Secure Three Level Authentication System Using Text-Based Password, Colour Pattern and Image

Owobu Joshua Mark, Dr. (Mrs.) Ugochi A. Okengwu

Abstract— There are many authentication system proposed and most of them still have weaknesses. Some of these focused on the physical and behavioral properties of the user such as voice recognition, and some others focused on knowledge of the user such as textual and graphical passwords. However, these systems are still not secure enough and allow attackers to steal the data easily. Therefore, there is need for something more secure and user-friendly to overcome this problem. In this thesis, a secure three level authentication system using text-based password, colour pattern and image to overcome the problem is present. The system is designed using the waterfall model, and implemented using (SQL, Html, and PHP), programming languages. The system will give a better secure environment to the user from unauthorized access.

Index Terms— Authentication, Colour pattern, Image, Password, Secure, Text-based.

1. INTRODUCTION

Since the inception of the internet, it created a world of cybercriminals with it. Rauti and Leppanen 2014 opined that the objectives of the cybercriminals are to steal information, commit online fraud businesses with a low risk of being caught. The low risk of being caught is due to compromised intermediate network. In the view of Mannan 2009, although this was true in the early days of networked computers, the internet evolution has allowed adversaries to live closer to and within end hosts. Hence, a large amount of attention in academia and industry has been inspired to investigate more into the concept of developing a secure user-authentication system to secure the commercial transactions among the organization and individuals with respect to stopping host adversaries.

Authentication is an activity to authenticate the persons' credential that wishes to perform the activity. The authentication process is complete if the credential matched, and then the user granted access. Generally, the user will need to provide their password to begin using a service of the system. User authentication authorizes human-to-machine interactions in operating systems and applications as well as both wired and wireless networks to enable access to networked and Internet-connected systems, applications and resources.

- *Author name is currently pursuing Master of Science (M.Sc.) degree in information technology in National Open University of Nigeria, Abuja, Nigeria, PH-+2348032392423. E-mail: joemark_77@yahoo.com*
- *Co-Author name is currently a senior Lecturer of Computer science in University of Port Harcourt, Nigeria, PH-+2348037239319. E-mail: ugochi.okengwu@uniport.edu.ng*
(This information is optional; change it according to your need.)

The current methods used for user authentication are categorised into single-factor authentication, two-factor authentication and three-factor authentication, which correspond to something the user knows, something the user has and something the user is, respectively (Gorman, 2003 ; Jiangshan, Guilin & Wei, 2014; Xinyi et al. 2011). The widely employed single-factor authentication is a simple password-based mechanism that employs a username/password combination to be authenticated. However, passwords can be easily stolen, forgotten or guessed (Gorman, 2003), and this mechanism is vulnerable to various attacks (Dimitriadis, 2007). In contrast, two-factor authentication is a much stronger mechanism that combines what the user knows with what the user has. Thus, it is based on the user's possession of an object for providing a challenge/response mechanism to increase the level of authentication security (De Cristofaro, Du, Freudiger and Norcie, 2014). The final authentication mechanism is based on authenticating the user via his/her biometrical characteristics (Gorman, 2003; Jiangshan, Guilin & Wei, 2014; Xinyi et al. 2011).

The most popular kind of password used for security purposes is text-based. However, these passwords are easy to breach and one may lose his/her private data to the wrong hands. With the rise in cyber-crime, security threats related to logins & accesses have become a major concern. In addition, the use of single security authentication is not sufficient to keep you protected from cyber threats.

Hence, to increase the security level we have developed a secure three level authentication system using text-based password, colour pattern and image that will make sure that only the authorized person will have access to the system or data. This system contains three-level logins having three different kinds of password systems.

The project comprises a passphrase, graphical password and image-based segmentation password. The password difficulty increases with each level making the access more secured. In this way, this PHP-based three level authentication system will help the users to keep their data safe from any hackers & cyber threats.

2. LITERATURE REVIEW

Authentication is the way a user is identified prior to being allowed access to the network and network services (CISCO, 2014). The National Institute of Standards and Technology (NIST) defined authentication as the process of establishing confidence in the identity of users or information systems (Burr et al. 2011). Online security is a major factor in organizations as hackers are on 24 hours trying to bridge into vulnerable organization's networks. Therefore, the first step towards establishing a secure connection with an organization is authentication (Basu and Muylle, 2003).

