MULTIFACTOR AUTHENTICATION FOR ONLINE SHOPPING SYSTEM

Muhammad Syazwan Nadzmi Bin Mohd Salwazi
University Kuala Lumpur
Malaysia Institute of Information Technology
Kuala Lumpur, Malaysia
syazwan.salwazi@s.unikl.edu.my

Amna Binti Saad
University Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
amna@unikl.edu.my

***Abstract*— In this project, a multifactor authentication system was integrated with an online store. Digital and computer security are now crucial for safeguarding user data. One threat is shoulder surfing [10], in which a criminal can steal a password by watching directly or by videotaping the authentication process. There are several methods for this authentication, with the multifactor authentication method being the most common and simple. Therefore, a novel strategy is proposed to address this issue, namely the development of multiple layers of system security through the use of multifactor authentications. Text, colour, and graphical representations are the three types of multifactor authentication that are used. At the conclusion of this project, an online shopping system is created to evaluate the effectiveness of the algorithm.**

Keywords—Cybersecurity, Multifactor Authentication, Website

I. INTRODUCTION

In recent years, technological advancements have resulted in the rapid digitalization of society, with everything taking place on the Internet at an increasing rate. Most users prefer to pay online, whether for bills, tickets, or paying the person next to them. In addition to payments, all activities, such as communication through email and messaging apps, keeping their documents in a digital locker, etc., happen online. As a result, there is a growing risk of cybercrime and privacy breaches since everything is done online. Online and offline platforms rely heavily on passwords to keep their data secure. For accessing accounts, passwords are used as the default method of authentication.

Alphanumeric passwords are either difficult to remember or easy to guess compared to traditional username-password authentication. Moreover, since many passwords are difficult to remember, users tend to use the same one for all their accounts. These problems associated with the traditional username-password authentication technique can be overcome by using alternative authentication methods, such as biometrics or graphical passwords. A graphical password authentication system user picks images from a graphic user interface (GUI) presented in a specific order.

Compared with alphanumeric characters, pictures are more accessible for the human brain to recall. Therefore, the advantage of graphical passwords outweighs the disadvantage of alphanumeric passwords.

According to how they authenticate passwords, multifactor authentication falls into two main categories [6]:

User identification based on recognition: When registering, a user is given a set of images to select from. As an example, pass faces use graphical passwords to recognize human faces. When creating a password, the user can choose from many images. The user must identify the pre-selected image from several images before he can log in.

Users are asked to reproduce something they created or selected at the registration stage through recall-based authentication. For example, a user can create a password by clicking any point in an image, and a tolerance around every pixel is calculated. As part of the authentication process, the user must select the points within the tolerance in the correct sequence to log in.

The rest of this paper is organized as follows: Section II reviews existing literature on related works by other researchers, Section III gives detail of the methodology, the result is provided in Section IV. Section V contains the conclusion.

II. RELATED WORK

This chapter includes a variety of study subjects related to this project. Existing literature must be analyzed by summarizing, interpreting, and critically analyzing the current field of research or body of knowledge. This discussion will focus on the technology and tools employed in this project. The researcher must understand which investigation components can be overlooked and still yield the desired results. This chapter will focus mostly on the methods and technologies being developed and integrated into the planned system.

A. Three-Level Authentication

The three level authentication combines the existing text-based password, pattern lock password/graphical, and one-time password schemes for increased security [1].

1. Text-Based Password Technique

   Text-based passwords are used as the first authentication level. It is prevalent for computer users to identify themselves through textual passwords due to their ease of use. Since its introduction four decades ago, this system has been popular because of its simplicity of

operation, cost-effectiveness, familiarity, and ease of operation. The text password is a (memo metrics) text-based technique. The user used them to log into the system as a shared secret by typing alphanumeric and special keyboard characters. Users must register their user ID and text password at this level. In addition to numbers, letters, and other special characters, the password can also contain symbols. Users must re-enter the information chosen at registration to log in. There are multiple text-based passwords, including alphanumeric and mnemonic passwords. According to the study articles, six alphanumeric passwords were initially used in the 1960s to protect secret data. An alphanumeric password, the passwords are as follows[2]:

- Password should be at least eight characters long.
- The password is not related to a user.
- Users should use upper and lower case, numbers and special characters.

