardware/software systems, where barriers to technological compromise have increased significantly. Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

1.2. Phishing Attacks

Phishing was a term originally used to describe email attacks that were designed to steal your online banking username and password. However, the term has evolved and now refers to almost any email-based attack. Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking an action. These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. These emails then entice you into taking an action, such as clicking on a link, opening an attachment or responding to a message. Cyber criminals craft these emails to look convincing, sending them out to literally millions of people around the world. The criminals do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know the more emails they send out, the more people they may be able to fool. [1]

The 5 most common types of phishing attack

1. Email phishing

Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organisation and sends thousands out thousands of generic requests.

The fake domain often involves character substitution, like using 'r' and 'n' next to each other to create 'rn' instead of 'm'.

Alternatively, they might use the organisation's name in the local part of the email address (such as paypal@domainregistrar.com) in the hopes that the sender's name will simply appear as 'PayPal' in the recipient's inbox.

There are many ways to spot a phishing email, but as a general rule, you should always check the email address of a message that asks you to click a link or download a attachment.

2. Spear phishing

There are two other, more sophisticated, types of phishing involving email. The first, spear phishing, describes malicious emails sent to a specific person. Criminals who do this will already have some or all of the following information about the victim:

- Their name;
- Place of employment
- Job title
- Email address
- Specific information about their job role.

One of the most famous data breaches in recent history, the hacking of the Democratic National Committee, was done with the help of spear phishing.

The first attack sent emails containing malicious attachments to more than 1,000 email addresses. Its success led to another campaign that tricked members of the committee into sharing their passwords.

3. Whaling

Whaling attacks are even more targeted, taking aim at senior executives. Although the end goal of whaling is the same as any other kind of phishing attack, the technique tends to be a lot subtler.

Tricks such as fake links and malicious URLs aren't useful in this instance, as criminals are attempting to imitate senior staff.

Scams involving bogus tax returns are an increasingly common variety of whaling. Tax forms are highly valued by criminals as they contain a host of useful information: names, addresses, Social Security numbers and bank account information.

4. Smishing and vishing

With both smishing and vishing, telephones replace emails as the method of communication. Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation.

A common vishing scam involves a criminal posing as a fraud investigator (either from the card company or the bank) telling the victim that their account has been breached.

The criminal will then ask the victim to provide payment card details to verify their identity or to transfer money into a ‘secure’ account – by which they mean the criminal’s account.

5. Angler phishing

A relatively new attack vector, social media offers a number of ways for criminals to trick people. Fake URLs; cloned websites, posts, and tweets and instant messaging (which is essentially the same as smishing) can all be used to persuade people to divulge sensitive information or download malware.

Alternatively, criminals can use the data that people willingly post on social media to create highly targeted attacks. [2]

1.3. Problem Statement

Along with the significant growth in Internet usage, threats such as phishing have also drastically increased. Criminals have become smarter, using highly sophisticated technologies and social engineering techniques to commit information theft. This threat has resulted in Internet users having less trust.

which led to the interest of banks in the security aspects of their networks and systems, and among these aspects of authentication, in most systems the user name and password are used Only to access the system for the login process, which is considered one of the old traditional methods, is easy to hack for the following reasons

- Passwords are easy to guess and break
- Repeated use of the same password in multiple accounts of the client

1.4. Objective Of the Thesis

The main objective of this projects to make banking account more secure and protect sensitive user information from phishing, which increases their confidence and their willingness to use these sites and use them without fear to their personal data and sensitive. Prevent password stolen attack by multi Factor Authentication of password instead of the actual password.

1.5. Research Hypotheses

- multi factor authentication can overcome replay attack .
- How to gain user confidence.

1.6. Significance of the research

In recent times, credibility has become an important issue due to the increase in the use of online applications, which is followed by the increase in penetration of sensitive information, and this leads to a decrease in confidence and the inability of banks in the event of loss or leakage of this information.

So there must be a secure method of user authentication between the client and the server over the Internet

Password-based authentication is the most popular method in a client / server environment.

But this approval has become easy to break and guess.

So it is very important to find secure authentication mechanisms.

1.7. Research Scope

In this research we proposed a secure and effective password-based user authentication system for client/server environment using md5 cryptographic hash function to protect password against Password stolen attack, and multi Factor Authentication to overcome Man in the middle attack.

1.8. Methodology

Banking application system (authentication system)

Authentication means that before end-user enters the login information on the login page that particular login page authenticates to the end-user that it's not fake. So, let's take a scenario in which user have to enter Username and Password, So how can user identify whether he/she is accessing the right page or not. So over here we can introduce third term that is whenever user will enter the username in the login page, will be checked.

1.9. Thesis Organization:

The remainder of this research is structured as follows.

The next Chapter background and related work. In chapter three will illustrate the methodology of the research. Chapter four the system design and implementation.

Chapter Five Conclusions and Future Work.

CHAPTER TWO

LITERATURE REVIEW and RELATED WORKS

2.1. Introduction

This chapter introduces some issues and definitions related to information security and user authentication mechanisms, along with some relevant previous studies.