Going by the present day, internet information insecurity that has ravaged the internet world globally, using only single-factor authentication is at high risk and not secure enough. Thus, the use of multi-factor password authentication will increase the security protection against attacks. The secure three level authentication system is an authentication system, which combines three existing password authentication scheme to form a better secure computer network and services.

Generally, we have three main categories of authentication methods, which are Token based authentication, Biometric based authentication and Knowledge based authentication.

Token based means "what you have". Token based techniques, use tokens such as key cards, bankcards and smart cards that are widely used by everyone. According to Mughele E. S. (2015), just as when a person loses a key, he would not be able to open the lock, a user who loses his token would not be able to login, as such the token-based authentication category is quite vulnerable to fraud, theft or loss of the token itself.

Biometric based techniques means "what you are". Babich, A, (2012), stated that Biometric based techniques uses physiological biometrics like measurement of human body, such as fingerprint, face geometry and iris. The main problem of this approach is the higher cost of the system and recognition can be slow.

Knowledge based technique means "what you know". It is the most used authentication method. According to Mughele E. S. (2015), Knowledge based technique includes both text-based and graphical-based password.

This thesis, proposed multifactor authentication system that is the combination of existing authentication techniques/methods. The project comprises of text password i.e. passphrase, graphical (Colour-Pattern) password and image based password for the three levels respectively. This way there would be negligible chances of bot or the possibility of cracking the passwords even if they succeed in cracking the first level or second level, it would be impossible to crack the third one. Hence, while creating the technology the emphasis was on the use of innovative and untraditional methods. Many users find the most widespread text-based password systems unfriendly, so in the case of three level password we tried creating a simple user interface and providing users with the best possible comfort in solving password. Below are the concepts of this 3-level authentication system.

The proposed three level authentication system involve the following:

a. Text-based Password technique (Level 1)

Lamport (1981) was the first to propose the concept of password-based authentication. The concept require authenticating a user based on an inputted username-password combination. In this authentication process, the system only stores the password-hash result to be compared with the submitted password after applying the hash function (Raza et al. 2012); however, it is vulnerable to password theft. Nevertheless, it is still utilized to access some internet applications that does not require strong protection against repudiation (Gorman, 2003), such as e-mail services and social networks (Jiangshan et al. 2014; Dimitriadis, 2007), although its security properties are not reliable (Jiangshan et al. 2014). Requesting longer and more complex passwords in an attempt to secure this mechanism has led users to write down their passwords, making them prone to theft (Dimitriadis, 2007).
Although password-based authentication takes place via a secure socket layer (SSL) channel, it is still vulnerable to sniffing attacks (Sumitra, Pethuru and misbahuddin, 2014) within the SSL handshake establishment process (Mahboob and Ikram, 2004). Here, the sniffer masquerades as the server and provides the user with a fraudulent certificate (Dimitriadis, 2007). Therefore, the system also becomes vulnerable to man-in-the-middle (MITM) and phishing attacks (Dimitriadis, 2007). Alongside password-based authentication vulnerabilities, users are required to manage and memorize too many passwords (Petsas, et al. 2015). Therefore, specialized password-manager (PM) software is available (Petsas, et al. 2015), which "manages and organizes passwords and personal identification in a secure manner. Such software can help reduce the effort in creating, memorizing, and changing passwords (Lackey et al. 2014).

Password managers are classified into web-based and browser-based PMs. However, while password managers are secure against phishing and pharming, they are still vulnerable to failures, which can be due to the web-based

PM server being targeted by cyber-attacks, or the browser-based PM information being stolen or lost due to damage to the local hard disk (Lackey et al. 2014).

Furthermore, a security analysis conducted on five popular web-based PMs, found that four of them namely, LastPass, RoboForm, My1Login, and PasswordBox, have critical vulnerabilities in which attackers can obtain the user's credentials Li et al. (2014). A good remedy for this is to include an extra object, which is possessed by the user and entered into the authentication mechanism, thus forming a stronger two-factor authentication Jiangshan et al. (2014). The password-based authentication mechanism cannot be employed as a secure stand-alone system to be used within financial institutions and e-commerce.

