I. J. Education and Management Engineering, **2022, 3, 13-21**
Published Online June 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijeme.2022.03.02

Development of Two-factor Authentication Login System Using Dynamic Password with SMS Verification

Abimbola Rhoda Iyanda, Mayokun Ebenezer Fasasi
Department of Computer Science and Engineering, Faculty of Technology, Obafemi Awolowo University, Ile-Ife, 220005, Nigeria
Email: abiyanda@oauife.edu.ng, maykay.fash@gmail.com

Received: 20 January 2022; Accepted: 25 March 2022; Published: 08 June 2022

Abstract: Two-factor authentication is a method of security that adds an extra layer of protection by requiring users to have two different authentication factors to verify identity. In recent years, institutions and organizations have become more concerned with the security aspects of their networks and systems, and one of these aspects is ensuring that the individual seeking access to the system is who he claims to be. With the advancement in technology and science over time, it has been seen that the safety and security of sensitive information or data transferred over the internet from one network to another has become increasingly relevant. The reliance on access to login accounts and the use of static passwords makes it easy for hackers, identity thieves, and fraudsters to gain access. Therefore, there is a need to find solutions to overcome the weaknesses to provide a more secure environment, hence, adding another step of authentication to individual identity makes it more difficult for an attacker to gain access to personal data. The proposed system generates dynamic password (OTP), which helps to add another level of security to the system against Dictionary attack, Brute-force attack especially Perfect-Man-In-The-Middle attack. The project used the Obafemi Awolowo University (OAU) e-portal login system as a case study. The system was implemented using the MySQL, CSS, HTML and PHP programming language and evaluated using reliability, effectiveness, efficiency, usability, expediency, and satisfactoriness as metrics. A questionnaire was formulated using a rating scale of 1 - 5, with 1 representing extremely poor and 5 representing excellent. The questionnaire was given to twenty (20) randomly selected students of OAU. The average score was determined and all the metrics scored higher than 4.0, which signifies a good rating. The system developed is a useful starting point for future development in security applications that require two-factor authentication. The result show that with the developed system, it can be assured that all logins are legitimate and that users are safe by verifying that the individual seeking access to the system is who he claims to be. A more user-friendly GUI is planned for the future and expanding the OTP algorithm such that password can be generated based on different cryptographic functions.

Index Terms: Two-factor Authentication, Dynamic Password, Verification, Records, Information, Attacks.

1. Introduction

An important aspect in the research field of information security is the use of authentication, and it focuses on methods for logging individuals into systems. Authentication is the process of establishing the appropriate level of assurance or confidence in the identity of the individual demanding access to any records. Identity authentication is very crucial in confirming that records (e.g. students' records, teachers' records, results etc.) are received or transferred by the authorized or envisioned recipient or sender.

Authentication is achieved through various techniques using authentication factors. The type of authentication factors to be employed depend solely on the sensitivity of educational records being retrieved. A simple authentication method can be formulated plainly as "Something we know", such as a password or PIN (personal identification number), or "Something we have", such as biometric data. Apart from that, other categories, such as "something we do," such as an Access Point Button, can be included in this taxonomy (WPS), "Somewhere we are", such as location-based cellular networks that can use a claimed identity to verify or challenge. The last category can reduce risk, but does not directly increase the level of security.

Standard authentication techniques can be used independently or in tandem with others. Multifactor authentication is a means of creating better authentication processes and increasing system security by combining multiple authentication methods [1].

Some graphical-based password methods have been used such as:

1. Knowledge-based Technique (KBT) which is based on confidential information that only the user knows is the most common and widely used authentication method [2]. Including low cost and ease of implementation, scalability, and extensive user knowledge.
2. Attribute-based Technique (Biometric): which is based on the distinctiveness of a user's human qualities?
3. Possession-based Technique (Token): which deals with the use of tangible items to represent a user's identity in order to gain access to a system?

Passwords are unique combination of characters, numbers, or words that are used for gaining permission to a device and are unique only to the user. Passwords ensure that computers and data are only accessible to those who have been given permission to view or use them [3]. Password can be grouped into (i) One-Time Password (OTP) [4], (ii) Cryptography [5], (iii) Encryption and Decryption [6, 7]: Data Encryption Standard (DES) [8], Triple Data Encryption Standard Algorithm [9], Advance Encryption Standard [8].