2.2. SECURITY SERVICES

a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers. Also the RFC 2828 defines security services as a processing or communication service that is provided by a system to give a specific kind of protection to system resources. Security Services implement security policies and are implemented by security mechanisms. X.800 divides these services into five categories and fourteen specific services as shown in the below Table. [3]

2.3. Types Of Security Services

types of security services defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. Perhaps a clearer definition is found in RFC 2828, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms. X.800 divides these services into five categories

and fourteen specific services Security services that are placed in the middleware layer of a distributed system can be trusted only if the services they rely on to be secure are indeed secure. For example, if a secure RPC service is partly implemented by means of SSL, then trust in the RPC service depends on how much trust one has in SSL. If SSL is not trusted, then there can be no trust in the security of the RPC service.

2.3.1. Authentication is the assurance that the communicating entity is the one that it claims to be. The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

1. Peer Entity Authentication- provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement to same protocol in different systems; e.g., two TCP modules in two communicating systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

2. Data-Origin Authentication- provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.[3]

2.3.2. Password

This type of authentication requires the supplicant recall what he knows. There are two parts in this method. First, the supplicant enters the username and second, the password. The password is the secret combination of words and numbers which the supplicant knows. [3]

2.3.3. Strength of Password Authentication

One of the strength is that longer password is very difficult to break. At the point when utilizing passwords, it's imperative to utilize solid passwords. A solid secret key has a blend of capitalized, lower case, numbers, and unique characters. Now security administrators recommend 12 characters passwords. [5]

2.3.4. VULNERABILITIES OF PASSWORD RETRYING

Due to the increasing growth of Internet and to offering numerous attractive applications, utilizations of websites have become very popular among all ages. Many of these websites among them, ask for usernames and passwords before utilizing their certain resources or facilities. However, from several studies it has been discovered that on an average, a user has to maintain a considerably higher number of accounts, e.g., 25 accounts as found from a study conducted by Florencio, et. Among these accounts, a user usually does not use the same password for all. There are several advantages of doing so, such as i) if one password gets compromised, the rest would still remain safe, ii) it is prescribed not to

utilize secret passwords in ordinary websites to lower down the possibilities of exposing secret passwords, and so on. Again, when a user has to maintain multiple passwords, memorability issue would always arise.

Although, we create accounts in several websites, however, only a few of them we access frequently. The rest of them, we do not use on a regular basis, mostly infrequently or seldom. Consequently, passwords of these websites are not remained memorized. Therefore, during the next visit, users may try some probable passwords. In this circumstance, retry attack is possible in two different ways. Firstly, if that website is a spoofing website, which acquires and stores all the passwords that is utilized during the authentication session; it would be able to capture several passwords when someone retries with multiple passwords. The attackers later can employ these passwords to breach other accounts of this particular user. The second one is a little bit trickier. In this case, the attacker would acquire the passwords by forcing a user to retry even though s/he has given the password correctly. In details, even though a user provides a valid password [6]

2.4. Cryptography

Cryptography is the study of art and science of preparing protected and secure data communication. The word cryptography is derived from the two Greek words; “kryptos” means “secret or hidden” and “graphos” means “to write”. The original message or text before going to any process is called plaintext or cleartext. The process of changing plaintext into secret form is called encryption. Once the original text has been encrypted, the resultant text is known as ciphertext or cryptogram. The process of converting ciphertext into plaintext is known as decryption.

2.4.1. Modern cryptography concerns with:

- Confidentiality - Information cannot be understood by anyone
 - Integrity - Information cannot be altered.
 - Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage
 - Authentication - Sender and receiver can confirm each other
- Cryptography is used in many applications like banking transactions, credit cards, computer passwords, and e-commerce transactions.

2.4.2. Three types of cryptographic techniques used in general.

1 - Symmetric-key Cryptography: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

2 - Public-Key Cryptography: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

3 - Hash Functions: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.[7]

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key. [8]

2.5. Factors of Authentication

An authentication factor is a category of security credential used to verify a user's identity and authorization before allowing that user to gain access to their account, send communications, or request data from a secured network, system, or application.

There are three common factors of authentication: something you are, something you know, and something you have. Let's break them down further:

- Something you are. This type of 2FA includes biometric methods like fingerprint, retinal or facial scans, handwriting analysis, or voice recognition. Most modern smartphones use face recognition, laptops often use fingerprint readers and you might even be asked to enter a handprint if you buy a season pass to an amusement park. Although this type of 2FA provides the strongest authentication of any two-factor authentication method, it's not perfect. Anyone who's ever had a device with the capacity to scan faces or fingerprints has experienced the frustration of trying and failing to get their iPhone to accept their face or fingerprint knows that.
- Something you know. This might be the most common factor used in two-factor authentication. Generally, this will be a password or personal identification number (PIN). Unfortunately, these

authentication factors are also the ones most vulnerable to security attacks. Many people use the same passwords on account after account, and if there's a breach on even one account, that means every account is compromised.

- Something you have. This type of factor is typically controlled through a device that is known to be in the possession of a rightful user (usually a smartphone). First, a user registers for an account with an email address and password, recording their phone number then. The user then logs into their account with that email address and password, at which point a one-time password is sent to the user's mobile phone number. Once the user enters that into their device, they gain access to their account and the system.

