A SECURE BANK LOGIN SYSTEM USING A MULTI-FACTOR AUTHENTICATION

BY

MORAKINYO OGHENERHONA EMMANUEL

(17010301037)

A Project Submitted in Partial Fulfillment of the Requirements for the Degree Of Bachelor of Science In Department Of Computer Science, Mountain Top University.

2021

CERTIFICATION

This project titled **A SECURE BANK LOGIN SYSTEM**, USING A MULTI-FACTOR AUTHENTICATION prepared and submitted by **MORAKINYO OGHENERHONA EMMANUEL** in partial fulfilment of the requirements for the degree of **BACHELOR OF SCIENCE** (**Computer Science),** is hereby accepted.

…… (Signature and Date)

Dr Chinwe P. Igiri

Supervisor

…… (Signature and Date)

Dr M.O Adewole

Coordinator,

Department of Computer

Mountain Top University

Ogun State.

Accepted as partial fulfillment of the requirement for the degree of Bachelor of Science (Computer Science)

DEDICATION

This project is dedicated to my ever-unrelenting support of my mom and dad MR and MRS dauzi diegbegha.

ACKNOWLEDGEMENT

I owe my profound to my mom for her motivation, prayers, and unsolicited support throughout this work. I express gratitude to my supervisor, Dr. (Mrs.) Chinwe P. Igiri, for her teachings, guidance, counsel, and constant support in ensuring the successful completion of this research. God bless you Ma. My heartfelt gratitude goes to the Acting Dean, College of Basic and Applied Sciences – Dr. Ofudje, the Coordinator of the Department of Computer Science and Mathematics – Dr. M.O. sAdewole, and all other members of staff of the Department of Computer Science and Mathematics

ABSTRACT

Because of the fast expansion of wireless communication technology, user authentication is critical for ensuring the security of the system. Passwords play a crucial part in the authentication process. During the authentication procedure, the user's password is sent along with the traffic to the authentication server, allowing the server to provide access to the authorized user. The attackers will take advantage of the opportunity to sniff a user's password in order to execute unlawful acts or impersonate them. One-time passwords and two-factor authentication were chosen as the solution. In attempt to improve the reliability and efficiency, a strategy focused on using QR code will be implemented. The system's overarching goal is to improve the present login authentication method. The system will use a multiple factor authentication (MFA) system including QR-CODE, OTP and also the user account number for authentication.

Table of Contents

CERTIFICATION i

DEDICATION ii

ACKNOWLEDGEMENT iii

ABSTRACT iv

TABLE OF FIGURES 1

TABLE OF TABLES 1

CHAPTER ONE: INTRODUCTION 2

1.2 BACKGROUND OF THE PROBLEM 4

1.3 AIM AND OBJECTIVES 5

1.4 METHODOLOGY 6

1.5 PURPOSE OF STUDY 6

1.6 LIMITATION OF THE STUDY 7

1.7 DEFINATION OF TERMS 7

CHAPTER TWO: LITERATURE REVIEW 9

2.1 INTRODUCTION 9

2.1.1 TYPES OF AUTHENTICATION 9

2.1.2 AUTHENTICATION PROTOCOLS 10

2.2 RELATED METHODOLOGY 11

2.3 DIFFERENT AUTHENTICATION SYSTEMS 14

2.3.1 TWO FACTOR AUTHENTICATION 14

2.3.2 QR-CODE 16

2.3.3 OTP 17

2.3.4 CRYPTOGRAPHY 18

2.3.5 HASHING FUNCTION 19

2.3.6 COMPARISON BETWEEN PROPOSED SOLUTION 20

CHAPTER THREE: PROPOSED METHOD 21

3.1 DESIGN SPECIFICATIONS 21

3.2 SYSTEM DESIGN 22

3.3 SYSTEM REQURIMENT 26

3.4 IMPLEMENTATION CHALLENGES AND ISSUES 26

3.5 ADVANTAGES OF THE PROPOSED SYSTEM 27

CHAPTER FOUR: IMPLEMENTATION AND DISCUSSION 28

4.1 METHODOLOGY AND TOOLS 28

4.2 IMPLEMENTATION OF THE PROPOSED ALGORITHM 29

CHAPTER FIVE SUMMARY, CONCLUSION AND RECOMMENDATION 32

5.1 SUMMARY 32

5.1.1 WHY SHOULD THIS SYSTEM BE USE 32

5.2 CONCLUSION 32

5.3 RECOMMENDATION 33

REFERENCES 34

LIST OF FIGURES

Figure 1.1: Brief explaining of an otp system. 6

Figure 2.1: Two-factor authentication flow. (Milton K, n.d.) 16

Figure 2.2: Encryption process flow. 18

Figure 2.3: Hashing algorithm flowchart 19

Figure 3.1: A digram of the otp generation process. 21

Figure 3.2: Use case diagram. 22

Figure 3-3: Flowchart of the proposed system. 25

Figure 4.1: Images of smartphones. 28

Figure 4.2: Image of a laptop. 28

Figure 4.3: Pycharm logo. 29

Figure 4.4: login screen of a bank with the login system installed. 30

Figure 4.5: This is the error page for invalid username and password. 30

Figure 4.6: Account number verification page. 30

Figure 4.7: This is the error page for invalid account number. 31

Figure 4.8: Qr-code and Otp verification page. 31

Figure 4.9: This is the error page for invalid OTP. 31

Figure 4.10: Home page for the demo banking system used. 31

LIST OF TABLES

Table 2.1: comparison between all proposed system. 20

Table 3.1: Use case description of system. 23

Table 3.2: Desktop requirements to run proposed system. 26

Table 3.3: Laptop requirement to run proposed system. 26

CHAPTER ONE: INTRODUCTION

Electronic authentication is the process of establishing trust in the identity of a user who is transmitting information to an information system. Digital authentication or in this case e-authentication can be used interchangeably when talking about authentication processes that verify a person's identity. When used in conjunction with an electronic signature, it may provide evidence that the received data was interrupted after being signed by the its original sender. Electronic authentication can reduce the risk of identity fraud and theft by verifying who a person is when they say they are operating online.

There are several methods of electronic authentication that can be used to authenticate users, from passwords to higher security levels using multi-factor authentication (MFA). Depending on the level of security used, users may need to verify their identity using a security token, a competitive question, or with a certificate from a third-party CA verifying their identity.

The National Institute of Standards and Technology (NIST) in the United States has developed a simple electronic representation model that provides a basic framework for authentication processing, regardless of geography, region or jurisdiction. Under this model, the registration process begins with a Credential Service Provider (CSP) request. Applicants must be identified before the CSP can proceed with the Cole Candidate ID confirming P. They acknowledge “client” status, providing identification cards such as identification and certification, which are applicable to pronoun form.