One approach for generating One-Time Password is through the use of a mathematical algorithm to create a new password based on the previous password, which means one-time passwords are a sequence and must be used in a predefined order. This is not secure because if a hacker discovers the user's password pattern, he can easily trace out future OTPs. The most cost-effective method will be to create a one-time password and then send it on a piece of paper that is already known to the person who generates OTPs on a computer. This is because these devices eliminate the costs of SMS messaging. Even though it is less expensive to send the OTPs this way, it is not feasible because the time it takes to deliver the password to the user may be too long.

Dynamic password that is the one-time password is a sequence password scheme that has been shown to be non-decryptable in principle. Its basic concept is to introduce an unknown factor into authentication, requiring users to provide different authentication messages each time. This allows apps to achieve a higher level of protection than the fixed password technology.

The other systems depend on algorithm-based electronic tokens. When a token is not correctly synchronized with the server, the OTP generators must manage the situation where the device needs the OTP to be entered on a default timeout, which results in additional development costs. Time-synchronized systems prevent this, although at the expense of having to keep a clock in the electronic tokens running.

In comparison to hardware tokens, the need to bring an extra item that serves no purpose other than creating one-time passwords can be removed if one has a phone or mobile computer. Considering the cost, using a cell phone as a token is the most cost-effective option since it eliminates the need to deliver devices to each end user. Many proprietary tokens, on the other hand, have tamper-proof functionality. The proposed work investigates and introduces the two-way authentication process, as well as its benefit over the one-way authentication framework. The limitation of these measures is that they may be costly for students, inconvenient to carry around, and can be forgotten at times.

The main objective of this study is to boost the security of OAU e-portal and address its security susceptibility introduced by the current method of authentication been used. The study presented a system that will mitigate this issue through two-way factor authentication using SMS verification. Adding another step of authentication to individual identity makes it more difficult for an attacker to gain access to educational records or break into individual account and hence, there is great reduction in fraud, data loss, and identity theft, thereby improving the security of the system. The other objectives include, identifying the threats that are introduced by one-way authentication as a method of authentication that is currently used by OAU e-portal and how it affects the security of their system. Also, to investigates and introduces the two-way authentication process, as well as its benefit over the one-way authentication framework such as having a system more secured, user friendly, less expensive, faster and efficient.

The rest of this paper is organized as follows: section 2 summarizes the related work done; section 3 focuses on the methodology; section 4 presents system evaluation and results discussion, and finally, section 5 concludes

2. Review Works

Over the years many works have been done in the area of authentication and discussion on some of the related works is mentioned below:

Authentication, by definition, is the method of verifying the genuineness of users or processes by checking their proof of identity. Password authentication, or the use of a username and password combination to login into one's account, is a common example of an authentication system. Logically, authentication is a process that comes before authorization. Authentication and authorization seem similar but they are not [10]. Authorization is the act of granting permission to something or someone.

With the advancement in technology and science over time, it has been seen that the safety and security of sensitive information or data transferred over the internet from one network to another has become increasingly relevant. Information must be secured from internal and external threats by using the appropriate protection tools. In addition to the procedures in place to prevent unauthorized users from accessing information through communications and to

ensure the validity of these communications, the majority of today's systems rely on the use of reusable passwords that may or may not expire to verify a user's identity.

Users have the tendency of using easily discovered passwords, and to duplicate passwords for multiple accounts or even by storing and writing down the password either on computers or papers and also making use of websites to save and remember password. The reliance on access to login accounts and the use of static passwords makes it easy for hackers, identity thieves, and fraudsters to gain access. Furthermore, cybercriminals tend to use a variety of tactics and attacks to obtain control to a user's login data, including guessing attacks and social engineering attacks. A better, more secure way of authentication is the "two-factor" or "strong authentication" based on one-time passwords, instead of authenticating with a simple password [11].

Two-factor authentication is a method of security that adds an extra layer of protection by requiring users to have two different authentication factors to prove their identity, which is more reliable and safer than the commonly used one-factor authentication. The first variable in a two-factor authentication system is the user's standard password and username, which they create when creating an online account. The second variable can be something you are, something you know or something you have. Something you know can be PIN or password; something you have can be a credit card, tokens or a smartphone; something you are can be Biometric pattern of a fingerprint, iris scan or voice print.

A typical two-factor authentication scenario is the withdrawal of money from an Automated Teller Machine (ATM). If a person wants to make a withdrawal the person has to insert his/her credit card to the ATM which is an example of something you have, after which the person would enter his/her pin or password which is an example of something you know, in order to gain access to their accounts. Using a two-factor authentication process can help to lower the number of cases of identity theft on the internet because the criminal would need more than just the users name and password details [12].