2.5.1. Two-Factor Authentication

Two-factor authentication (2FA) is a security process whereby users must provide two different authentication factors to verify their identity and access their account. This process ensures better protection of both a user's personal information, credentials, and other assets, while also improving the security around the resources the user can access. Certainly, two-factor authentication provides a higher level of security than authentication methods that rely on only one authentication factor (single-factor authentication), where the user provides only one factor (usually a password or PIN). A 2FA method would require a user to provide not just a password or a PIN, but a second factor, ranging from a biometric factor (a facial, retinal, or fingerprint scan) to a possession factor (a one-time use code sent to a smartphone known to be in a user's possession).

That extra layer of security means that even if an attacker knows a user's password, they won't be allowed access to their online account or mobile device. In fact, two-factor authentication has long been used to control who can access sensitive data and systems, and security professionals urge enabling two-factor authentication on all your online accounts, computers, and mobile devices.

Two-factor authentication is a key component of cybersecurity and the work done by Cybersecurity Analysts.[9]

2.5.2. multi-factor authentication?

Multi-factor authentication, or MFA, is a method of account access security that requires users to verify their identity in two or more ways to be able to sign in. This is much more secure than the traditional sign-on approach that only requires one method of authentication – usually a password.[10]

Multi-factor authentication (MFA) is a method of logon verification where at least two different factors of proof are required. MFA is also referred to as 2FA, which stands for two-factor authentication. MFA helps keep protect your data (email, financial accounts, health records, etc.) or assets by adding an extra layer of security. [11]

What are the types of multi-factor authentication?

There are generally three recognized types of authentication factors:

- **Something You Know** – includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.

- **Something You Have** – includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.).
- **Something You Are** – includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

By combining two or three factors from these three categories, a multi-factor authentication is crafted. Multi-factor authentication is preferred, as it is much more difficult for an intruder to overcome. With just a password, an attacker only has to have a single attack skill and wage a single successful attack to impersonate the victim. With multi-factor authentication, the attack must have multiple attack skills and wage multiple successful attacks simultaneously in order to impersonate the victim. This is extremely difficult and, thus, a more resilient logon solution.

Most online services and accounts offer true multi-factor authentication, and the number is growing. One excellent example of a multi-factor authentication supporting online service is that of PayPal. They currently offer at least two different multi-factor options. One option involves a credit card-sized device that produces on-demand a one-time-use six-digit PIN. The second option sends an SMS text message to your cell phone with a six-digit PIN. In either case, the PIN is used alongside your name

[11]

2.6. Hash Function

A hash function H is a transformation that takes a variable-size input m and proceeds a fixed-size string, which is called the hash value h . Hash functions with just this property have a variety of general computational uses, but when working in cryptography the hash functions are regular chosen to have some supplementary properties. This is a contract in lots of programming languages that allocate the user to dominate equality and hash functions for an object, that if two objects are the same their hash codes must be the same. Hash functions compress a n (arbitrarily) large number of bits into a small number of bits.

The hash function properties are:-

- Output does not reveal information on input.
- Hard to find collisions (different messages with same hash).
- One way cannot be reversed. [12]

2.7. Biometrics

A biometric identifier is one that is related to intrinsic human characteristics. They fall roughly into two categories: physical identifiers and behavioral identifiers. Physical identifiers are, for the most part, immutable and device independent:

- **Fingerprints:** Fingerprint scanners have become ubiquitous in recent years due to their widespread deployment on smartphones. Any device that can be touched, such as a phone screen, computer mouse or touchpad, or a door panel, has the potential to become an easy and convenient fingerprint scanner. According to Spiceworks, fingerprint scanning is the most common type of biometric authentication in the enterprise, used by 57 percent of companies.

- **Photo and video:** If a device is equipped with a camera, it can easily be used for authentication. Facial recognition and retinal scans are two common approaches.
- **Physiological recognition:** Facial recognition is the second most common type of authentication, according to Spiceworks, in place at 14 percent of companies. Other image-based authentication methods include hand geometry recognition, used by 5 percent of companies, iris or retinal scanning, palm vein recognition, and ear recognition.
- **Voice:** Voice-based digital assistants and telephone-based service portals are already using voice recognition to identify users and authenticate customers. According to Spiceworks, 2 percent of companies use voice recognition for authentication within the enterprise.
- **Signature:** Digital signature scanners are already in widespread use at retail checkouts and in banks and are a good choice for situations where users and customers are already expecting to have to sign their names.
- **DNA:** Today, DNA scans are used primarily in law enforcement to identify suspects -- and in the movies. In practice, DNA sequencing has been too slow for widespread use. This is starting to change. Last year, a \$1,000 scanner hit the market that can do a DNA match in minutes -- and prices are likely to keep dropping.

Behavioral identifiers are a newer approach and are typically being used in conjunction with another method because of lower reliability. However, as technology improves, these behavioral identifiers may increase in prominence. Unlike physical identifiers, which are limited to a certain fixed set of human characteristics, the only limits to behavioral identifiers is the human imagination.