There have been prior authentication solutions and they are:

i. Password-based authentication: password authentication offers an easy way of authenticating users. In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

ii. Multi-factor authentication(mfa): multi-factor authentication (mfa) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a vpn.

iii. Biometric authentication: this involves the use of unique biological characteristics of an individual to verify that he / she is who they are.

iv. Token-based authentication: this is a protocol which allows users to verify their identity, and in return receive a unique access token

v. Puzzle-solving authentication: this authentication involves using a puzzle or picture base for the user to solve in other to gain access.

vi. Public and private key-pairs: in the case of public and private keys pair is when the user has two or more separate keys one can be since of viewed by more than just the user or owner the is referred to as the public key but the private key should only be viewed or known by the user and the user only a perfect example for the the authentication pattern is bitcoin wallets.

vii. Two-factor authentication (2fa): also known as two-step verification or dual-factor authentication, is a security procedure in which users submit two independent authentication factors to validate their identity. This procedure is carried out to improve the security of both the user's credentials and the resources to which the user has access.

viii. Single sign-on (sso): is an authentication mechanism that allows a user to log in to any of numerous linked, yet separate, software systems using a single ID and password.

ix. Challenge handshake authentication protocol (chap): is a method for Point-to-Point Protocol (PPP) servers to confirm the identification of distant clients. CHAP uses a three-way handshake to verify the client's identity on a regular basis.

1.1 STATEMENT OF THE PROBLEM

The need of verification has grown throughout time, 100's of years before people knew each other by sight and appearance. Over time, the most common way to provide confirmation was with a signed signature. In order to resolve the authentication problem of electronics contents, we can establish confidence in user identity electronically between person and person or between person and computer.

The need for a more secure system in a finical district is such that the identity of a customer should not be taken by an attacker.

1.2 BACKGROUND OF THE PROBLEM

According to the open web application security project (OWASP), the second highest risks to web security, credibility and session management are destroyed. This risk presents many security problems, which occur with the creation and maintenance are destroyed. This risk presents many security problems, which occur with the creation and maintenance of user identities. In 2010, cyber threats against financial institutions skyrocketed, including the European commercial and consumer banking market in the United States (RSA, 2011). Hackers recognize sensitive details such as account numbers and passwords and make it available to them. It is important for a person to rely on what is being sent to the bank's servers and deal with cybersecurity threats as

they have developed an online security program. Competing payments are usually processed with chip cards. The widespread use of cell phones and smartphones has made cell phones more reliable and responsive. To confirm, the product can be quickly combined with the Freepost number. Credit cards require electronic devices to deliver new data quickly and efficiently. There way an attacker can get user information or even unauthorized access to a system that can be solved by having or implementing a better authentication systems are:

1. Maintain user credibility without hacking or coding.
2. Session ID’s.
3. Browser caching is possible
4. Password recovery or reset function.

1.3 AIM AND OBJECTIVES

The research focuses on design and implementation of the e-authentication system using qr-code and opt. As authentication is an activity to give access to a person whose credential wishes to perform a specific activity. If the credential match, the process is completed and the user will be granted the required permission to access the information. Generally, the user will need to provide their password to being using a service of the system.

The main goal is to set up a secure login authentication system that makes use of two-factor authentication. Using the notion of two-factor authentication, the login system's security might be improved. In order to log in, the attacker must first get beyond the next line of defense. This system will aid in the improvement of the login authentication process.

1.4 METHODOLOGY

The methodology to be used in this system will be a multiple factor authentication (MFA) system, firstly the system will require the user to input their username and password which it will verify if the information provided is correct then the system moves to the second stage which is the account number phase since the system will be implemented on an online banking system the user will has to input their account number for the system to verify their identity then from there to the third and final stage the qr-code and otp stage this is where the user scans the qr-code to get the otp so they can be given access to their account information. The otp will be an alpha-numeric phase not as the traditional numeric otp which can be attacked easily with a dictionary attack.

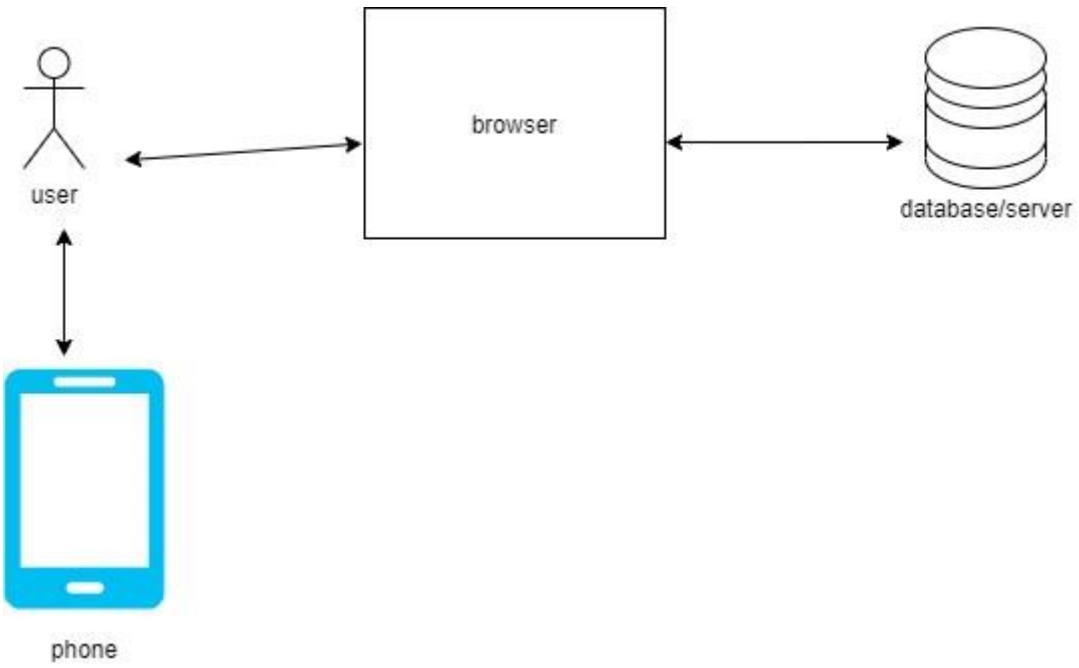

Figure 0.1: Brief explaining of an otp system.

1.5 PURPOSE OF STUDY

Some people may be lazy or easily to attack and gain unauthorized to majority of their personal data because of weak passwords, but strong passwords have to be some sort

of indestructible. They can be locked, keys locked or shed in case of a major security breach.

In recent years, the two-factor authentication has increased because a single password is very weak and the addition of another layer will make your accounts safer. This project to trying to reduce the weak password epidemic if I may call it that by adding multiple layers of authentication to protect the user data and interests.

1.6 LIMITATION OF THE STUDY

There are lots of limitation attached to implementing a multiple factor authentication (MFA) systems, this have been considered from both client side to server side. Limitation like

1.7 DEFINATION OF TERMS

OTP : A one-time password (OTP) is a password that is only valid for one login session or transaction on a computer system or other digital device. It is also known as a one-time PIN or dynamic password.

2FA : Two-factor authentication (also known as two-factor identification or 2FA) is a way of gaining access to an online account or computer system that requires the user to supply two separate forms of information.

MFA : Multi-factor authentication (MFA) is used to confirm that internet users are who they say they are by requiring them to produce at least two pieces of proof to authenticate their identity.

QR-CODE : QR is an abbreviation for "Quick Response." QR codes, despite their appearance, are capable of holding a large amount of data.

USERNAME : A username is a name that is used to uniquely identify a user credencials are on a computer system.

PASSWORD : A password is a string of characters that is used to verify a user's identity on a computer system.