The first level of the proposed system is text-based (passphrase) authentication password. User authentication through textual password is conventional in computer system because it is easy to use. Gayathiri Charathsandran (2012), state that text-based password is popular since last 4 decades, for its easiness, cost effectiveness, simplicity and familiarity to all users. Text-based password contain alphanumeric and/or special keyboard characters and the user to authenticate her/himself to the system used it as a shared secret.

At this level, users need to register his/her Email ID and text password in the system. The password can be numeric, alphabets and any characters that make sure it is strong. To login, users need to reenter the registered information that he/she submitted in the registration process.

It should be noted that, text-based password also have many categories like alphanumeric password and mnemonic (prompt) password. According to Priti and Lalit (2013), alphanumeric password came into existence in the 1960s for security purpose that secure the confidential data.

In alphanumeric password, the password require the following:

a. Password should be at least 8 characters long
b. Password should not be easy to relate to the user
c. Password cannot be word that can be found in dictionary and public dictionary
d. Users should combine upper and lower case letters and digits

Failure to fulfill the above stated requirement, it becomes very easy to crack or guess this type of password by third person because it is not strong enough.

In an attempt to strengthen the password, mnemonic phrase-based passwords is recommended for users. Cynthia et at. (2006), state that, a mnemonic password is one where a user chooses a memorable phrase and uses a character (often the first letter) to represent each word in the phrase. Weining et al. (2016) are of the view that it helps users to generate secure and memorable password. They also suggested that it is the most widely recommended and studied strategy.

To create mnemonic passwords users are directed to do so by following the steps below:

a. Think of a memorable sentence or phrase containing at least seven or eight words. • Select a letter, number, or special character to represent each word in your password. A common method is to use the first letter of every word.
b. Ideally, the password should contain a mixture of lower case and upper case letters, numbers, punctuation, and special characters (such as ^ or %).
c. Remember the phrase.

b. Graphical (Colour-Pattern) Password Technique (Level 2)

This authentication system uses end user's visual memory, a graphical password method where users have to set password based on some colour combinations through RGB button combinations.

To overcome the shoulder surfing attack, Gao et al. (2009) proposed a graphical password scheme, which uses colour login, and provide resistant to the shoulder surfing attack. This scheme is very strong but has drawbacks like, the probability of accidental login of Colour login is too high and the password space is too small.

The second level of the proposed system is colour-pattern authentication password. The user is required to select a colour combination of RGB button that is preferable by him/her.

c. Image Recognition Passwords technique (Level 3)

According to Ahmad Almulhem (2011), graphical passwords refer to using pictures (also drawings) as passwords. In the views of Antonella et al. (2005), in theory, graphical passwords are easier to remember, since humans remember pictures better than words. Furthermore, graphical password should be more resistant to brute force attacks, since the search space is practically infinite.

The third level is an image based password where users can upload their desired image into the system and then create password by segmenting (cropping) it and assigning them serial numbers. During login process, the system will automatically disperse the image segmentations and users have to arrange it as set by them initially.

Xiaoyuan et al. (2005), state that in general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce

something that he or she created or selected earlier during the registration stage.

In 2000 Brostoff and Sasse from Real User Corporation proposed a new graphical authentication scheme that is called Pass face algorithm According to Real User Corporation: The science behind pass-faces, (June 2004), Pass-faces is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces.

Greg Blonder introduced an early recall-based graphical password approach in 1996. In the approach that is builds on Blonders idea, a user create a password by clicking on several locations on an image. To login the user must click on previously selected locations on the image or close to those locations. Major problem this scheme faced with is that the number of predefined click areas is relatively small so the password had to be quite long to be secure. In addition, the usage of predefined click areas required simple and plain images, instead of complex, real world and crowded scenes.

In 2002, Pass logix Inc. Company developed a new graphical authentication scheme called Passlogix v-Go algorithm. At registration phase, the password is created by a chronological situation with repeating a sequence of actions. In this method user is required to click on various items on the image in the correct sequence in order to be authenticated. One drawback is that this technique provides only a limited password space, therefore causing the password to be kind of guessable or predictable.

In 2005 Wiedenbeck et al. proposed a new graphical authentication scheme called PassPoint algorithm. During the registration, the user is required to click on several locations on an image. At authentication phase, the user has to click on previously selected locations on the image or close to those locations. This method covers the limitations of Blonder algorithm because the images that are used for this method should be rich enough, complex and crowded. Any pixel in the image is a candidate for a click point so there are thousands of possible memorable points and combinations. One drawback is that it takes more time to input the password than text-based password users spend.