Today, this approach is often used to distinguish between a human and a robot. That can help a company filter out spam or detect attempts to brute-force a login and password. As technology improves, the systems are likely to get better at accurately identifying individuals, but less effective at distinguishing between humans and robots. Here are some common approaches:

- **Typing patterns:** Everybody has a different typing style. The speed at which they type, the length of time it takes to go from one letter to another, the degree of impact on the keyboard.
- **Physical movements:** The way that someone walks is unique to an individual and can be used to authenticate employees in a building, or as a secondary layer of authentication for particularly sensitive locations.
- **Navigation patterns:** Mouse movements and finger movements on trackpads or touch-sensitive screens are unique to individuals and relatively easy to detect with software, no additional hardware required.
- **Engagement patterns:** We all interact with technology in different ways. How we open and use apps, how low we allow our battery to get, the locations and times of day we're most likely to use our devices, the way we navigate websites, how we tilt our phones when we hold them, or even how often we check our social media accounts are all potentially unique behavioral characteristics. These behavior patterns can be used to distinguish people from bots, until the bots get better at imitating humans. And they can also be used in combination with other authentication methods, or, if the technology improves enough, as standalone security measures.[13]

2.8. Related Work

There are many studies and scientific papers in the field of authentication and user authorization of how to request access to systems in this research and we will mention some of them

2.8.1. Techniques for detecting zero day phishing websites

Phishing is a means of obtaining confidential information through fraudulent web sites that appear to be legitimate. There are many phishing detection techniques available, but current practices leave much to be desired. A central problem is that web browsers rely on a black list of known phishing sites, but some phishing sites have a lifespan as short as a few hours. A faster recognition system is needed by the web browser to identify zero day phishing sites which are new phishing sites that have not yet been discovered. This research improves upon techniques used by popular anti-phishing software and introduces a new method of detecting fraudulent web pages using cascading style sheets (CSS). Current phishing detection techniques are examined and a new detection method is implemented and evaluated against hundreds of known phishing sites. [14]

2.8.2. PHISHING WITHIN E-COMMERCE

E-Commerce has been plagued with problems since its inception and this study examines one of these problems: The lack of user trust in E-Commerce created by the risk of phishing. Phishing has grown exponentially together with the expansion of the Internet. This growth and the advancement of technology has not only benefitted honest

Internet users, but has enabled criminals to increase their effectiveness which has caused considerable damage to this budding area of commerce. Moreover, it has negatively impacted both the user and online business in breaking down the trust relationship between them. In an attempt to explore this problem, the following was considered: First, E-Commerce's vulnerability to phishing attacks. By referring to the Common Criteria Security Model, various critical security areas within E-Commerce are identified, as well as the areas of vulnerability and weakness. Second, the methods and techniques used in phishing, such as phishing e-mails, websites and addresses, distributed attacks and redirected attacks, as well as the data that phishers seek to obtain, are examined. Furthermore, the way to reduce the risk of phishing and in turn increase the trust between users and websites is identified. Here the importance of Trust and the Uncertainty Reduction Theory plus the fine balance between trust and control is explored. Finally, the study presents Critical Success Factors that aid in phishing prevention and control, these being: User Authentication, Website Authentication, E-mail Authentication, Data Cryptography, Communication, and Active Risk Mitigation. [15]

2.8.3. Separable Identity-Based Ring Signatures

Email *phishing* attacks are one of today's most common and costly forms of digital identity theft, where an adversary tricks a user into revealing their personal information by impersonating an established company. Such attacks could be mitigated with digitally-signed emails, if these signatures did not:

destroy the traditional repudiability of email, and require the unrealistic, widespread adoption of a Public-Key Infrastructure (PKI).

In order to overcome these obstacles, we introduce, define, and implement separable (a.k.a. crossdomain) identity-based ring signatures (SIBR, pronounced “cyber,” signatures). The ring structure of these signatures provides repudiability. With identity-based public keys, a full PKI is no longer required. Separability allows ring constructions across different identity-based master key domains. Together, these properties make SIBR signatures a practical solution to the email spoofing problem. Our construction yields a number of interesting components. First, we present several novel proofs of knowledge of bilinear map pre-images. We then present new identity-based identification (IBI) and signature (IBS) schemes based on these proofs. We note how our constructions share system

parameters with the existing identity-based encryption schemes of Boneh-Franklin and Waters, thereby forming complete identity-based cryptosystems. We finally construct the first SIBR signature schemes by transforming our new signature schemes and certain other signature schemes. [16]

2.8.4. One-Time Password Authentication

A great quantity of user passwords nowadays has been leaked through security breaches of user accounts. To enhance the security of the Password Authentication Protocol (PAP) in such circumstance, Android app developers often implement a complementary One-Time Password (OTP) authentication by utilizing the short message service (SMS). Unfortunately, SMS is not specially designed as a secure service and thus an SMS One-Time Password is vulnerable to many attacks. To check whether a wide variety of currently used SMS OTP authentication protocols in Android apps are properly implemented, this paper presents an empirical study against them. We first derive a set of rules from