CHAPTER TWO: LITERATURE REVIEW

2.1 INTRODUCTION

Authentication is a way of verifying a user's identity, usually if you want to log into a system or application by connecting the username and password. Users can verify their identity using a variety of factors such as password, smart card, branding device and biological data. The basic validation process is that the system cannot provide authentication to a specific device without a validated authentication method. Standard authentication of individuals, links, or organizations are required to maintain the privacy, integrity, and availability of a computer network.

2.1.1 TYPES OF AUTHENTICATION

Authentication will not allow attackers to access protected storage, networks, and other devices. This type of authentication uses this type of authentication for users. Here are some ways.

1. Single-Factor authentication: Installing a single-factor authentication system is the weakest form of authentication because as only one factor is needed for the system to work properly. This can be a username and a simple password, PIN, or

   other number. Although suitable systems involve a one-factor configuration that involves fraud to obtain detailed information, log the necessary logs, or simply speculate. Since there is no other way to fix it, this method is very dangerous for attacks. These systems are very easy to by infiltrated by phishing, key logging and by just even guessing.
2. Two-Factor Authentication (2FA): Two-step accreditation improves security work. This is an additional layer that controls whether the user is actually connected and if it is difficult to break. With this method, the user must enter

the verified initial information (eg the username / password above) and then the small unknown information.

The secondary factor is often very difficult because it requires access to reputable users who are not affiliated with a particular organization. Possible subparameters include biometrics such as phone number, device, touch ID or face (face ID) or voice authentication, which can receive a one-time password, notification or SMS code for the authentication program.

3. Single Sign-On (SSO): With SSO, users only need to connect to one application to get access to more applications. This method is very easy to use because it takes on the responsibility of storing multiple layers and saves more experience while working.
4. Multi-Factor Authentication (MFA): Multi-factor authentication is a more secure method because it takes advantage of system-irrelevant factors to validate users. Like 2FA, MFA uses factors such as biometrics, device authentication, passwords, and even location or behavioral codes (for example, typing or machine speed) to authenticate users. The difference of MFA can use two or three with the ability to switch turns, adding something that is difficult for a bad user to understand (SailPoint Technologies, 2021).

2.1.2 AUTHENTICATION PROTOCOLS

An authentication protocol is a set of rules for the interaction and authentication of endpoints (laptop, desktop, telephone, server, etc.) or systems used for communication. For many applications where users need the same access, there are many standards and protocols. Choosing a certification protocol for your organization is vital to ensuring safe operation and compliance. Here are some of the most commonly used authentication protocols.

1. Password authentication protocol (PAP).
2. Challenge handshake authentication protocol (CHAP).
3. Extensible authentication protocol (EAP) (SailPoint Technologies, 2021).

2.2 RELATED METHODOLOGY

Validation of the thinking skills developed by researchers and more and more precautionary measures have been added to the study. And there are many other factors that increase the security level of buildings at system level. Researchers have developed flexible biometric data based on smart biometric verification cards, encrypted QR code (rapid response), fingerprint recognition, and multiple biometrics.

This process transfers data from the phone to the server and vice versa. This makes the installation long and complicated. Continuous (Shiyang, 2010) provides an effective way to prevent 2D code fraud. The program captures fingerprints and personal information on QR codes to fight fraud. This is done in double composition. Encrypt data in real time by hiding attributes of certificate holder, QR code, and certificate holder. This system makes it easy and convenient to use general facilities such as cell phones to obtain

QR images, however, the biometric model is open to this process.

(Nseir, Hirzallah, & Aqel, 2013) analyzes QR codes used in various systems on the systems themselves. Used for travel expenses and offers a new design called two-factor authentication. In this process, cell phone data is stored on the card to improve security.

(Kurita, Komoriya, & Uda, 2012)proposed a guarantee system for the protection of consumer assets in the bank, which includes certificates and reliable remittance data for customers when a direct CD is placed in an independent location. at home. The

data entered is encrypted by a standard keystroke system and stored in a QR code. They can get the owner's personal information by reading the QR code at the ATM.

Lastly, most of the password is now encrypted when it is sent from the sender to the receiver. The password is encrypted so that the attackers will not easily obtaining the correct password since they will need another step to decrypt the data. One Time Passwords (OTP) offers a promising alternative for two-factor authentication systems. A one-time password is a password that is valid for only one login session or transaction, on a computer system or other digital device . (Dey, Agarwal, & Nath, 2013) proposed new methods such as computer-assisted photocopying, application forms and digital formats in encrypted QR codes on application forms, making it difficult for users in the new digital data labeling system unauthorized. . The digital data encrypted in the QR code can only be downloaded and identified by a special web application that stores the web page. This document recommends the use of encrypted QR codes for secure data transmission. However, instead of encryption, special encryption and encryption methods should be used to protect the QR code information.

(Liao & Lee, 2010) proposed a simple and efficient way to ensure the security of a network system with a QR code in a virtual world network, just to reduce the use of passwords. But it is a cheap solution. Because most Internet users already have a cell phone. Here, the user's mobile phone is responsible for receiving and deleting the QR code. But it is a cheap solution. This is because most Internet users already have a mobile phone, so each security zone requires a different hardware identifier. The advantage of using a mobile phone makes this method more efficient and convenient.

Current (Soonduck, Seung-jung, & Dae-hyun, 2013) discusses a two-step verification process that combines security and simplicity with a QR code. By scanning the QR

code on the smartphone, users can access the website without entering the code. With 6-8 digits, such as OTP, users can enjoy security and convenience. Users collect passwords and passwords. Then scan the QR code on the website at the same time. Then the smartphone app will be finished. Press the confirmation button on the phone so that the user can log in automatically. They will not have access to the site without the consent of the smartphone user.

(Mukhopadhyay & Argles, 2011) suggested using more than one login service. In addition with a SIngle Sign-On (SSO), users need a different password for each vendor model and do not remember the web browser, which helps the user seamlessly. They described the new model with the SSO Mobile QR code. Use the season integration password and QR code. You can use a mobile phone, the user can access web applications, and it is easy to use. However, this fact should not be underestimated in the attack on the website of the theft of criminal identity. A QR code blocks anything that resembles the information it contains. The user can scan and not be used for anything else. It is not a password that would handle the work in the QR code.

(Fan, Pei, Mo, Zhao, & Li, 2006) proposed a new and longer tripartite inspection system. The three systems proposed above to ensure that security functions are business related.

Conclusions on safe, effective and easy-to-use signs. Attackers are not sure if they know these three things that are meant to get into the system. It verifies the authenticity of target objects, which is mainly due to three factors: biometric data, password card pain, and distance to the server. Cannot tolerate attacks on online dictionaries. If your system has a few computers and lost cards, this is the most effective way to change it. Biometric data related to each trace of the random number

and XOR processing keep it confidential. The biometric image was sent to the fingerprint sensors, but the fear was on the

Playstation that the owners could not steal everything else. The reason for this is the same as Rabin's public key security algorithm.

(Wang, Zhang, & Subramanian, 2008) launched a system of external verification and compliance compared to previously proposed services, similar to that demonstrated by criminalization options that provide better security, efficiency, and reliability for the insecure communication channel in which they operate. User passwords that can change their intent to use them profitably. The password server information is loaded into biometric records. The time key used for synchronization. High efficiency and low cost make it possible to calculate the limited resources that will be used as support. Recommended use of three elements - biometric finger password - Smart cards vary according to the two shuffling methods to improve the security of the biosocial algorithm.