Many approaches have been used for authentication such as Fingerprint [13] which creates a single-use, time-limited password that will be used in addition with the username and password to login to the linked web site. This is limited in that the application of mobile phones that support fingerprints is very expensive to acquire and fingerprint requires soft fingers without injuries to work properly while the proposed system does not require a biometric feature to function and it is cost efficient. The application of mobile phones with support fingerprint is very expensive to get and fingerprint requires soft fingers without injuries to work properly. Two-factor identity authentication mechanism has also been adopted [14]. This uses username and password mechanism for the first authentications step and QR code is then generated by the system as a one-time password for the second authentication step which will be manually checked by the user with the help of web camera. The proposed model is different in that it uses a quick response code which is a type of barcode that can be read by a digital device and stores information as a series of pixels in a square-shaped grid.

The necessity of the users having a device that uses QR reader to read the QR code and a web camera to scan the QR code makes it costlier and if the user chooses to get QR codes through email, it will require the usage of the internet, raising danger of insecurity and perhaps delayed delivery. Using SMS in exchange for email [15] may have delay too, causing the OTP to expire and in addition attracts telecommunications charges. In addressing some of these issues, [16] proposed a secure login using OTP that is encrypted and mobile based login techniques which secures login to web server by generating OTP then encrypting it by advance encryption standard (AES).

In this case, users do not need to manually input OTP; it is encrypted and sent to a mobile phone via email. The user simply reads the email for verification, then types his or her application password into the encrypted OTP and sends it to the system's web server. Nevertheless, this method still stands the risk of hacking and brute-force attacks on OTP, as well as the possible delay in email delivery which may be due to a weak internet connection, hence, causing the OTP to expire. In the proposed system, the OTP is generated from the server and uses short messaging system which is more secured, user friendly, faster and efficient.

[17] developed a Two-factor Authentication Scheme for online financial transactions using Graphical Password with a view to make the user have easy login by providing pre-selected images for remembering his password. The generated images and the parameters are stored in the smart card and are sent to the user by the secure medium. The smart card is inserted into the system at login and the login request will be sent. After confirmation of digital credentials by both sides, the server sends portfolio images to the user who will then select the password. This scheme helps to authenticate the users of e-services and allow access to the resources for strong security. There are still needs for tangible analysis against common attacks such as SQL injection, Phishing attack, and guessing attack.

The proposed system (using OAU eportal as case study) adopted in its implementation an additional layer of security, which is the two-factor authentication using dynamic password generation. Also, the OTP is generated from the server, hence makes it more secured, user friendly, faster and efficient.

3. Methodology

This part explains the method used in the development of the system.

3.1 System Design

The password generation was done by writing an OTP generator function in PHP. The Dynamic password (also known as the OTP) is delivered to the cell phone using a SMS gateway provider (Ebulk SMS). The Dynamic password generator will make sure that similar passwords are not generated twice and the generated password will be removed automatically from the database. The two-factor authentication technique was based on Static password derived by the user and a dynamic password. In this technique, the user provides their personal details such as username, email address and phone numbers to serve as their password. Fig. 1 shows the system architecture.

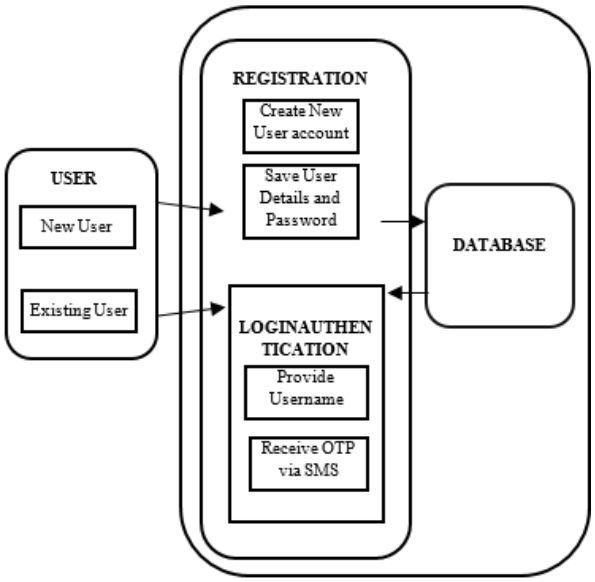

Fig. 1. System architecture

The system objective is to be able to generate a unique code that can't be guessable by anyone and encrypt the provided password for preventing any form of database threat so as to make the system scalable. The design of the system was represented using flowchart (Fig. 2) and use case (Fig. 3) diagrams. The design process is as follows:

1. The user starts the system and types their password and username into the system.
2. The inputted username and password are checked to confirm if they are in the database, if it is not, an error message will be displayed.
3. The user is re-directed back to the registration interface.
4. An OTP will be generated using a function and calls the sms Api to send the dynamic password to the registered number.
5. The user receives an SMS.
6. The user enters the OTP and clicks the submit button.
7. If OTP entered is the same with the OTP sent the user is granted successful access to the system.

