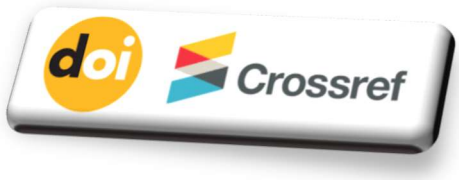
Journal, Advances in Mathematical & Computational Sciences
Vol. 9 No. 2, 2021
www.mathematics-computationaljournal.info



Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA

Available online at https://www.isteams.net/ mathematics-computationaljournal.info
DOI: dx.doi.org/10.22624/AIMS/MATHS/V9N2P1
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

Network Security Based On Two-Factor Authentication System

Sarumi, J.A. (PhD)
Department of Computer Science
Lagos State Polytechnic
Ikorodu, Lagos Nigeria
E-mails: jerrytechnologies@yahoo.co.uk; sarumi.j@mylaspotech.edu.ng
Phone: +2348023408122

ABSTRACT

The paper examined the network security based on a two-factor authentication login system using OTP with SMS. The quest for the application of tighter security measures to web, desktop and mobile applications developed has been a major concern to a lot of people. Faced with the challenges of poor security and vulnerability of users, resulting to applications being hacked by unauthorized people, this research delved into developing a more secured login application that sends a secret pass code to the registered phone number of a user for identification purpose. The aim of the application is basically to ensure that users are safe, and all logins are authorized. The application was developed with PHP, MYSQL, CSS, BOOTSTRAP, HTML technologies and WAMP Server.

Keywords: Geno-generative, database, sensor, swarm, Top-k

Sarumi, J.A. (2021): Network Security Based On Two-Factor Authentication System.
Journal of Advances in Mathematical & Computational Science. Vol. 9, No. 2. Pp 1-14. DOI: dx.doi.org/10.22624/AIMS/MATHS/V9N2P1
Available online at www.isteams.net/mathematics-computationaljournal.

1. INTRODUCTION

Security is a major concern today in all sectors such as banks, governmental applications, military organization, educational institutions, etc. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. With the development of science and technology and means of storage and exchange of information in different ways, or so-called transfer of data across the network from one site to another site, several proper strategies for using passwords have been proposed. Some of which are very difficult to use and others might not meet the company's security concerns. Some solutions have been developed to eliminate the need for users to create and manage passwords.

A typical solution is based on giving the user a hardware token that generates one-time-passwords, i.e. passwords for single session or transaction usage. Moreover, token also have disadvantages which include the cost of purchasing, issuing, and managing the tokens or cards. From the customer's point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards which are likely to get lost or stolen. So this project work is aimed at introducing the provision of OTP with SMS in Web application.

In addition to the procedures adopted to prevent access of information into the hands of unauthorized persons through communications and to ensure the authenticity of these communications. Today security concerns are on the ascent in all areas. Most systems today rely on static passwords to verify the user's identity, store them on their system or asking the websites for remembering their password etc. Utilization of static passwords in this expanded dependence on access to IT systems progressively presents themselves to Hackers, ID Thieves and Fraudsters. In addition, hackers have the preference of using numerous techniques / attacks such as guessing attack, shoulder surfing attack, dictionary attack, brute force attack, snooping attack, social engineering attack etc. to steal passwords so as to gain access to their login accounts. Quite a few techniques, strategies for using passwords have been proposed but some of which are especially not easy to use and practice. To solve the password problem in banking sectors and for online transaction two factor authentications using OTP and SMS have been implemented.

1.1 Study background

The information and communication technology improves significant impact in all areas of daily life, in the management of our personal lives and interaction with others or in the management of institutions and activities dealing with customers. Because of the rapid development of information technology and the growth in exchange for increasing the number of gaps security threats are discovered, the need to secure information and keep abreast of this development is an optimal goal, the strategy seeks to achieve by the advanced international institutions that deal with information technology. Knowing that, and in under difficult economic circumstances, a lot of work organizations around the world have sought to increase their investment in the development of information and personnel security technologies, so as to believe in the representation of the foundation stone for the construction of its information secure system.