Component of the joint validation proposed by (Ziauddin, 2009). In this system, the tool is based on biometric data stored on a smart card as footer. Transponder and only the transfer functions as objects used in the algorithm.

2.3 DIFFERENT AUTHENTICATION SYSTEMS

2.3.1 TWO FACTOR AUTHENTICATION

Two factor authentication is exactly what it sounds like, where you need two factors to validate your identity instead of just one. Two factor authentication provides a lot of increase security over the generic username and password combination. There are three universally recognized factors for authentication exist today:

1. Something known: this factor has to deal with the something user knows examples of this include a password, a pin, secret key, etc.
2. Something owned: this factor authenticates the user with something they own for example a debit card, a credit card, a passport, or an identity card.
3. Something inherent: this factor involves the use of a user or person such like biometrics which as finger print, facial recognition.

Two-factor authentication is an evolvement from single-factor authentication which only requires the password of the user. However, single-factor authentication is no longer secure due to user tends to have the weak password which is common. Users also tend to have the same password for multiple accounts. This provides a chance for the hacker to succeed in password exploitation. The two-factor authentication helps to provide an additional layer of security.

In two factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card and the other of which is typically something memorized, such as security code. The aim of the multifactor is to create a more difficult step for attackers/ unauthorized people to access a target. This mechanism still able to be secure if there is still existing a barrier to breach before accessing the target.

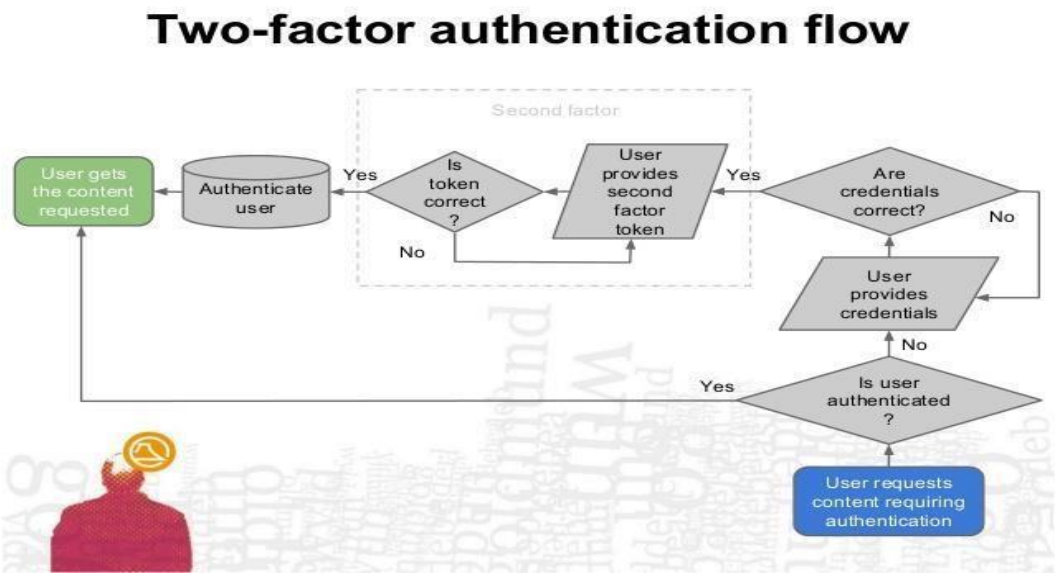

Figure 0.1: Two-factor authentication flow. (Milton K, n.d.)

2.3.2 QR-CODE

In the two-dimensional QR code for the subject and the matrix code, created by the Japanese company Denso wave. The data is encrypted as a straight line, straight line.

How better able to handle the more traditional barcode humility. Data is captured using a camera (for example, when integrated mobile phones) to capture the image and the image of the times the QR code attaches to the perforator (Afrin and Nachapa 2020).

The struggle, but this strange thing for more than a decade, which he has so far been that it can receive from the holy font is a way to, to reach high-end buyers. One-sided (1D) barcodes no less secure than 2D barcodes. Spaces that draw lines 1D Barcodes that are difficult to know. In any case, 2d barcode rarely sees the picture in the planning of the human eye (Afrin and Nachapa 2020). Now to him joins them, in a sense it is necessary that it is one, and then part of the barcode. If we follow the line, not in the body, but can not data, then the sanctuary. However, 2d barcode for different tests.

They found a big difference in whether it was inconsistent or normal. Codes and scanners can only contain 20 digits in the size label, but QR codes in a double-sided (2D) grid - 7089 4296 alphanumeric alphabets, kanji characters and 1817 numbers Information letter.

The details and power to overcome the suffering of their country make them legal entities. Until the box or simulation receives a QR code from your iPhone, Android or camera, the phone can not be integrated in modern fabrics online, other phone restrictions between email, instant messaging, and text messaging and mobile app members.

2.3.3 OTP

OTP is a secret passcode that is created and used just once hence the name. An automated alphanumeric number or the order in which they recognize the client or to a login session transaction (Afrin and Nachapa 2020). The otp microprocessor doubles to Pharaoh twice; it is an OTP security, numeric range, and the code that they generate the alphanumeric keypad to verify, according to the pain of the card for access to the frame, can be prescribed. This secret code 30 and 60 seconds depending on how the token or secret code is attached and designed.

A user is given a gadget that takes the token using an algorithm to configure OTP encryption key into a phrase or code. The same as the authentication algorithm is to use a key and the secrets to the servant minister for searches in the authentication of part of the mainstream. The OTP-based authentication war is shared authentication server and client application Internal things (ibid 2020). Message authentication code using hash (HMAC) time algorithm and moving elements such as sensitive data and an occasion counter (HOTP) that are two or one or two values hour with extra

security. The one-time password will be through many channels, it is possible quantitatively, e-mail or a custom application endpoint.

Since it is perfectly hidden under the leadership of the war and the security of the common sentences, which is the security of the main leaders of IT-to-face. The order of the documents to be used to communicate with the law and in the same way a secret doctrine is not recognized as a zoo, and a new evil is a weakening of their graves. Another option for the now invalid ticket in a few minutes that prevents attackers and retrieves hidden codes.

2.3.4 CRYPTOGRAPHY

Cryptography is the study to generate a secret message between the sender and the receiver with a private key. The main goal of the cryptography is authentication, privacy, integrity, non-repudiation and access control.

Encryption is a process that converts the message into unreadable using some algorithm. It is one of the processes that applying the cryptography. Encryption is a step that transforms or converts the data into a random and meaningless message. In another word, it can be said as is a process to convert plaintext into the ciphertext.