3.2 System Implementation

The application was built on a windows 10 computer with the following device requirements: a system running on AMD or higher processor and Xampp, needed to be able to open and run the PHP file in an offline environment.

Cascading Style Sheets (CSS) and Hypertext Markup Language (HTML) were used to create the client-side component. There is no operating system or device-related changes required because it runs within the user's web browser. The client component represents the functionality of a web application with which the end-user interacts. HTML was used to design the interface of the system presented to the users to interact with on the internet via a browser while CSS describes the presentation of a document and it was used to design the text and the web pages written by the HTML on the internet.

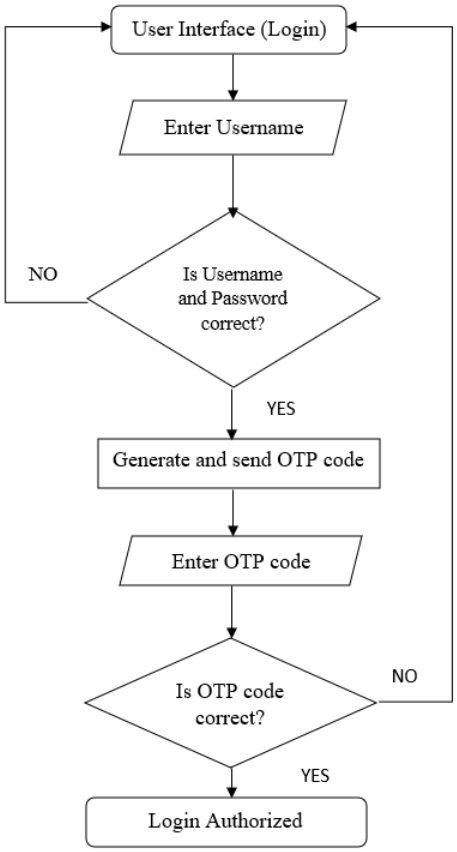

Fig. 2. System flowchart

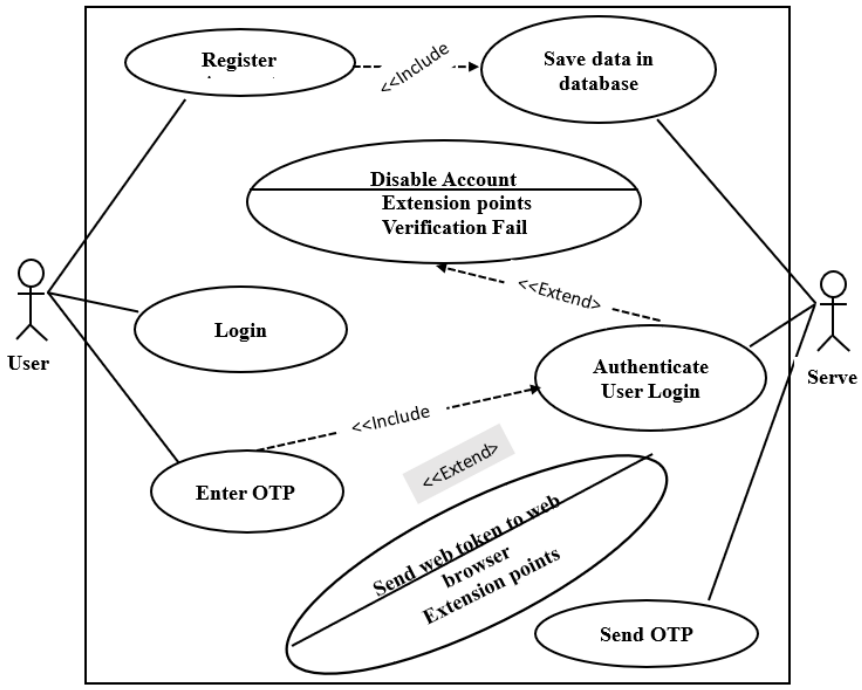

Fig. 3. System use case diagram

MYSQL Database Server is the database construct that enables PHP and Apache to work together to access and display data in a readable format to the browser. It was used to create the database of the system. The database holds user information such as usernames, passwords, e-mail addresses, and phone numbers of the users. It also holds OTP

query, which consists of two tables: the OTP and the user. The OTP table stores the OTP code generated by the OTP generator, and the user table stores the user's password and username derived by the user. Whenever a client requests an OTP via a short message service, the server verifies the user's credentials, generates the OTP, and immediately sends it back to the client. PHP (Hypertext Preprocessor) is a server-side scripting language that allows the website to be truly dynamic. It is the back-end programming language that was used in creating the system which was used to serve webpages to the users on the internet.