RFC documents as the guide to implement secure SMS OTP authentication protocol. Then we implement an automated analysis system, AUTH-EYE, to check whether a real-world OTP authentication scheme violates any of these rules. Without accessing server source code, AUTH-EYE executes Android apps to trigger the OTP-relevant functionalities and then analyzes the OTP implementations including those proprietary ones. By only analyzing SMS responses, AUTH-EYE is able to assess the conformance of those implementations to our recommended rules and identify the potentially insecure apps. In our empirical study, AUTH-EYE analyzed 3,303 popular Android apps and found that 544 of them adopt SMS OTP authentication. The further analysis of AUTH-EYE demonstrated a far-from-optimistic status: the implementations of 536 (98.5%) out of the 544 apps violate at least one of our defined rules. The results indicate that Android app developers should seriously consider our discussed security rules and violations so as to implement SMS OTP properly.[17]

CHAPTER THREE

METHODOLOGY

3.1 Introduction

A few centuries ago, signature and eventually a wax seal were the only way to certify the authentication of a document. Since that time, and until today, when a signature is apposed to a treaty by a president or to the wedding license by a happy couple, it is assumed that:

- The signature binds the signer to whatever the document states.
- The document will not be changed once the parties have signed it.
- A signature on one document will not be transferred fraudulently to another.

And from here will be the use of digital signature as another tool to make sure the password entered by the user and increase the security of properties of integrity, authentication, and non-repudiation are respected.

3.2 Digital Signature

The digital signature category is the most secure and most full-featured type of signature. It relies on public key cryptography (PKC). Different PKC schemes have been used to implement digital signature and data encryption. For example:

- The RSA (Rivest-Shamir-Adleman) scheme.
- The Digital Signature Algorithm (DSA) scheme.
- The ElGamal scheme.
- The elliptic curve digital signature algorithm (ECDSA) scheme.

When using these schemes to implement digital signature, a pair of mathematically related keys is involved: A private key, and a corresponding public key. Public keys are published and can be stored in

directories. Private keys must be kept secret and only known by the user, and so are usually stored on encrypted portions of a hard drive, on Smart Cards or stored on a network and delivered only after the appropriate password is entered. The algorithms used are asymmetric. This key system obeys to these mathematical properties:

- Encrypting a message with a private key, and then decrypting the result with the corresponding public key, will restore the initial message.
- Given a public key, it is not possible to find out the corresponding private key. .[18]

3.3 Technologies and Requirements

❖ Software Requirements

Application Language :	HTML / CSS / Java Script and PHP
Operating System :	Linux / Windows
Protocols :	HTTP
Web Server :	Apache

❖ Hardware Requirements

Any mobile device which is capable of communicating with GSM networks. Any computer which have an Intel p4 or above processor, minimum server configuration of 512 MB RAM and 10 GB free hard disk space. Web server capable of uploading PHP Scripts.