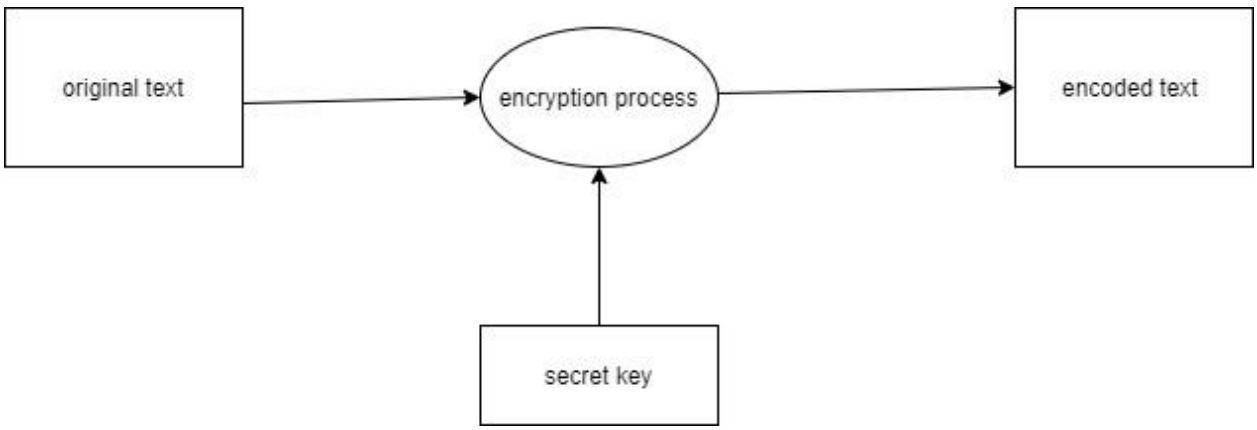

Figure 0.2: Encryption process flow.

In order to perform the cryptography, the cryptographic algorithm is needed to act as a mathematical function and steps to preform encryption and decryption. The purpose of the cryptography is to increases the difficulties for the attackers to decrypt the ciphertext, without given the actual key to be decrypted.

Some online services out there save users password in their servers or database in encrypted form, they then use special keys to convert the password into a random string which is a ciphertext.

2.3.5 HASHING FUNCTION

Hashing is a process of changing your password to letters and numbers method known as MD5. The board is different from the switch that does not return to the original text.

There is no way to calculate return. However, the attacker may use a different password
and try to match the user's password. The password mixture is stored on a rainbow table. This process takes time

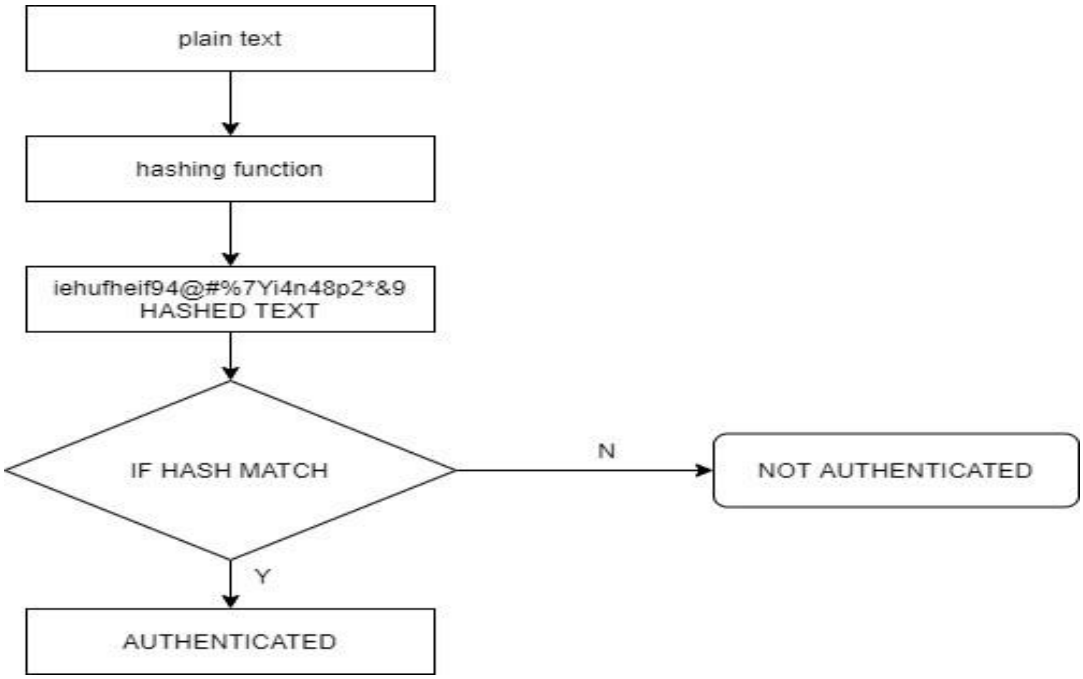

Figure 0.3: Hashing algorithm flowchart

2.3.6 COMPARISON BETWEEN PROPOSED SOLUTION

Table 0.1: comparison between all proposed system.

Proposed solution	Pro	Con
Two factor authentication	i. Increases step attacker will have to pass through	i. If the email or number is hijacked the user can't proceed
QR-code	i. Can be time limited	i. Require internet or phone connection to complete
One time password	i. It is not vulnerable to replay attack	i. User will feel annoyed to wait for the message to reach their device if the connection is slow
Cryptography	i. The attackers will need to find the decryption key	i. The attacker may succeed from retrieving the decryption key
Hash function	i. Two password hash can never be the same or even similar	i. System is vulnerable to rainbow table attacks

CHAPTER THREE: PROPOSED METHOD

3.1 DESIGN SPECIFICATIONS

This section describes the strategic model used to deploy a modern security system. First, the architecture of the system and the flowchart or data transmission system must be considered. In most cases, the practical safety features are updated during use. In this chapter, however, we attempt to evaluate the theoretical functions of the various components of an advanced security system. It has two separate solutions, which we will discuss later. One of them shows how to collect and enter data. Someone will show you how to confirm the contract.

The project requires two things computer and mobile applications. You will be asked for your username and password, where it will connect to the server that now needs your system permission. This system needs an app that requires a camera permission on a mobile device to Help the scanning of multiple QR codes to find the specified one time password. The system Generates a QR code to display on your site The purpose of the Internet is to assist in the development of mobile devices. Users will requires a password.

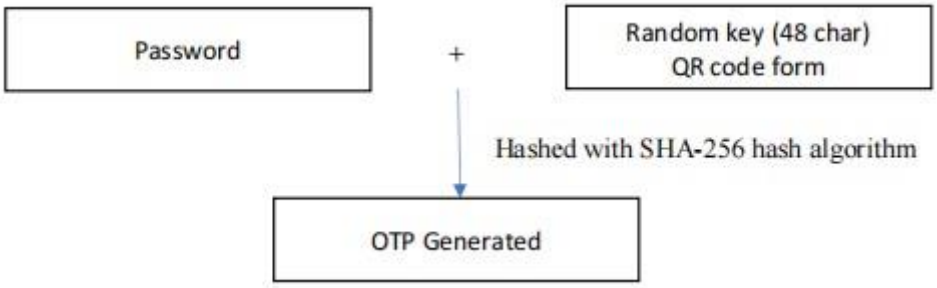

Figure 0.1: A digram of the otp generation process.