Today, there is a growing interest in graphical passwords but most of the graphical password authentication schemes have not been widely adopted.

Security

Security is a primary goal and the main requirement for any user authentication mechanism. There are lot of strategies use in attacking of systems. Unfortunately, no system offers the perfect security; therefore, there is need to evaluated systems according to their vulnerabilities and susceptibility to different attacks. According to Ahmad (2011), there are various types of attacks against systems, such as:

3. METHODOLOGY

The proposed system is designed using the waterfall model. This model has six main phases, which are requirements analysis, system design, implementation, testing, development and maintenance.

In the proposed system, the following will take place:

1. Users will be required to fill a registration form with required details.
2. Next, users would be required to set password for first level, second level and third level subsequently.
3. After the passwords are set for the three level, users can now login into the system.
4. While login the system will ask for the first level password. On entering the password correctly, the second level password is asked and then third one.
5. After the user has provided the correct password in the third level, he is authenticated and can now access the system.

a. System Architecture

The system architecture in two phase: 1) Registration phase 2) Login Phase

1. **Registration Phase**: In the registration phase in Figure 1, the user should provide user's details like user name and user conventional textual password, which is as strong as much and difficult to guess. This will protect the system from attacker. User have to register with his/her email address and textual password for validation phase of authentication. At pattern-lock level, the security has been imposed using patterns, where the user will be asked to select a colour combination patterns as difficulty level, which is unique for each individual user. After the two levels in registration, the next level is to register the user-preferred image, which the system will then cropped and codded to secure the image. On successful completion of the registration process, all the data about the users is then stored in database for the purpose of authorized use of the system.
2. **Login Phase**: In this login process, user need to pass the entire three level authentication to authenticate. In the figure 2, user need to provide the registered user name and password at text-based password authentication level, which is level 1. Then, user need to select the registered colour pattern-lock in level 2. In this level, the pattern is unique to each user. After the system verifies all the above levels, the system will display the registered user image in an already cropped format that is segmented into nine layers and the user is required to rearrange the cropped image by clicking on each segmented layer with the original image arrangement.

Each of the Nine segmented layer appears in coded format as the user click on it, once the image is successfully rearranged, the system verifies it and if okay, the system authenticate by granting the user access to the database.