Password

Password is a set of secret characters or words utilized to gain access to a computer, web page, network resource, or data. Passwords help ensure that computers or data can only be accessed by those who have been granted the right to view or access them (Stein,2016).

One Time Password (OTP)

A One-Time Password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. An OTP is more secure than a fixed password, especially a user-created password, which might get prone to attacks after a certain period. OTPs may replace authentication login information or may be used in addition to it, to add another layer of security. OTP is password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs can either be time synchronized or be based on mathematical algorithms, time synchronized OTPs being the more famous type. A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and, through text-to-speech conversion, to any mobile or landline telephone, text messaging has a great potential to reach all consumers with a low total cost to implement (Kavya, 2015).

Cryptography
Discipline or techniques employed in protecting integrity or secrecy of electronic messages by converting them into unreadable (cipher text) form. Only the use of a secret key can convert the cipher text back into human readable (clear text) form. Cryptography software and/or hardware devices use mathematical formulas (algorithms) to change text from one form to another (Beal, 2016).

Encryption and Decryption
Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text). Decryption is the process of converting cipher text back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of cipher text, the key that was used to encrypt the data must be used. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of cipher text without possessing the key. It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks (Marumari, 2016).

Data Encryption Standard (DES)
The Data Encryption Standard (DES) is an outdated symmetric-key method of data encryption. DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. Once the go-to, symmetric-key algorithm for the encryption of electronic data, DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm. Originally designed by researchers at IBM in the early 1970s, DES was adopted by the U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data. It was the first encryption algorithm approved by the U.S. government for public disclosure (Rouse, 2016).

Triple Data Encryption Standard Algorithm
Triple data encryption standard (DES) is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte (Supriya, 2013).

Advanced Encryption Standard
The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. The origins of AES date back to 1997 when the National Institute of Standards and Technology (NIST) replaced aging Data Encryption Standard (DES) which vulnerable to brute-force attacks (Rouse, 2016).

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Logically, authentication precedes authorization (although they may often seem to be combined). The two terms are often used synonymously but they are two different processes (Rouse, 2017).

Two Factor Authentication

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

1. Something You Know (Such As A Password)
2. Something You Have (Such As A Smart Card)
3. Something You Are (Such As A Fingerprint Or Other Biometric Method)

Using a Two Factor Authentication, process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email, because the criminal would need more than just the users name and password details (Bradley, 2017).

1.2 Aims of the Study

This research is aimed at providing a two-factor authentication system for clients using mobile device to access financial services through web pages or mobile applications. The outcome will ensure the following:

1. Provides a cost effective and user-friendly authentication.
2. Avoids the use of a simple username and password system, which is not secure anymore.
3. No additional use of hardware.

1.3 Significance of the Study

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

1. First factor is just usual password that every one creates while registering or creating an account.
2. The second factor is the one time password, that we generate using some secured functions and sent through SMS gate way to the customer's registered mobile number.
3. This authentication method will be implemented using a simple bank application.
4. The authentication of a user happens in two steps and by the user providing the system with two passwords. One password is the general password that he/she has to enter every time a user wants to login. The second password is the One Time Password (OTP) that we generate in our application and send it to the end user via SMS on his mobile phone which must be typed in, for the user to be granted access to the system.

2. RELATED WORKS

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

- The first related work by NilayYlldmm, AsafVarol (AsafVarol, 2015). They proposed Android Based Mobile Application Development for Web Login Authentication Using Fingerprint Recognition Feature; this study uses the Samsung Galaxy S5 fingerprint recognition feature and IMEI number to generate single time passwords. Within a limited timeframe, the secure passwords can be used to sign in/log in to online user accounts related to government, banking and education. The Android based Web Login Authentication application has been developed to use the mobile biometric feature login processes. The main purpose of the program is to produce a single use, time constrained password by fingerprint authentication that will be used along with user name and password for login to the related web site. The application consists of two parts. The first part is the web side and the second part is the Android application side, which generates the password. Initially, the user is presented with the login screen application and choose login with fingerprint option, if user not register; user can choose register finger print option. After the fingerprint verification step, the IMEI number will be queried in the database of the web site. Thus, the user can be exposed to two conditions:

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

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

- The second related work by Mete Eminagaoglu, EceCini, GizemSert, and DeryaZor (Mete et al, 2015) they proposed two factor authentication systems with QR codes for web and mobile application. This study has been implemented by developing a two factor identity verification system where the second factor is the user's mobile phone device and a pseudo randomly generation alphanumerical QR code which is used as the one-time password token sent to the user via e-mail or MMS. The study use username and password mechanism for the first authentication step and the system generate QR code as one-time password as second authentication step. The user verifies himself to the system by scanning QR code to the web camera manually. In the beginning the user enters username and password to the authentication server, if entry data correct; the system must send QR code automatically to user via of one the selective options; MMS or E-mail then the system checking, verifying and validating QR code. If the user displays the QR code's image to the web camera properly; the data encoded in the QR image is automatically sent to the server application and checking for verification and validation. If the scanned QR image by the camera is the correct QR code, then the second stage of the authentication process is finalized and the user is automatically directed to the authorized page in the application. If the scanned QR image by the camera is not verified by the server; the authentication process automatically fails and a warning message is displayed where the user is automatically

directed to the first login page. The system records the last date and time of the last successful /unsuccessful user entry. The system store QR code up to five minute, after that QR code will be deleted. Password is store in database encrypted with AES Symmetric encryption. The login began the user fill username and password if correct QR code one-time password send to mobile phone or E-mail and then scan it to web camera to verify. The limitation of this study use QR code that means required QR reader and web camera, then more cost and If the user selects E-mail approach to receive QR code that means internet needed thereby increasing the risk as well as may be delayed to arrive.

- The third related work by Indu S, Sathya T.N, and Saravana Kumar V (Sathya et al, 2015). They proposed Stand Alone and SMS Based Approach for Authentication Using Mobile Phone In this study they develop a complete two factor authentication system using mobile phones. The system using a mobile phone as a software token for One Time Password generation. The OTP valid for a session and for a single use. The system consists of a server connected to a GSM modem and a mobile phone client running a J2ME application. Two modes of operation are available for the users based on their preference and constraints. The first is a stand-alone approach that is easy to use, secure, and cheap. The second approach is an SMS based approach that is also easy to use and secure, but more expensive. The stand-alone approach generates OTP without connecting the client to the server. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. In case the first approach fails to work, the password is rejected, or the client and server are out of sync, the mobile phone can request the OTP directly from the server without the need to generate the OTP locally on the mobile phone. In order for the server to verify the identity of the user, the mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone. The user will then have a given amount of time to use the OTP before it expires. This approach will require both the client and server to pay for the telecommunication charges of sending the SMS message. Another limitation of this study could be that the SMS may be delay for some minute for arrive to phone that means the OTP may became expire and this study needs telecommunications charges that must be paid for
- The fourth related work by, Ms. E. Kalaikavitha, Mrs. Juliana gnanaselvi (Kalaikavitha et al, 2013). They proposed secure login using encrypted one-time password and mobile based login methodology, in this study they secure login to web server by generating one-time password then encrypt it by advance encryption standard (AES). User no need to enter OTP manually, because of security reasons OTP is encrypted and sends to mobile by electronic mail (Email). User just read the mail for verification and type application password with that encrypted OTP and sends it to the system Web server is used to send mail to user. The limitation of this study use internet to send OTP by Email that means increase vulnerability of hacking and brute force of OTP as well as the Email may be delay because use internet that means the OTP may become expire.

2.1 Types of Existing systems:
There are several systems for dealing with two-way mobile authentication. They may differ in delivering the password to the authorized user or a different entity based on the security constraints. Some of them are as follows;

Tokens
A token is a device used to authorize the user with the services. A token may be software or hardware. Software tokens are used to identify the person electronically, i.e. it may be used as a password to access something. Hardware tokens are small hand held devices which carry the information which stores cryptographic keys, digital signatures or even bio-metric data by which we can send generated key number to a client system. Mostly all the hardware tokens have a display capability. The hardware tokens include a USB, digital pass etc.
Drawbacks

1. A token shall be carried all the time.
2. Special software is required to read the token.
3. Anyone can access the information that has the token i.e. in case of theft.