3.4 Data Flow Diagram

Login Online Banking System

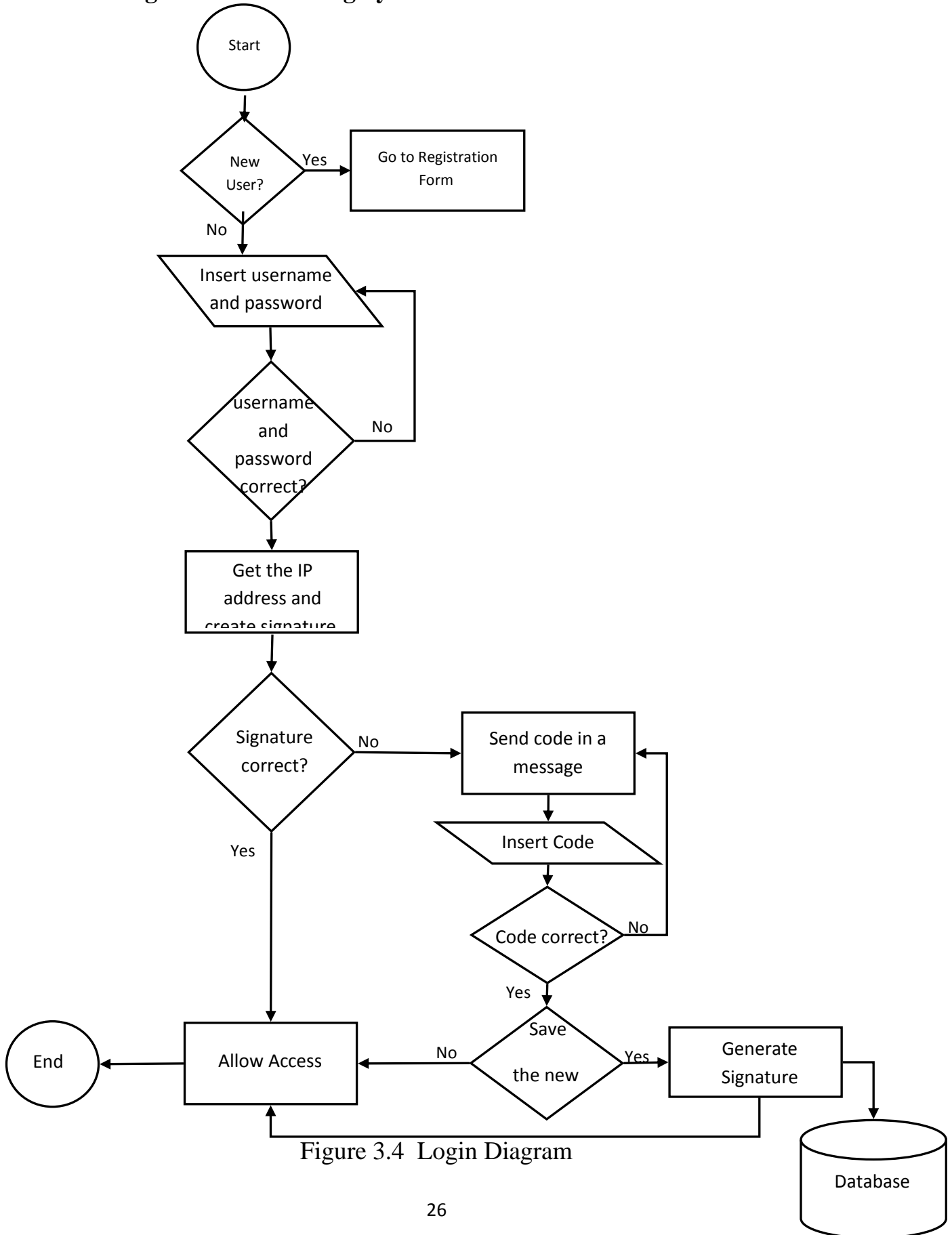


Figure 3.4 Login Diagram

CHAPTER FOUR

SYSTEM DESIGN AND IMPLEMENTATION

4.1 ActiveXperts SMS and MMS component 5.1

SMS and MMS ActiveX/COM component for Microsoft Windows platforms. Send and receive SMS messages via a GSM/GPRS modem (incl. WaveCom, MultiTech, Siemens, Motorola, Falcom Samba), HTTP-POST provider, SMPP provider or TAP/UCP provider. Send and receive MMS messages via MM1 (GPRS), MM4 (SMTP) or MM7 (XML/SOAP). Features: delivery reports, Unicode, multi-part, ringtones, pictures, WAP bookmarks, WAP push, Flash and many more advanced features. Samples included ASP, ASP.NET, Visual Basic .NET, CShare C# .NET, Visual Basic, C++, ColdFusion, Java, Delphi, PHP, HTML, VBScript and more. Runs on any Windows platform, including Windows 2008 x86/x64 Windows 2003 x86/x64, Windows 2000, Windows 7 x86/x64[19]

4.2 Programming Process

Below are the steps to be followed to demonstrate two way mobile authentication systems:

1. Create a project flow design.
2. Design good looking and attracting web pages and site flow with Hypertext markup language (HTML) .
3. Decide the database structure to store the registered user's contact, log-in and account details.
4. Develop the code needful to navigate the application dynamically.

5. Integrate the axmstool HTTP/HTTPS API to our system to send the code
6. Test the application to locate and remove any bugs.
7. Compile the tested application and deploy the files in the server.

4.3 Programming Maintenance:

Apart from the bugs, we have to maintain the program we created. Program Maintenance is a term used for the updating of a program after the program is put into use. This updating may be a result of the users request or a change in the way the program needs to operate.

4.4 Implementation

4.4.1 index.php

This is the home page of the site and includes links to home, login, new user sign up, help.