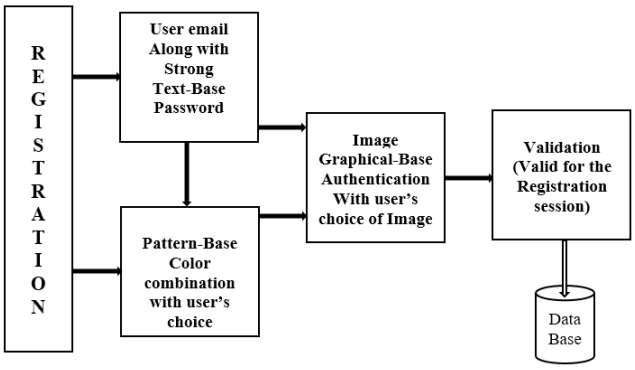

Figure 1: Block Diagram of Registration Phase for Proposed System

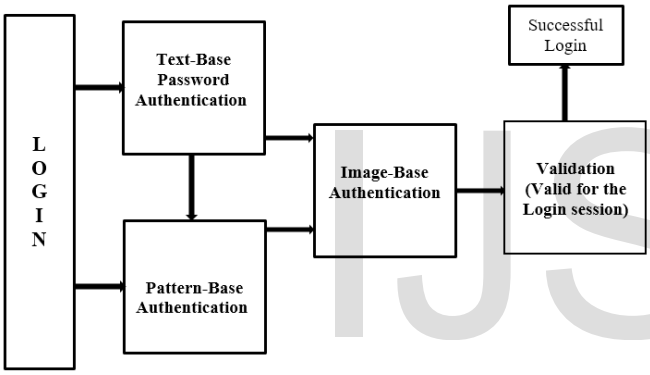

Figure 2: Block Diagram of Login Phase System for Proposed System

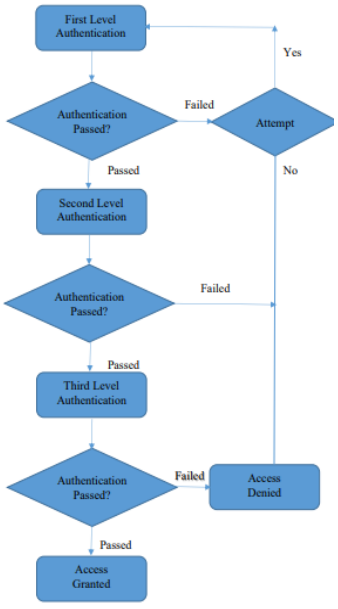

Figure 3: Flow Diagram of the Proposed Secure 3-level Authentication

Existing System Architecture VS Proposed Architecture

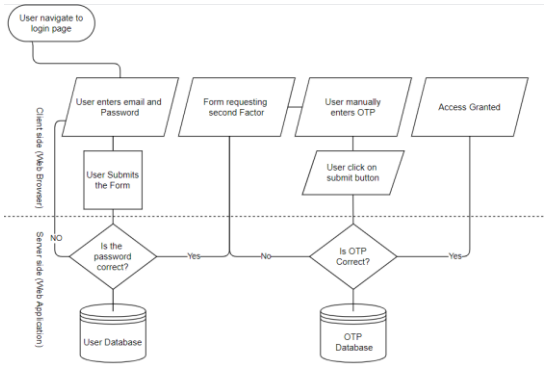

Figure 4: Existing System Architecture

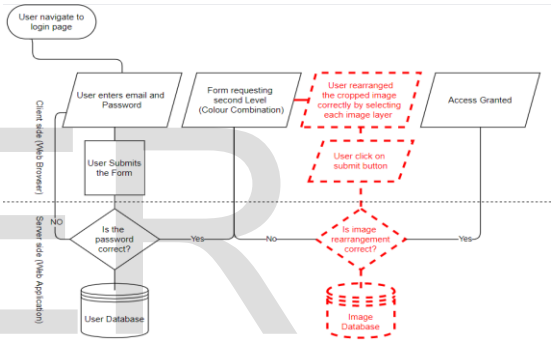

Figure 5: Proposed System Architecture

4. RESULTS

The result of this work is discussed under the following headings:

a. System Implementation

The Project is loaded in Visual XAMPP Server & Notepad++. We used that software's for Design and coding of the project. Created and maintained all databases into My SQL, in that we create tables, write query for data storage or record of project.

b. System Requirements

Hardware is the physical components that makes up a complete personal computer. It refers to the physical interface of the component that can be, felt, seen and touch.

Software is a program used by computers to facilitate their operations and utilization. It gives the computer the capacity of doing whatever the user wants. A computer without software is like an empty box. Software can be of two types; namely

1. System software
2. Application software

The system software is a program written by manufacturer to create an interface for the user. It creates a communication session between the hardware and the user, this software has no limited requirement since it is platform independent. It can run on any vendor's operating system. The application software also known as a user program is developed to help provide a particular solution to a problem.

a. Hardware Requirements:

For the systems to run properly, the following hardware is required:

1. i3 Processor Based Computer or higher
2. Memory: 1 GB
3. Hard Drive: 50 GB
4. Monitor
5. Internet Connection

c. Software Requirement:

For the Three Level Image Password Authentication to run properly, the following software is required

1. Windows 7 or higher
2. WAMP Server
3. Notepad++
4. My SQL 5.6
5. Web Browser

d. Choice of Development Environment

As earlier noted PHP, programming language would be used for this project. PHP started out as a small open source project that evolved as more and more people found out how useful it was. Rasmus Lerdorf unleashed the first version of PHP way back in 1994.

e. System Testing and Evaluation

As the project is on bit large scale, we always need testing to make it successful. If each components work properly in all respect and gives desired output for all kind of inputs then the project is said to be successful. Therefore, the conclusion is-to make the project successful, it needs to be tested.

The testing done here was System Testing checking whether the user requirements were satisfied. The code for the new system has been written completely using PHP as the coding language, Notepad++ as the interface for front-end designing. The new system has been tested well with the help of the users and all the applications have been verified from every nook and corner of the user.