Biometrics
A biometric authentication is the advanced form of authentication. A biometric authentication is nothing but it scans the user's characteristics such as finger print and eye retina and stores in the form of a string. When the user tries to authenticate it, it matches with the stored data and then gives access when a commonality is achieved and when the user has gained access he can enter the password to view the required information.

Drawbacks

1. Biometric authentication is convenient only for limited applications, since the system becomes very slow for a large number of users.
2. Finger prints can be taken on a small tape and can be provided for the hardware
3. Additional hardware is required to detect the fingerprints and eye retinas.

Mobile ID
Mobile Id offers a strong two-way authentication by authenticating the user to the service and service to the user. The mobile id works is such a way that the user is required to send the code generated by the application after which the Mobile id generates a code to identify the user with the service.

Drawbacks

1. Mobile phones with 2.5 G and third generation only are supported.
2. Software is to be installed into the mobile device.

OTPs versus other methods of securing data:
One-time passwords increase the vulnerability to social engineering. The attacks in which the phishers attempt to find the already used OTPs that they used in the past. Even though OTPs are most secured than the passwords we usually remember. The users of OTP systems are still vulnerable to MIM attacks, the OTPs shouldn't be shared with the others and the use of an OTP in layered security is more safer instead of using the OTP alone; we can achieve layered security by using an OTP in combination with a password that is memorable to the user. The benefits of using layered security is that a single sign-on in combination with one master password is safer than using only one layer of security during the sign-on.

Thus the inconvenience of password fatigue can be avoided if we have long sessions with many passwords that needs to be entered during the mid-session. however, the drawbacks of using different kinds of security during a single sign-on is that one has the problems with security precautions every time they log in even if one is logging into the computer to access data which doesn't need as much security as some other sensible transactions that computer is used for. Two Way Mobile Authentication System is an innovative authentication system that provides access to Web-based resources by using a two-way user authentication through the existing personal mobile phones. It is used to solve the security flaws of the web based Internet and Intranet, by involving the users to authenticate themselves using their personal mobile phones.

The registration of the users has to be done in a secured manner before he can actually use the system. It is designed to provide security to Web-based Internet and Intranet applications, and requires users to authenticate themselves with two unique criterions - a username and password, and a code which they get only during authentication (a one-time password OTP sent to their mobile phone) before they are permitted to access a secured web resource. With 2WMAS, we can positively identify users and deliver services easily and in a most secured way to users, without having the need of an additional security system. End users can have the advantages of a very simple process that omits the need to remember multiple passwords.

3. METHODOLOGY

3.1 System Design and Program Design

Data Capturing
This is the way of producing data in a machine sensible from the source and read directly by a suitable device into the destination. The captured in this proposed system is certifying all stages required in the processing, in other to ensure an authentic information been generated.

Method of Data Collection
We adopted the Interview Method which involves two persons, interviewer and interviewee. The interviewer ask questions from the interviewee and record the answer or response down. The answers given by the interviewee determines the information printed out when inputted into the system.

INPUT FILE DESIGN FOR ONBOARDING A NEW STAFF OR CLIENT

S/N	FIELD NAME	FIELD TYPE	WIDTH
1.	Username	Text	12
2.	Phone number	Number/Text	14
3.	Password	Number/Text	12
4.	Confirm Password	Number/Text	12

INPUT FILE DESIGN FOR EXISTING STAFF OR CLIENT

S/N	FIELD NAME	FIELD TYPE	WIDTH
1.	Username	Text	14
2.	Password	Number/Text	14

3.2 Use Case Diagram

In software engineering, a use case is a list of steps, typically defining interactions between a role (actor) and a system, to achieve a goal. The actor can be a human or an external system. Below is the use case diagram of the network security based on two factor authentication system:

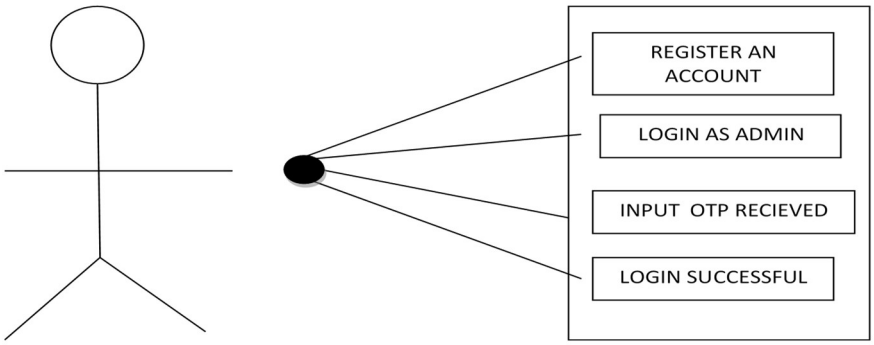


Figure 1: Use-case Diagram

Admin - System Flowchart

The flowchart shows the diagrammed sequence of events that occur during the operation of the system. The flowcharts of the activities of the users of the system are shown below:

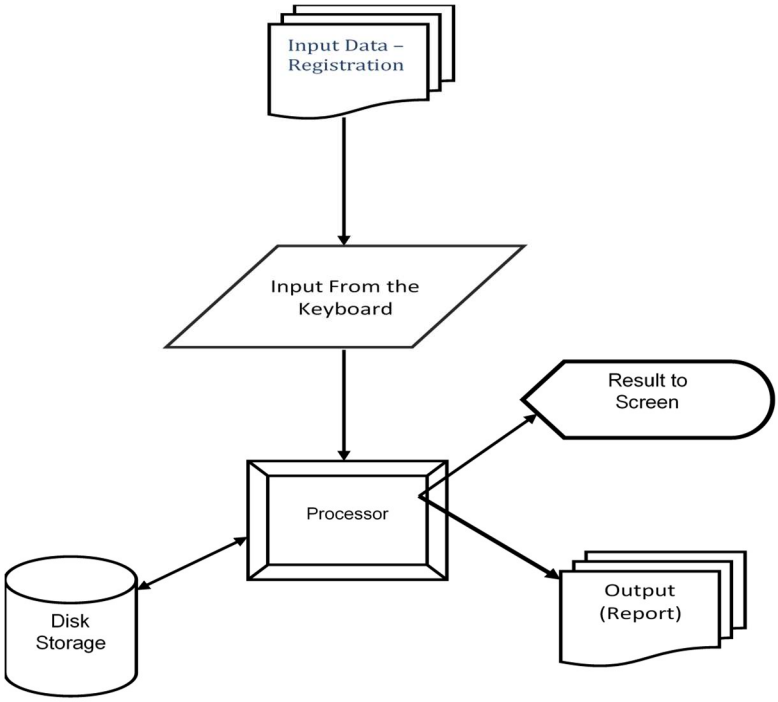


Figure 2: System Flowchart

4. SYSTEM IMPLEMENTATION AND EVALUATION

4.1 Design Implementation

The network security based on two factor authentication system was implemented using various development tools.

Program Logic

The client side application was designed and programmed using Wamp server. The information used on the system was stored in database management application using MYSQL. 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) and Cascading Style sheets (CSS).
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 BULK SMS HTTP/HTTPS API to our system to send SMS (which include the one-time password (OTP) generated by the algorithm)
6. Test the application to locate and remove any bugs.

Implementation Plan

This system will be implemented using a parallel approach plan i.e the new system will run alongside with the old system with a view to strengthening the inadequacies of the old system.

Input Design and Specification

Computer is designed in such a way that sometimes it is called GIGO, denoting that what goes in is what comes out. The input forms are designs generally based on the necessary data that needs to be entered into the system. The data are captured through the keyboard and stored on a magnetic disk in a MySQL database.

Program 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.

Installing The New System

The requirements for the installation of the proposed system are mentioned in the following sections:

Hardware Requirements

The software designed needed the following hardware for an effective operation of the newly designed system.

1. *A system running on AMD, Pentium II or higher processor*
2. The random access memory (ram) should be at least 512mb.
3. Enhanced keyboard.
4. At least 20 GB hard disk.
5. V.G.A or a colored monitor.
6. Any mobile device which is capable of communicating with GSM Networks.