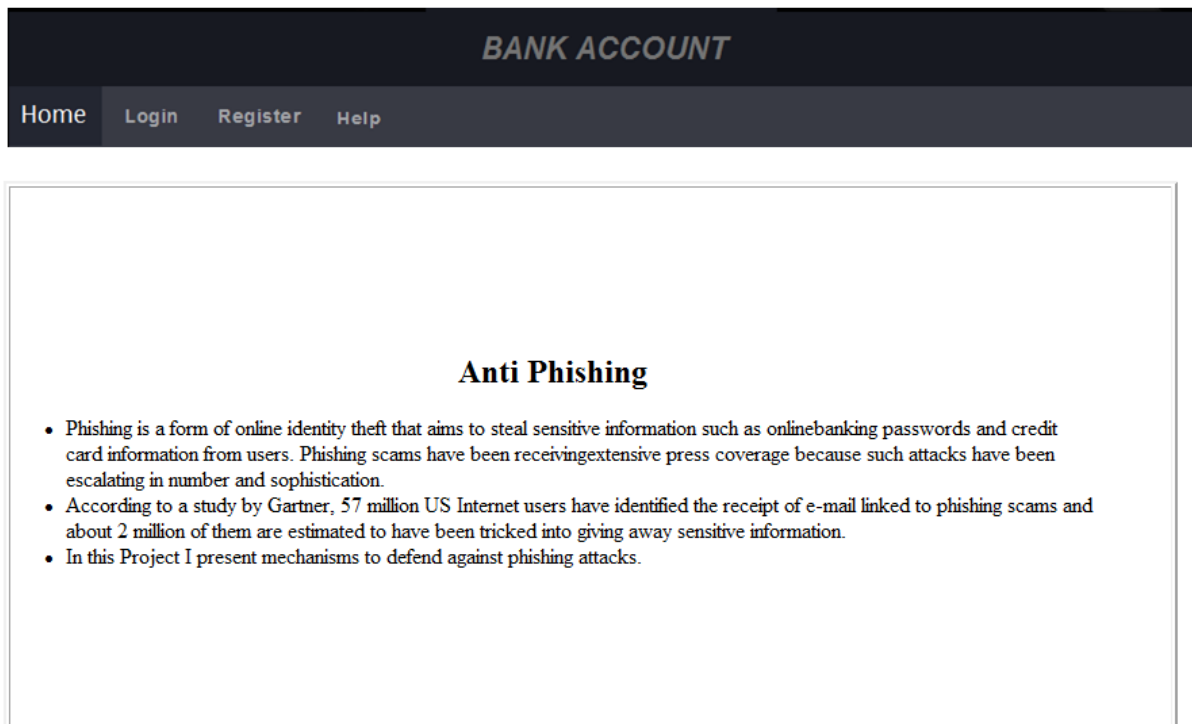


Figure 4.1. Home Page

4.4.2 Register.html

This is the registration page of a new user to the bank, where the user enters his login and contact details. This program performs basic client side (HTML). On submitting this page will redirect to regform.php

The image shows a web browser window with a dark header bar. The header bar contains the text "BANK ACCOUNT" in a light, italicized font. Below the header bar is a navigation menu with four items: "Home", "Login", "Register", and "Help". The "Register" item is highlighted. Below the navigation menu is a registration form titled "Register Form". The form contains seven input fields, each with a label to its left: "First Name", "Last Name", "User Name", "Password", "Confirt", "Email", and "Phone". At the bottom of the form are two buttons: "Send" and "Reset".

Figure 4.2 Register Page

4.4.3 Regform.php

This page checks whether the username submitted in register.html already exists in the database, if exists then, it will again redirect to register.php throwing an error —username already exist, please try another one...and if does not exist, It will perform the following steps:

1. Inserts a new user login details in user_login table namely, username and password. The user_id is an auto incremented field and increments its value by 1.
2. Based on the last inserted user_id in user_login table, it will insert a digital signature of the user.
3. Displays the login form and on submitting this form will redirect to login_home.php

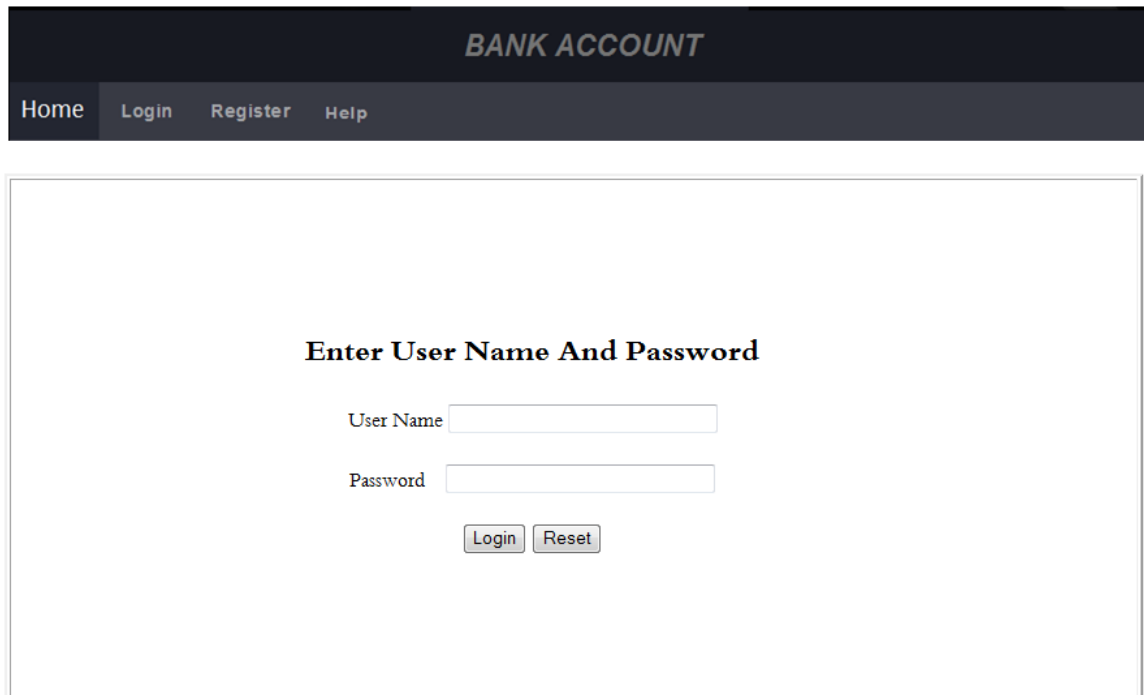
4.4.4 Login_home.php

It checks the whether the posted login details are valid or not. If they are invalid then, it redirects to index.php throwing an error message —invalid username / password

Else if valid then, it performs the following steps:

1. Connects to the database and fetch the username and password submitted and stores in a session variable and get ip address and Then integration of the password and user name and address of the computer and encrypted (generate DS) It checks the whether the generate login details are valid or not if valid then allow to go to index page else we will be go step 2
2. Creates code user function reound number and stores it in a session variable.
3. Retrieves the contact number of the user, based on the user_id from the table user_details.