Although some applications were found to be erroneous, these applications have been corrected before being implemented. The flow of the forms has been found to be very much in accordance with the actual flow of data.

f. Screenshots of Output

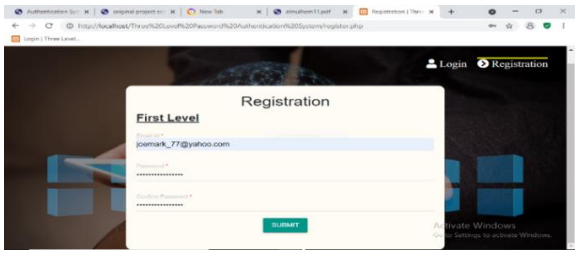

Figure 4: First Level registration with your email and text-based password

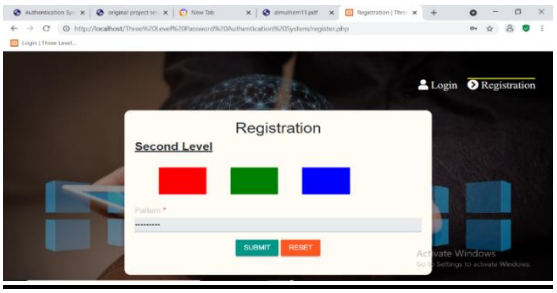

Figure 5: Second Level registration choosing desired colour Pattern combination

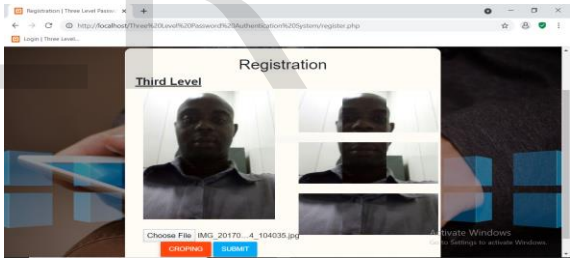

Figure 6: Third Level registration uploading desired Image Pattern for Cropping

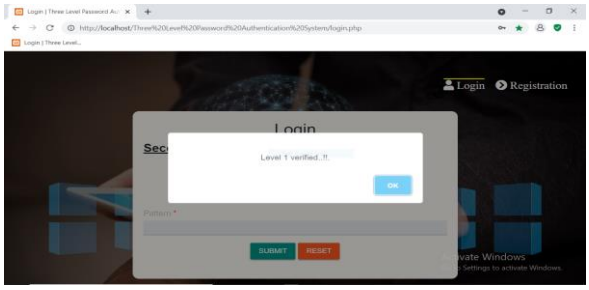

Figure 7: First Level Authentication Verified

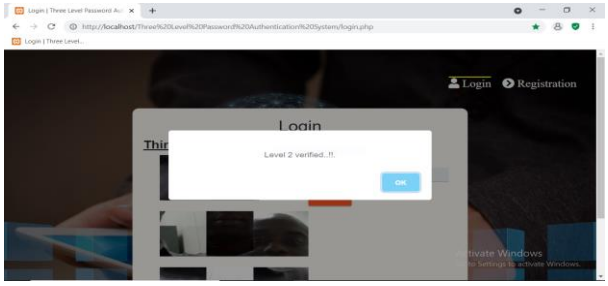

Figure 8: Second Level Authentication Verified

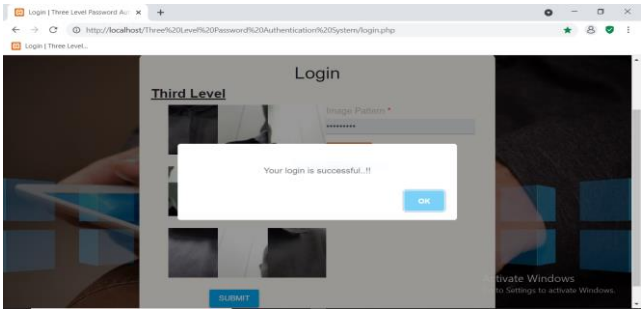

Figure 9: Third Level Authentication Verified and Login successful

5. CONCLUSION

The three level security approach applied on the above system, makes it highly secure along with being more user friendly. This system will definitely help thwarting Shoulder attack, Tempest attack and brute-force attack at the client side.