The OTP generation function is the function is used to produce the OTP which consists of two functions: the randomActivate()- the one in charge of deriving the dynamic password which will loop six times to get the random OTP and the second function which is the active_exist($code)- has a single argument, this function makes sure that the OTP cannot be inputted twice. The system requests for the username and password and the dynamic password (the OTP) which is derived from the OTP generation function is sent via short message service on the user's phone number. The user must then input the OTP code to authenticate themselves and be granted access at the server's side.

On the server side, a database is required to hold user information such as first and last names, passwords, email addresses, and phone numbers. Since the password field was hashed, the hashes cannot be reversed if the database was hacked. An OTP database was created which consists of two tables the OTP and user. The OTP table stores the OTP code generated by the OTP generator and the user table stores the user's password and username derived by the user. Whenever a client requests an OTP via a short message service, the server verifies the user's credentials, generates the OTP, and sends it back to the client immediately. The OTP code was made sure to be as random as possible and to be unpredictable and irreversible. An OTP code is generated which lasts for a maximum of 60secs to 90secs.

Fig. 4 shows the student registration page where unregistered users do their registration while Fig. 5 shows where the registered users can log in to the system (home page). Fig. 6 shows the OTP confirmation page where the OTP code created by the OTP generator function, which is sent to the user, is inputted to gain access into the system. The Dashboard interface shows that the user has successfully logged into the system (Fig. 7).