4. Creates a query string to send an SMS based on smstool API procedure and sends an SMS to the contact number retrieved.
5. After sending the SMS it will redirect the page to `authenticate_password.php`



BANK ACCOUNT

Home Login Register Help

Enter User Name And Password

User Name

Password

Login Reset

Figure 4.3 Login Page

4.4.5 System Test and Result

Testing Objectives In light of the diversity of existing software testing, It is advantageous to consider the types of tests as they become available to a designer. This will also help identify the scope of a particular test and clarify its main advantages and disadvantages as well as make the developer aware about the limitations of this test.

Functional Tests are used to exercise the code with nominal inputs (input values) for which the expected values are available. We also know the boundary conditions for these inputs. For instance, functional testing of matrix multiplication can involve some data (matrices) for which the results are known in advance.

Security Tests are utilized in order to determine the widely defined performance of the software system such as an execution time associated with various parts of the code, response time(in case of embedded systems),and device utilization. The intent of this type of testing is to identify weak points of a software system and quantifying its shortcomings, leading to further improvements.

We performed lot of tests to this application some of the test case are as follows.

Cases :-

1. To ensure correct username and password.

Expected Results	It should be login when provided the correct username and password and generate digital signature the page should be redirected to another page access should be denied if they are wrong or allow to access if they are truee
Prerequisite	The user should have a valid username and password.
Steps	<ul style="list-style-type: none">• Enter the correct username and password in the fields provided.• Click on the login button• Perform the above steps above with entering wrong username and correct password and correct username and wrong password
Results	<ul style="list-style-type: none">• When provided the correct username and password the page gets generate digital signature .• When provided the correct username and wrong password or wrong username and correct password, the access is denied asking to enter the correct username and password.

Table. 5.1

2. To check whether the code number is delivered to mobile phone and when entered it redirects to transaction page

Expected Results	After a successful login the page should be redirect to a transaction page.
Prerequisite	The user should have a mobile phone registered with the username and password.
Steps	<ul style="list-style-type: none">• Check for a field asking to enter a code number• Wait for a code number sent to your mobile and enter the code number into the field.• Follow the above steps and enter a random code number.
Results	<ul style="list-style-type: none">• The page is redirected to a transaction page when entered the correct code number sent to a mobile phone.• The page displays an error message stating that the login is failed.

Table. 5.2

Chapter Five

Conclusion And Future Work

5.1 Conclusion

The goal of this research is to look at the study and implementation of authentication more than traditional password and user name method. And it was the first step of analysis, where we studied the traditional authentication systems, and how caught by and after the piece you design a system to solve the problems and the weakness of the user name and password authentication method. In this thesis new methods is designed based a program (ON LINE BANK) using PHP languages and the use of MD5 encryption algorithm, And AXMSTOOL to send the code via SMS to user If you do not match the digital signature.

5.2 Future Work:

Should be more in-depth the topic of significance, make interfaces more appealing to the user, and its application to real systems operate on the ground, in order to achieve ratification and integration for users, and can make several choices for authentication of the bather in the regulations in order to choose which is best for him.

Reference

- [1] https://www.libertybank.com/wp-content/uploads/2020/12/SANS-What_is_phishing.pdf .
- [2] <https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack>
- [3] Istam Uktamovich Shadmanov “A Survey on Security Services and Mechanisms in Distributed Systems“
- [4]http://www.idconline.com/technical_references/pdfs/data_communications/Security_Services.pdf
- [5] Nilesh A. Lal, Salendra Prasad, Mohammed Farik “ 15.A-Review-Of-Authentication-Methods “
- [6] Noman Ranak¹, Saiful Azad¹, Safwan Fathi Bin Mohammad “An Analysis on Vulnerabilities of Password Retrying “
- [7] <https://economictimes.indiatimes.com/definition/cryptography>
- [8] Wasim Munir “ Independent Study Report – Cryptography “
- [9] Rockey Killer , “Anti-Phishing (2-way Authentication System)”
- [10] <https://expertinsights.com/insights/what-are-the-3-types-of-multi-factor-authentication/>
- [11] <https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/#gref>

[12] Priteshwar Nath Sallam, Jitendra Agrawal “A New Approach 160-bit Message Digest Algorithm“

[13] <https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html>

[14] Michael Blasi “Techniques for detecting zero day phishing websites “

[15] Gregory M. Megaw” PHISHING WITHIN E-COMMERCE“

[16] Michael Blasi “Techniques for detecting zero day phishing websites“

[17] Surya Nepal, Diethelm “An Empirical Study of SMS One-Time Password Authentication in Android Apps “

[18] Chafic Maroun Rouhana Moussa “Digital Signature and Multiple Signature”

[19] <https://activexperts-sms-and-mms-component.soft112.com>