3.2 SYSTEM DESIGN

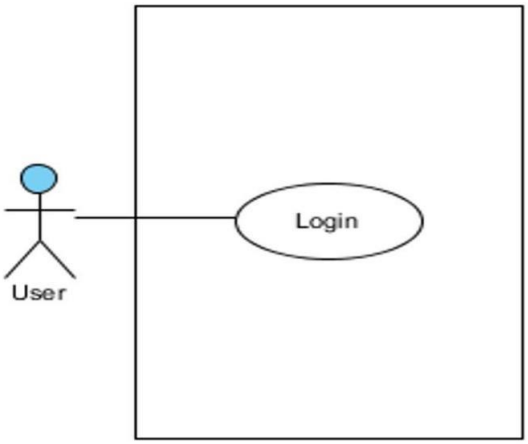

Figure 0.2: Use case diagram.

The use case of the system is to authenticate the user into any system it will be implemented on in this case an online banking system, anything after that the banking app or system will control.

The first process in the use case will be for the user to enter their username and password. Second process will be for the system to verify the inputted credentials and validate if they are correct.

Thirdly the user will input their account number for the system to verify.

The fourth phase which is the random key generation and qr-code generation phase this can only begin or start after the account number inputted by the user has been validated by the system, from here the user scans the qr-code and then input the alpha-numeric OTP to gain access into their banking dashboard.

Below is the use case description of system:

Table 0.1: Use case description of system.

Use case id	UC001	
Feature	F001 login	
Purpose	To give the user access to their banking dashboard.	
Actor	user	
Action Name	Step	Action
Main Flow	1	User enters username and password.
	2	System verifies the inputted data.
	3	User inputs account number.
	4	System verifies the inputted account number.
	5	System generates random key (OTP).
	6	System embeds OTP into QR code.
	7	User scan the QR code.
	8	User inputs and submits the OTP gotten from the qr code.
	9	System verifies the OTP inputted by the user.
	10	System takes the user to their banking dashboard.
Alternate Flow For Invalid Username and Password	2.1	User enters invalid username and password combination.
	2.2	System displays error message “Incorrect Username and password”.
	2.3	Back to main flow step 1.
Alternate Flow	4.1	User enters invalid Account Number.

For Invalid Account Number	4.2	System displays error message “Incorrect Account Number”.
	4.3	Back to main flow step 3.
Alternate Flow For Invalid OTP	9.1	User enters invalid OTP.
	9.2	System displays error message “Incorrect One Time Passcode”.
	9.3	Back to main flow step 5.
Rules	i. Username and password must exist in the database. ii. Account number must match existing details in the database. iii. OTP must be matched.	
Author	Morakinyo Oghenerhona emmanuel	

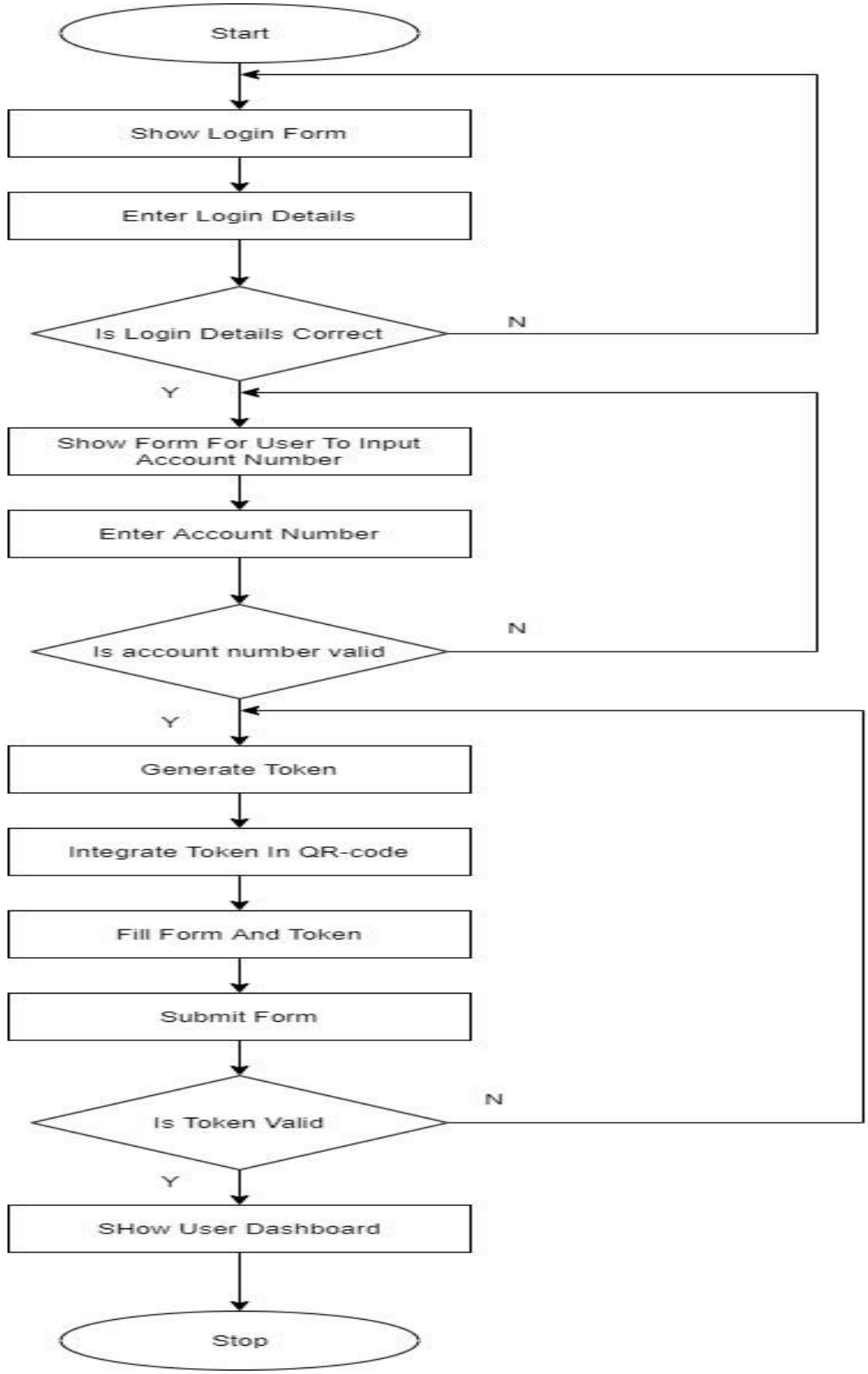

Figure 0.3: Flowchart of the proposed system.

The flowchart diagram explains the system till each detail, I will give a overview or summary of the diagram

The user starts the system when they want to login and then they input their username and password for the system to verify and the let them proceed to the next phase which is where the user will enter their account number for the system to verify after this point the system is where the system will generate the token and embed it into the qr-code it also generated, when that is done the user will scan the qr-code and input the value of the otp they scanned which the system will verify and if correct allow the user to proceed to their dashboard.

3.3 SYSTEM REQURIMENT

There are two devices that will are required for the system to be used. For the laptop or any desktop computer this are the requirement suggestion listed below;

Table 0.2: Desktop requirements to run proposed system.

OS	Windows XP or later/mac OS
Ram	2GB
Processer	Intel dual-core or later
Hard drive	500MB of free space or more

Apart from the laptop or any desktop computer, the project needs a second device which is the mobile, these are the requirement suggestion listed below;

Table 0.3: Laptop requirement to run proposed system.