Software Requirements

The software requirements include: -

1. A window 7 or higher version for faster processing.
2. Xamp or Wamp is also needed to be able to open and run the php file in an offline environment.

4.2 System Outputs

What follows are set of outputs from running the system

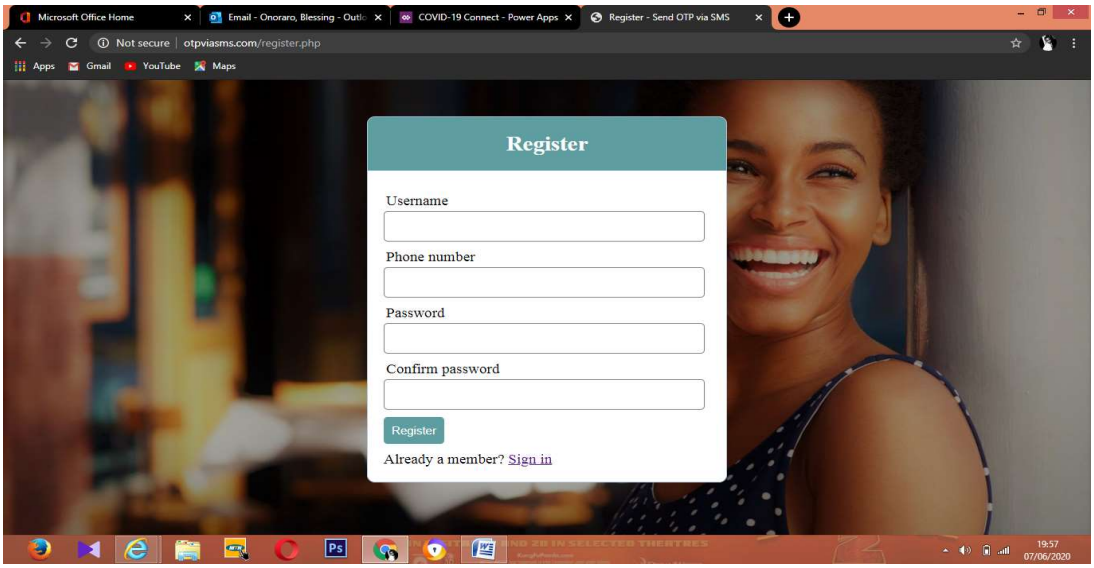


Fig 3: Registration Page for Fresh User

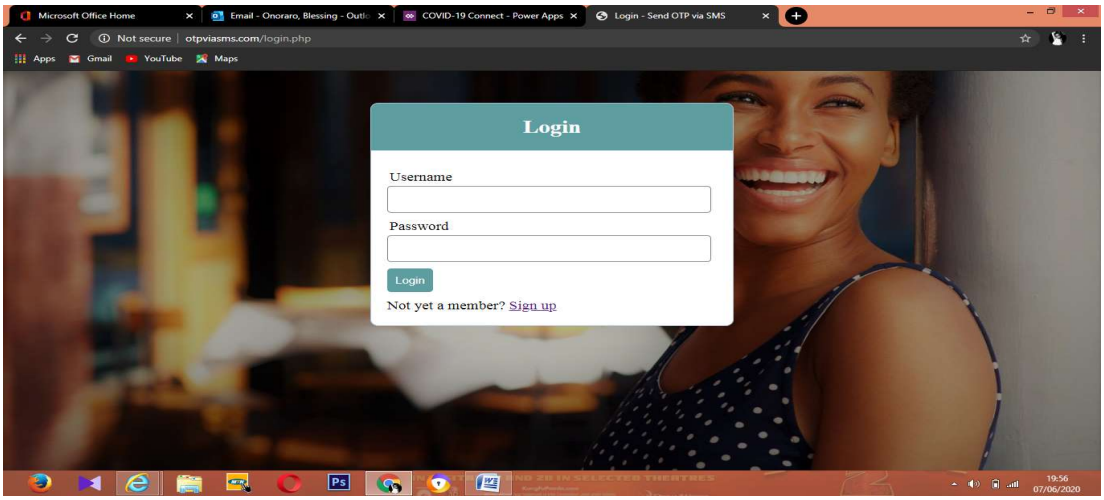


Fig 4: Registration Page for Existing User

OTP WRONG LOGIN

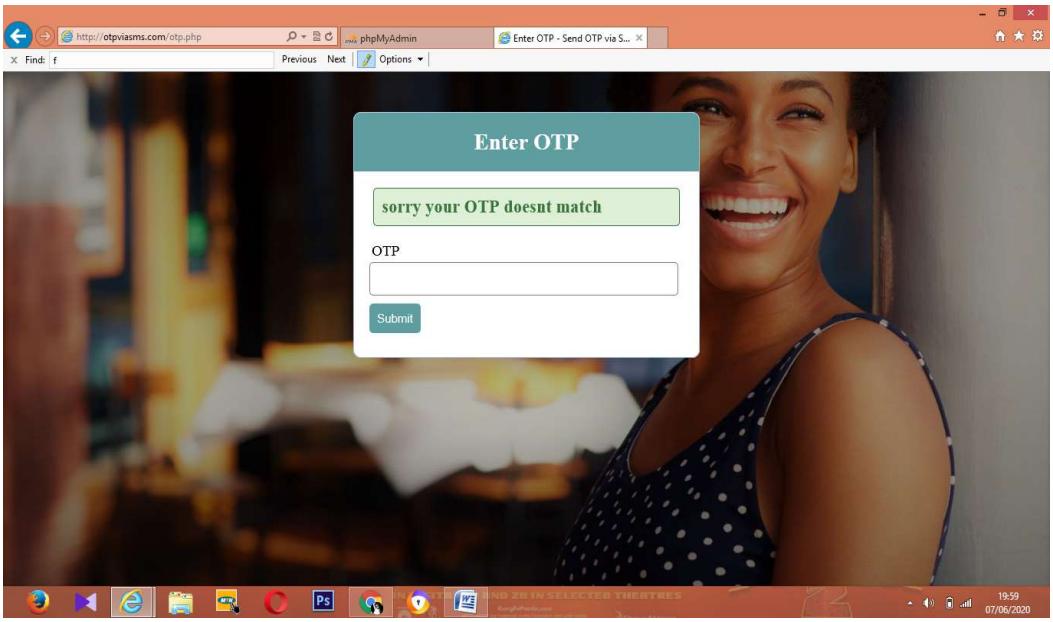


Figure 5: Prompt for OTP Wrong Login

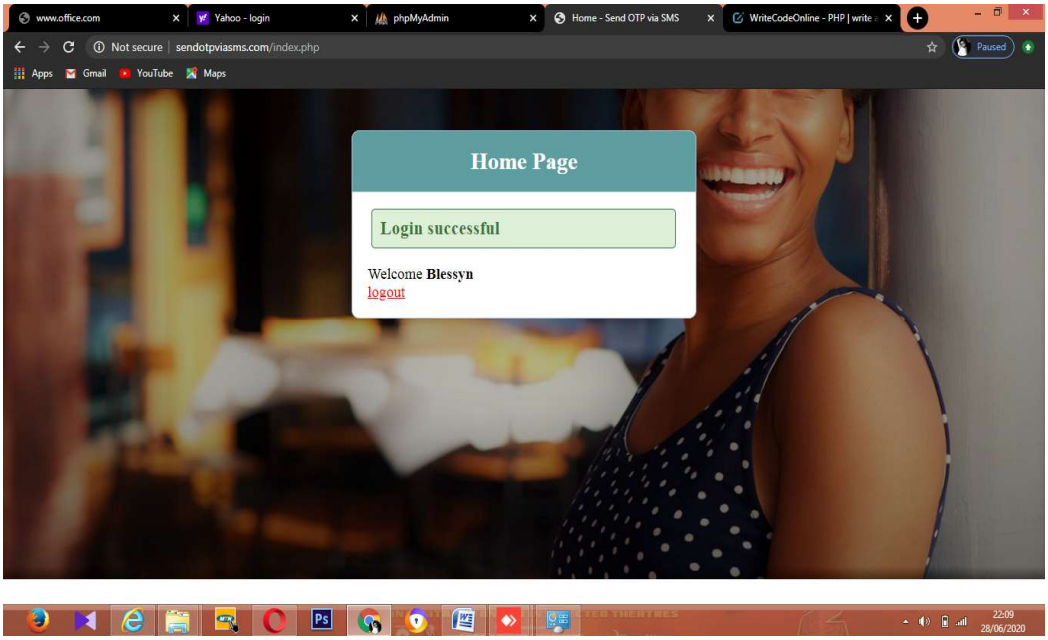


Figure 6: Prompt for OTP Successful Login

SUMMARY, CONCLUSIONS AND RECCOMENDATIONS

Summary

Based on the various researches for this work, including the idea of introducing the two authentication logins into the system has been proven worthy. It is to the best of my ability with the assistance from various sources that a software is developed for the purpose of this work which, it has added great value to the society at large. Thereby eradicating the fear of network/system security breach. This gave room to the detailed investigation and analysis of the various means of login/ password security and how to improve to a more secured way of saving our various logins and other means of accessing important pages with more security and more convenience.

Conclusions