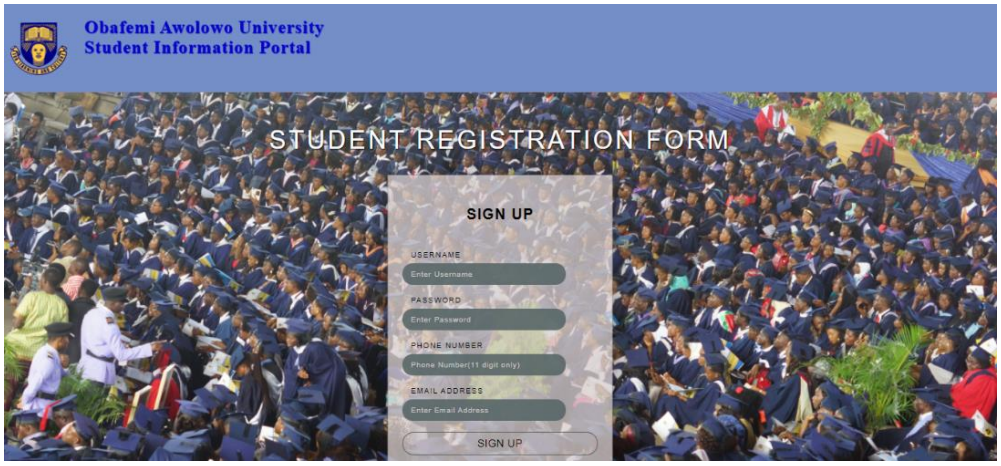

Fig. 4. Student Registration Page

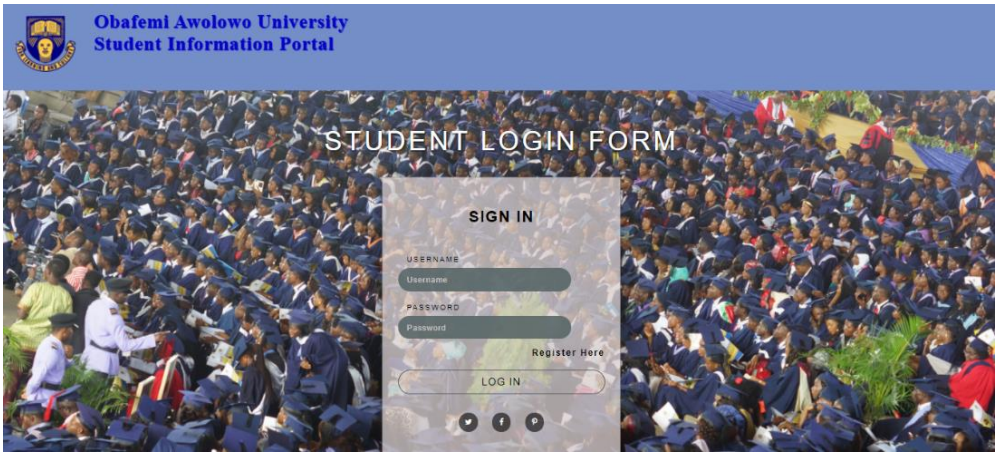

Fig.5. Student Login Page

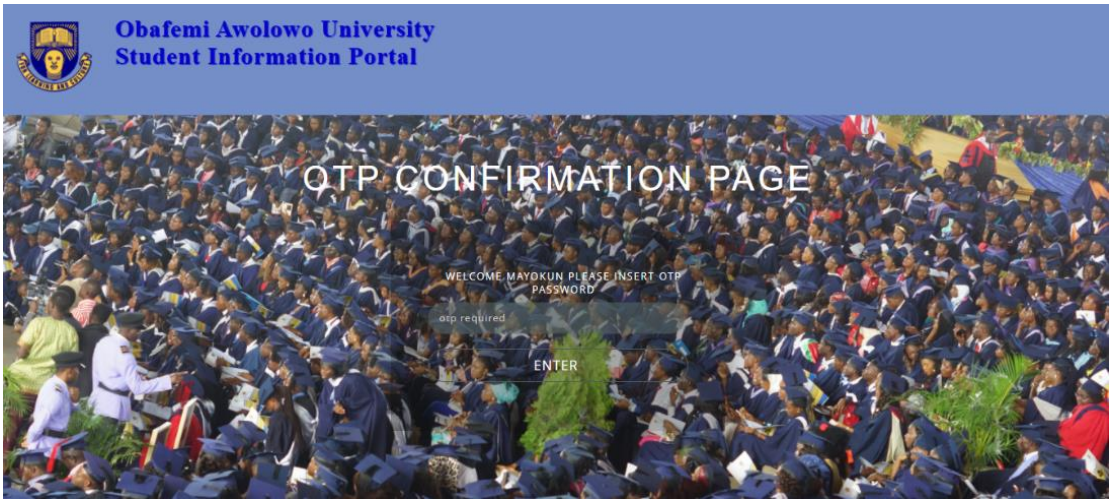

Fig.6. OTP Confirmation Page

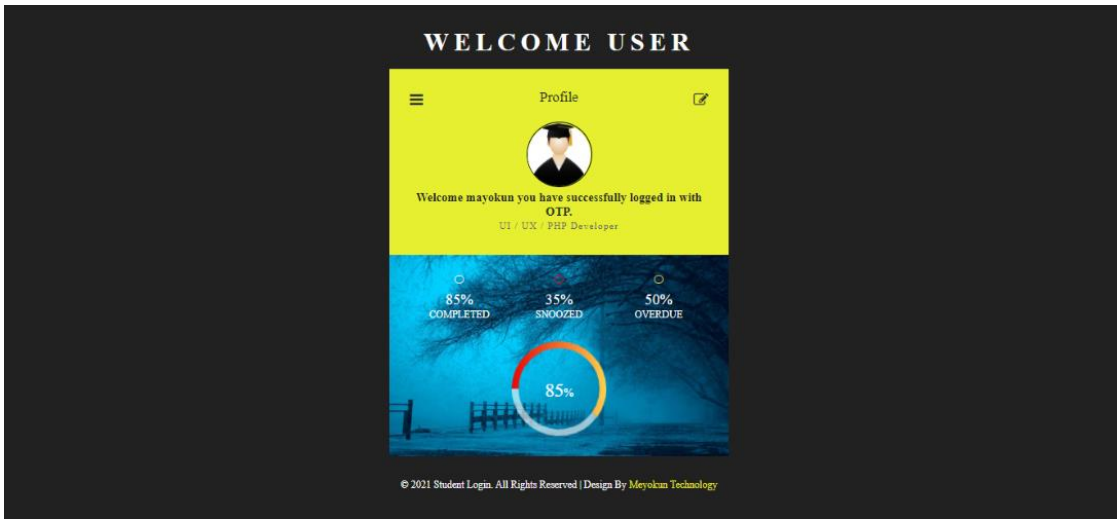

Fig. 7. Student Dashboard

4. System Evaluation and Results Discussion

An experiment was conducted to check if the OTP generator function will generate the same OTP code for users. Different numbers of users were created for the testing, and for each user, a different number of OTP code was generated and they were all unique. The overall process from the server's side of receiving the request, checking the factors, creating, and sending the OTP took less than a second. Following a successful test and evaluation, the results were thoroughly scrutinized and compared to operational specifications to confirm that they complied with the objective's parameters. This validates the suggested system's effectiveness and efficiency when dealing with multiple users.