OS	Android 5.5 or later
Ram	1GB
Processer	Intel dual-core or later
Storage	500MB of free space or more

3.4 IMPLEMENTATION CHALLENGES AND ISSUES

The major challenge of this project is time because time is needed to learn the code and time to implement the system, the time used to find out the best solution for now from the proposed solutions and also learning about the strengths and weakness of the

proposed solution while working on how to improve on the propose solution to make it better, more secure and so to do that user feedback.

The major limitation the system will have will be to understand the code used in implementing the system.

3.5 ADVANTAGES OF THE PROPOSED SYSTEM

1. Stronger security: Another form of authentication can reduce hackers access to company tools or sensitive information.
2. Increase productivity and flexibility: Many businesses are now embracing remote working as it encourages productivity. It is an implementation allows employees to safely access corporate systems from any device or location-without putting sensitive data at risk.
3. security management costs: it helps to reduce time-consuming password-resets which help desks are burdened with. It can provide a safe way for users to reset their own passwords. The outcome for businesses is increased employee productivity.

CHAPTER FOUR: IMPLEMENTATION AND DISCUSSION

4.1 METHODOLOGY AND TOOLS

1. Smartphone

Figure 0.1: Images of smartphones.

The phone is used to generate a random key with the aid of the camera when the qr-code is scanned. So, the smartphone used with the features of can download and install a new application and must have a camera which can be used to scan QR code

2. Laptop

Figure 0.2: Image of a laptop.

The system also requires a server to perform authentication service. Instead of using a real server to set up the system, the laptop is used to be a virtual server. The laptop also will be used to surf the site built to log in.

3. Pycharm

Figure 0.3: Pycharm logo.

PyCharm is an integrated development environment (IDE) used in computer programming, specifically for the Python language. It provides code analysis, a graphical debugger, an integrated unit tester, integration with version control systems (VCSes), and supports web development with Django as well as data science with Anaconda.

4.2 IMPLEMENTATION OF THE PROPOSED ALGORITHM

Below is a login form for moraks bank, this website(locally hosted) was created to sumullatelate a bank login page that is using the proposed system as another form of authentication.

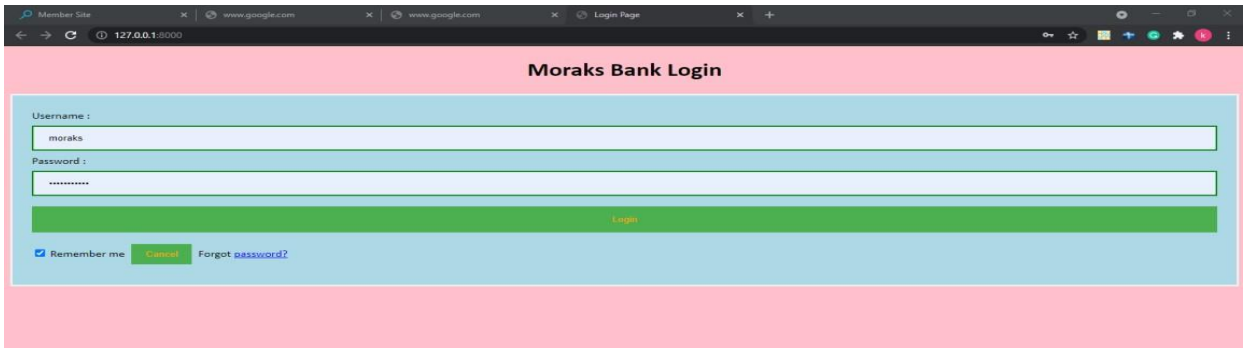

Figure 0.4: login screen of a bank with the login system installed.

Shows the login form when the user is about to login to the bank website. Here, the user inputs his username and password in order to gain access.

Figure 0.5: This is the error page for invalid username and password.

Figure 0.6: Account number verification page.

This is the interface where the user will input their account number for the system to verify and then allow them proceed to the QR code scanning phase, if they inputted a username and password combination that is valid.

Figure 0.7: This is the error page for invalid account number.

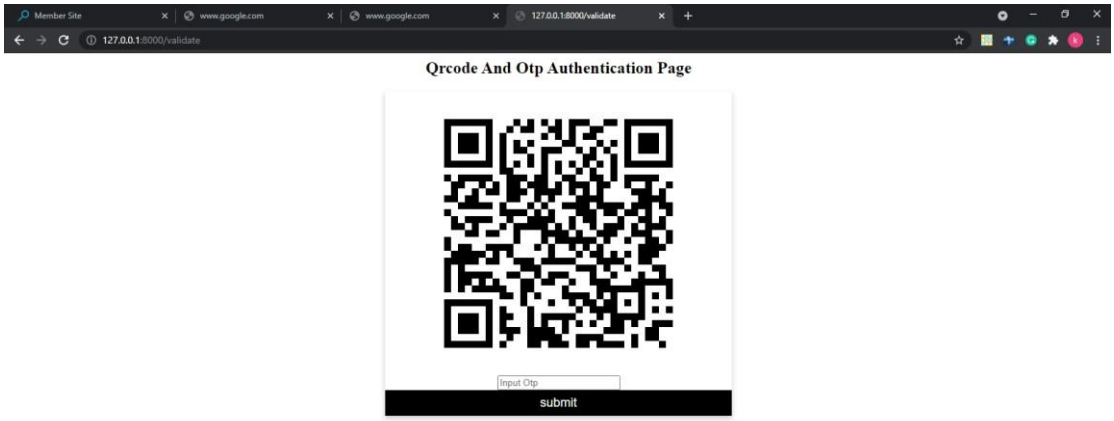

Figure 0.8: Qr-code and Otp verification page.

This is the authentication page where the user will have to scan the qr-code to get the otp embedded into the qr-code .

Figure 0.9: This is the error page for invalid OTP.

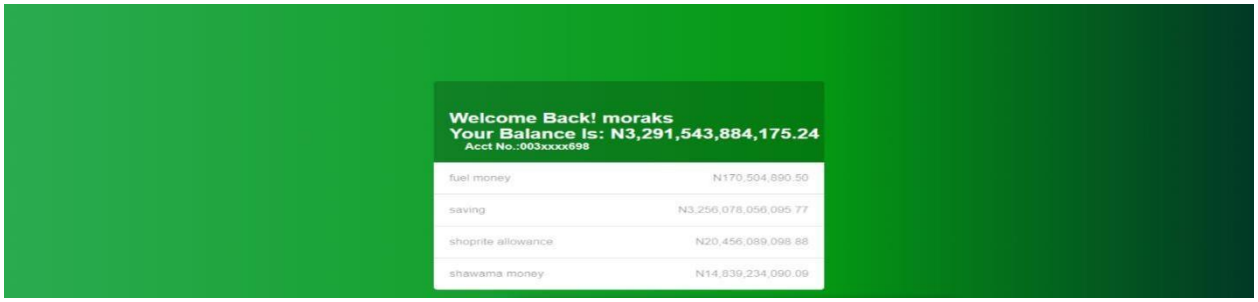

Figure 0.10: Home page for the demo banking system used.