Based on initial analysis, observations and answers during the interviews, a few preliminary statements can be noted. All interviewed persons stated that the two authentication factor makes it more safe and convenient to transact and login to their systems. All of this was achieved through the SHA-1 algorithm, and then the implementation of the design for the password generation was carried out in PHP. This was followed by an application development of this software with a dashboard and testing the implementation of the two-way authentication system with such an application. The One Time Password (OTP) was sent to the GSM user through bulk SMS solution, a SMS gateway provider. During the testing of the implementation, it was found that the system was working fine and that the implementation of the two-way authentication system was working and had better security compared to the conventional one-way authentication system. The OTP password generator ensured that the same password was not repeated and the OTP will be deleted from the database immediately after. My project goal to study and implement a two-way authentication method was successful and the functionality implemented by me was working satisfactorily.

Recommendations

Probing deeper, the demo application in this project also provide a strong foundation for future work in Two Factor authentication for security applications.

1. Future developments include a more user friendly GUI and extending the OTP algorithm so that password can be generated based on different cryptographic functions.
2. In addition to that we can add features such as giving as choice to the user to choose from different ways to authenticate him to the system to which he was supposed to authenticate.

REFERENCES

1. Archibon, A.A (2014). Ref 101: "The Nitty-Gritty Of Referencing In Research". Retrieved from http://nairaproject.com/blog/complete-guide-on-how-to-reference-in-research.html
2. Gurpreet Singh, Supriya, (2013). "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications.
3. John Jacob , Kavya Jha , Paarth Kotak , Shubha Puthran (2015). "Mobile Attendance using Near Field Communication and One-Time Password".
4. Margaret Rouse, (2016). "Authentication", http://searchsecurity.techtarget. com/definition/authentication.
5. Margaret Rouse, (2016). "Data Encryption Standard (DES)", search security. techtarget.com/definition/Data-Encryption-Standard.
6. Margaret Rouse, "Advanced Encryption Standard (AES)", http:// searchsecurity. techtarget.com/definition/Advanced-Encryption-Standard, 27-12-2016 2:55 PM.
7. Marumari, (2016). "Data Encryption and Decryption", https://developer.mozilla. org/enUS/docs/Archive/Security/Encryption and Decryption.
8. Michael Pearce, (2014). "Assessing and Improving Authentication Confidence Management", University of Canterbury, New Zealand and University of the District of Columbia.
9. Smart SMS solution SMS Gateway developer Api available at http://smartsmssolution.com/developers/api_http.php
10. Suzumura T, Trent S, Tatsubori M, Tozawa A, Onodera T (2008). Performance comparison of Web Service Engines in PHP, Java and C,IEEE International Conference on Web Services.
11. Vangie Beal, (2016). "Cryptography", http://www.webopedia.com/TERM/ C/cryptography.html,
12. Yu Tao Fan, Gui ping Su (2009). "Design of Two-Way One -Time-Password Authentication Scheme Based On True Random ,Numbers". Second International Workshop on Computer Science and Engineering.