Developing a good and logically sound test plan is very vital to developing a bug free software system. Table 1 shows the unit test plan developed for the testing of this system. The system was evaluated using mean opinion score (MOS) with some evaluation metrics predetermined at the start of the project: reliability, effectiveness, efficiency, usability, expediency, and satisfactoriness. Reliability shows how reliable and secure the system is; effectiveness shows how fast the system is; efficiency shows how efficient the system is; usability shows how user-friendly and sustainable the system is and satisfactoriness shows the satisfactory level of the users and how well they enjoyed using the new system. The MOS of the system was done by administering questionnaires to people. The system aimed at targeting every user with an opinion and there is no restriction to any class. The evaluation of the system was carried out among 20 randomly selected students of Obafemi Awolowo University used as respondents to obtain their review of the system.

The questionnaire was formulated using a rating scale of 1 - 5, with 1 representing extremely poor and 5 representing excellent. 60%, 35% and 5% of the respondents rated reliability of the system has been Excellent, Good and Average respectively while 25%, 55% and 20% of the respondents rated effectiveness of the system has been Excellent, Good and Average respectively. 50%, 40% and 10% of the respondents rated efficiency of the system has been Excellent, Good and Average respectively while 40%, 35%, 15%, 10% of the respondents rated usability of the

system has been Excellent, Good, Average and Bad respectively. 45%, 15%, 30%, 10% of the respondents rated expediency of the system has been Excellent, Good, Average and Bad respectively while 30 %, 50 %, 20 % of the respondents rated users' satisfaction has been Excellent, Good, Average respectively. The new system provided more security because no one other than the user can log-in due to the generated dynamic password that will be sent to the users for validation.

The average score was determined and it was observed that all the metrics (reliability, effectiveness, efficiency, usability, expediency, and satisfactoriness) scored higher than 4.0, which signifies a good rating and presented the proposed framework as the best choice for authentication on OAU e-portal. Table 2 shows the system evaluation result.

Table 1. Unit Test

	Tested Data	**Expected Result**	**Actual Result**
1	OTP	To correspond with what is in the database storage.	It corresponded with the pin in database and was validated.
2	Username and password	Must be correct password given to the student by the admin.	The password was correct and was able to display page for registration.
3	Administrator login	Expected to login if and only if it is the administrator.	Was able to login because of correct identity.
4	Queries	To view user's information and OTP code.	Was successful.
5	Data connections and linking buttons	To see if the interface is connecting to database and view other pages.	Was able to connect to database and can also display other pages.

Table 2. System Evaluation Result

	Extremely Poor (1)	**Bad (2)**	**Average (3)**	**Good (4)**	**Excellent (5)**	**Average Score (5)**
Reliability	-	-	1	7	12	4.6
Effectiveness	-	-	4	11	5	4.0
Efficiency	-	-	2	8	10	4.4
Usability	-	2	3	7	8	4.1
Expediency	-	2	6	3	9	4.0
Satisfactoriness	-	-	4	10	6	4.1

5. Conclusion

With the advancement in technology and science over time, it has been seen that the safety and security of sensitive information or data transferred over the internet from one network to another has become increasingly relevant. Two-factor authentication is a method of security that adds an extra layer of protection by requiring users to have two different authentication factors to prove their identity, which is more reliable and safer than the commonly used one-factor authentication. This study aimed at developing a strong authentication system which is the two-way factor using SMS verification. The system was developed to provide insight on the vulnerabilities of the traditional one-way authentication factor being currently used on OAU e-portal and offer a robust authentication system which is more secured, less expensive, faster and efficient. Thus, using this proposed scheme, critical application will be secured against Dictionary attack, Brute-force attack and Replay attack especially Perfect-Man-In-The-Middle attack. In summary, single factor authentication, which consists of a password and a username, is no longer deemed secure on the internet. Automated password collection algorithms can easily discover easy-to-guess passwords like age, names, and dates of birth. Two factor authentications has been introduced to meet the demand of organization for providing better and more secured authentication option for its users.