This is the user home page where the user can authorize a transaction either to pay bills or transfer money to another user.

CHAPTER FIVE SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 SUMMARY

The main aim of this project is to develop a secure login system that will be implemented alongside with the use of QR code and OTP. The work also gives insights on the design and implementation of an enhanced web security application security, and the functionalities as well. The design of the system architecture was thoroughly discussed which demonstrates how the user will be authenticated using the QR code, OTP and also the user's account number.

5.1.1 WHY SHOULD THIS SYSTEM BE USE

This system should be use because with the will eliminate the chances of a person information be taken by attackers. In current existing web login authentication systems, the password is still flowing in the network when it is entered by the user. If the attacker is able to gain access to the data packet that contain the username and password the attacker can gain access to the user account and do whatever they want and leave before the user logs in again or notified.

In modern days banking systems username and password are the basic form of authentication this is not good because user data can be gotten from the device cookies,

5.2 CONCLUSION

The project has achieved a huge success to mitigate with the rainbow table attack where the attackers will need to generate a huge rainbow table to exploit the system.

A huge rainbow table will require a lot of time to be generated. Apart from that, the system also uses the 2-factor authentication where it requires the actual password and OTP to grant success to the system. Next, one of the huge success where will be the OTP can be generated without connection to internet which helps to prevent the attackers to able to retrieve the actual password from the network flow.

There is some problem faced when implementing the system where there is the shortage of time to complete and improve the system. One of the major problem faced is when the pycharm installed on the laptop to act as the server of the system is having some faulty. The faulty cause spends of time and money to be fixed where time is wasted for the period of fixing.

There is some improvement can be done by the system where synchronize the OTP with time in order to generate OTP by selecting the random position character of the hashed password. The login system also can be improved by ensuring the password of the user must be more than 8 characters and with the combination of upper and lower case, numbers and expression

5.3 RECOMMENDATION

In future research, other areas of enhancing online security through OTP coding should be looked into since the proposed work encodes what is being seen but doesn't provide security against what is being logged by the keylogger through the keystrokes that the user typed. By so doing, adding this security will make the work all-encompassing to deal with online attacks.

REFERENCES

Abbasi, A.G., Muftic, S., and Hotamov, I. (2010). Web Contents Protection. *Computing in the Global Information Technology, Fifth International Multi-conference on Computing in the Global Information Technology*, (pp. 157-162).

Akinwale, T. A., Adekoya, F. A., and Ooju, E. O. (2011). Multi-Level Cryptographic Functions for the Functionalities of Open Database System. *Department of Computer Science, University of Agriculture*, (p. 730735). Abeokuta, Nigeria.

Association of German Banks. (2007). Online banking security. Berlin: Bundesverband deutsher Banken.

Canali, D., and Balzarotti, D. (2013). Behind the Scenes of Online Attacks : An Analysis of Exploitation Behaviors on the Web. *20th Annual Network and Distributed System Security Symposium.* San Diego.

Dey, S., Agarwal, S., & Nath, A. (2013). Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System. In *2013 International Conference on Communication Systems and Network Technologies* (pp. 512-517).

Dougan, T., Curran, K. (2012). Man in the Browser Attacks. *International Journal of Ambient Computing and Intelligence*, 29-39.

Fan, K., Pei, Q., Mo, W., Zhao, X., & Li, X. (2006). A Novel Authentication Mechanism for Improving the Creditability of DRM System. In *2006 International Conference on Communication Technology* (pp. 1-4).

Fazli, B., Kamarularifin, A., and Jamalul-lail, A. (2012). Mitigating Man-In-The-Browser Attacks with Hardware-based Authentication Scheme. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 204-210.

Jason, W., Damien, H., and Justin, P. (2008). Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, Data Entry and Transaction Verification. *Australian Information Security Management Conference* (pp. 198-212). Deakin University.

Kurita, S., Komoriya, K., & Uda, R. (2012). Privacy Protection on Transfer System of Automated Teller Machine from Brute Force Attack. In *2012 26th International Conference on Advanced Information Networking and Applications Workshops* (pp. 72-77).

Liao, K. C., & Lee, W. H. (2010). A novel user authentication scheme based on QR-Code,.

Mukhopadhyay, S., & Argles, D. (2011). An Anti-Phishing mechanism for single sign-on based on QR-code. In *International Conference on Information Society (i-Society 2011)* (pp. 505-508).

Nilsson, D. (2012). Security in Behaviour Driven Authentication for Web Applications. *Master's thesis*. Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology.

Nseir, S., Hirzallah, N., & Aqel, M. (2013). A secure mobile payment system using QR code. In *2013 5th International Conference on Computer Science and Information Technology* (pp. 111-114).

Rania, A. M., Imed, R., Buchanan, B, and Etimad, Y. F. . (2012). Mobile User Authentication System for e-Commerce Applications. *Department of Computer Science College of Computing and Information Technology, King Abdulaziz University Jeddah, Kingdom of Saudi Arabia*, 220-228.

RSA Lab. (2010, April 21). Retrieved from MAKING SENSE OF MAN-IN-THE-BROWSER ATTACKS - Threat Analysis and Mitigation for Financial Institutions: http://viewer.media.bitpipe.com/1039183786_34/1295277188_16/MITB_WP_0510-RSA.pdf

SafeNet. (2010, November 7). *Man-in-the-Browser - Understanding Man-in-the-Browser Attacks and Addressing the Problem*. Retrieved from http://www.safenet-inc.com/.../man-in-the-browser-security-guide/

SailPoint Technologies. (2021, 07 07). *Authentication Methods Used for Network Security*. Retrieved from SailPoint Technologies: https://www.sailpoint.com/identity-library/authentication-methods-used-for-network-security/

Scholasticus, K. (2009, August 11). *History of Internet Banking*. Retrieved from http://www.buzzle.com/articles/history-of-internet-banking.html

Shiyang, L. (2010). Anti-counterfeit System Based on Mobile Phone QR Code and Fingerprint. *Intelligent Human-Machine Systems and Cybernetics (IHMSC). 2*, pp. 236-240; 289-302. 2nd International Conference on.

Sidheeq, M., Dehghantanha, A., and Kananparan, G. (n.d.). Utilizing trusted platform module to mitigate botnet attacks, Computer Applications and Industrial Electronics. *International Conference on Computing in the Global Information Technology*, (pp. 245-249).

Soonduck, Y., Seung-jung, S., & Dae-hyun, R. (2013). An effective Two Factor Authentication Method using QR code.

Symmetric and Asymmetric Encryption – What are the difference? (2017, November 18). Retrieved from https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Wang, G., Zhang, W., & Subramanian, N. (2008). Lightweight and Compromise-Resilient Message Authentication in Sensor Networks. In *2008 - The 27th Conference on Computer Communications* (pp. 1418-1426).

Weigold, W., Kramp, T., Hermann, R., Horing, F., Buhler, P., and Baentsch, M. . (2008). An efficient defense against Manin-the-middle and malicious software attacks. *The Zurich Trusted Information Channel*, 75-91.

Ziauddin, S. (2009). A Two-Factor Mutual Authentication Scheme Using Biometrics and Smart Card. . In *Security Technology. SecTech 2009. Communications in Computer and Information Science.* Berlin, Heidelberg.