Three-Level Security system is definitely a time consuming approach, as the user has to traverse through the three levels of security, and will need to refer to his email-id for the one-time automated generated password. Therefore, this system cannot be a suitable solution for general security purposes, where time complexity will be an issue. However, will definitely be a benefit in areas where high security is the main issue, and time complexity is secondary, as an example we can take the case of a firm where this system will be accessible only to some higher designation-holding people, who need to store and maintain their crucial and confidential data secure. In near future not only we will add more features but also make our system customizable.

The security of both personal and corporate information cannot be over emphasize, as cyber insecurity increases due to activities of cyber criminals, it is a welcome development for IT professionals and software developers to also step-up their game through continues improvement on existing information security software's. I therefore recommend that this new system be adopted into organizations because it will further enhance the security of their information's and by using it, if there is any gray area in the system that was not captured by the developer, it will be pointed out for future work hence promoting continues improvement.

6. ACKNOWLEDGMENT

Special gratitude goes to my project supervisors Dr. (Mrs.) Ugochi A. Okengwu for working with me to ensure that this work met the academic requirements of the university. In addition, I will not fail to express my appreciation to the Centre Director and all staff of Port Harcourt Study National

REFERENCES

[1] Ahmad Almulhem (2011) Computer Engineering Department King Fahd University of Petroleum and Minerals Dhahran, Saudi Arabia: A Graphical Password Authentication System.

[2] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152, July 2005.

[3] Babich, A, 2012, Biometric Authentication, Type of Biometric Identifier

[4] Cynthia Kuo, Sasha Romanosky, Lorrie Faith Cranor; 2006; Human Selection of Mnemonic Phrase-based Passwords

[5] De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability study of two-factor authentication. arXiv preprint arXiv:1309.5344.

[6] Dimitriadis, C. K., & CISA, C. (2007). Analyzing the security of Internet banking authentication mechanisms. Information systems control journal, 3, and 34.

[7] Gayathiri Charathsandran, 2012, Text Password Survey: Transition from First Generation to Second Generation

[8] G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.

[9] Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

[10] H. Gao, X. Liu and R. Dai, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on\ Innovative Computing, Information and Control, Dec. 2009, page. 675-678.

[11] Jiangshan Yu, Guilin Wang, Yi Mu, Wei Gao: An Efficient Generic Framework for Three-Factor Authentication With Provably Secure Instantiation. IEEE Trans. Inf. Forensics Secur. 9(12): 2302-2313 (2014)

[12] Lackey, A. E., Pandey, T., Moshiri, M., Lalwani, N., Lall, C., & Bhargava, P. (2014). Productivity, part 2: cloud storage, remote meeting tools, screencasting, speech recognition software, password managers, and online data backup. Journal of the American College of Radiology, 11(6), 580-588.

[13] Li, Z., He, W., Akhawe, D., & Song, D. (2014). The emperor's new password manager: Security analysis of web-based password managers. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (page. 465-479).

[14] Mahboob, A., & Ikram, N. (2004). Transport Layer Security (TLS)–A Network Security Protocol for E-commerce. Technocrat PNEC Research Journal, 1, 2004.

[15] Mannan, M. A. (2009). Authentication and securing personal information in an untrusted internet (Doctoral dissertation, Carleton University).

[16] Mughele Ese Sophia, 2015, Three – Level Password Authentication

[17] Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015, April). Two-factor authentication: is the world ready? Quantifying 2FA

adoption. In Proceedings of the eighth European workshop on system security (page. 1-7).

[18] Priti Jadhao, Lalit Dole; 2013; Survey on Authenticate Password Technique

[19] Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. World Applied Sciences Journal, 19(4), 439-444.

[20] Rauti, S., & Leppänen, V. (2014). Man-in-the-browser attacks in modern web browsers. In Emerging Trends in ICT Security (pp. 469-480). Morgan Kaufmann.

[21] Real User Corporation. The science behind passfaces, June 2004.

[22] Salikka A/P EH TIP, 2017. Implementation of Security System By Using 3-Level Authentication

[23] Sumitra, B., Pethuru, C. R., & Misbahuddin, M. (2014). A survey of cloud authentication attacks and solution approaches. Int. J. Innov. Res. Comput. Commun. Eng, 2(10), 6245-6253.

[24] Weining Yang, Ninghui Li, Omar Chowdhury, Aiping Xiong, Robert W. Proctor; 2016; An Empirical Study of Mnemonic Sentence-based Password Generation Strategies

[25] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463–472, 2005.