The proposed system generates dynamic password (OTP) which helps to add another level of security to the system. This produces a one-time password (OTP) and sends it to the GSM user using EbulkSms, an SMS gateway service. During testing, it was discovered that the system was operational and that the two-way authentication system was functional and secure when compared to the traditional one-way authentication system. The OTP password generator assured that the same password was never used twice by instantly removing it from the database. The result show that with the developed system, it can be assured that all logins are legitimate and that users are safe by verifying that the individual seeking access to the system is who he claims to be. A more user-friendly GUI and expanding the OTP algorithm such that password can be generated based on different cryptographic functions is planned for the future.

References

[1] Maayan, G. D. (2020). 5 User Authentication Methods that Can Prevent the Next Breach. https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/. Visited: March 2022

[2] Dhamija, R., & Perrig, A. (2000). Deja {Vu--A} User Study: Using Images for Authentication. In 9th USENIX Security Symposium (USENIX Security 00).

[3] Stein, A. (2022). "What Is Password Hacking?", http://itstillworks.com/password-hacking-7273695.html. Visited: March 2022

[4] Jacob, J., Jha, K., Kotak, P., & Puthran, S. (2015, October). Mobile attendance using near field communication and one-time password. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1298-1303). IEEE.

[5] Beal, V. (2021). "Cryptography", https://www.webopedia.com/definitions/cryptography/. Visited: March 2022

[6] Al-Hazaimeh, O. M. A. (2013). A new approach for complex encrypting and decrypting data. International Journal of Computer Networks & Communications, 5(2), 95.

[7] Thitme, S., & Verma, V. K. (2016). A recent study of various encryption and decryption techniques. International Research Journal of Advanced Engineering and Science, 1(3), 92-94

[8] Loshin, P. and Cobb, M Techtarget. [Online] (2022). Encryption". https://www.techtarget.com/searchsecurity/definition/encryption. Visited March, 2022

[9] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

[10] Techtarget (2021). Authorization. https://www.techtarget.com/searchsoftwarequality/definition/authorization. Visited: December 2021.

[11] Jorstad, I., & Jonvik, T. (2009, October). Strong authentication with mobile phone as security token. In 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (pp. 777-782). IEEE.

[12] Wallen, J. (2020). "What is Two Factor Authentication", https://www.lifewire.com/how-to-use-two-factor-authentication-4686242. Visited: March 2022

[13] Yıldırım, N., & Varol, A. (2015). Android based mobile application development for web login authentication using fingerprint recognition feature. In 2015 23nd Signal Processing and Communications Applications Conference (SIU) (pp. 2662-2665). IEEE.".

[14] Eminagaoglu, M., Cini, E., Sert, G., & Zor, D. (2014, September). A two-factor authentication system with QR codes for web and mobile applications. In 2014 Fifth International Conference on Emerging Security Technologies (pp. 105-112). IEEE.

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

[16] Kalaikavitha, E., & Gnanaselvi, J. (2013). Secure login using encrypted one time password (OTP) and mobile based login methodology. International Journal of Engineering and Science, 2(10), 14-17.

[17] Quadry, K. M., Govardhan, A., & Misbahuddin, M. (2021). Design, Analysis, and Implementation of a Two-factor Authentication Scheme using Graphical Password. International Journal of Computer Network & Information Security, 13(3).

Authors' Profiles

Dr. Abimbola R, Iyanda holds a B.Sc. degree in Computer Engineering, an M.Sc. and Ph. D. degrees in Computer Science from Obafemi Awolowo University, Ile-Ife, Nigeria. The thrust of her research is in the area of Computing and Intelligent Systems Engineering with focus on Speech and Language Engineering research aiming at domesticating computer technology and the computational rendering of indigenous ideas. She is a Member of the Nigerian Society of Engineers, Association of Professional Women Engineer in Nigeria, Council for the Regulation of Engineering in Nigeria, Association for Women in Science for the Developing World (OWSD) and Nigeria Computer Society. Her present employment is with the Computer Science and Engineering Department, Faculty of Technology, Obafemi Awolowo University, Ile-Ife, Nigeria.

Mr. Mayokun E. Fasasi holds a B.Sc. degree in Computer Engineering from Obafemi Awolowo University, Ile-Ife, Nigeria.

How to cite this paper: Abimbola Rhoda Iyanda, Mayokun Ebenezer Fasasi, " Development of Two-factor Authentication Login System Using Dynamic Password with SMS Verification", International Journal of Education and Management Engineering (IJEME), Vol.12, No.3, pp. 13-21, 2022. DOI: 10.5815/ijeme.2022.03.02