2. Colour Code Technique

In order to go to the next stage, users will need to input the colour code they choose during the registration process. There are three colours, and the user must select any three colours in a specific order [11]. At the end of the session, the user must enter the same code again in the same order each time they log in. The user must memorize the code to pass the security check because the colours will always appear randomly. There are 120 possible colour combinations, so entering the same combination often won't work. Once the user has entered the proper sequence, they will only have one chance to complete it, and they will be sent back to the login page if the pattern does not match [3].

3. Graphical Password Technique

The authentication technique for graphical passwords consists of two independent components: Password enrollment and verification are the first two steps in the password enrollment process. During registration, the user selects a theme that determines the thumbnails used during registration and then registers a sequence of thumbnails that correspond to the related password. The user must enter the enrolled image sequence for verification as soon as the device is powered on or booted [4]. After successful login, users can change their password by choosing a new sequence and theme. The display interface provides images in a size that is simple to pick, hence reducing input errors. The fundamental mechanism that controls randomness. Picture Password offers users the option of selecting a predetermined theme that matches their personality or creating their own choice of photographs to be shown [8]. All thumbnail photos must be in a present digital format, which can be made with Photoshop or GIMP. In addition to a random arrangement of individual thumbnail photos, many thumbnail images may be arranged to create a single composite image, similar to a mosaic, where each thumbnail image contributes a portion to a bigger image [9].

III. Research Methodology

According to the Oxford Dictionary, methodology is a system of methods used to investigate the concept of the ones in a particular area, study, or activity. A project methodology is a method for designing, planning, implementing, and achieving a project's objectives. This project requires planning strategies to run each task, and it is essential to know the process. In addition, it allows for effective decision-making and problem-solving throughout the project management process.

Using Agile software development techniques is one of the simplest and most efficient ways to translate business needs into software solutions. Several characteristics of agile software development methods include continuous planning, learning, improvement, collaborative teamwork, and evolutionary development. In addition, the ability to adapt to change is also promoted, as well as the facilitation of the change process itself.

A. Flowchart

In computing, a flowchart represents a method, system, or algorithm. They are commonly used in many fields to document, study, plan, improve, and often communicate complex processes in clear, understandable diagrams.

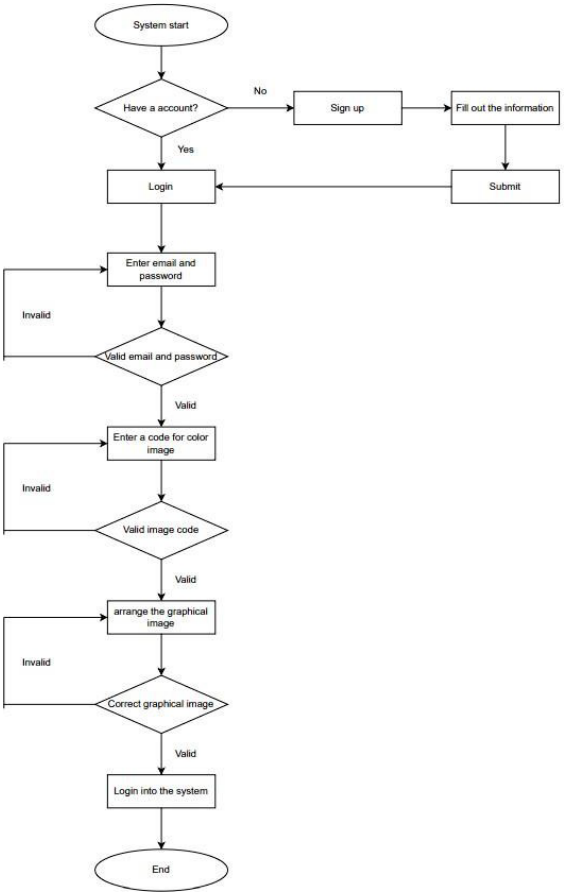

Figure 1: Flowchart for Login

B. Logical Diagram (Use Case Diagram)

Use case diagrams are the primary method of identifying system/software requirements for newly developed software programs. The expected behavior (what) is specified in use cases, not the exact method of achieving that behavior (how).

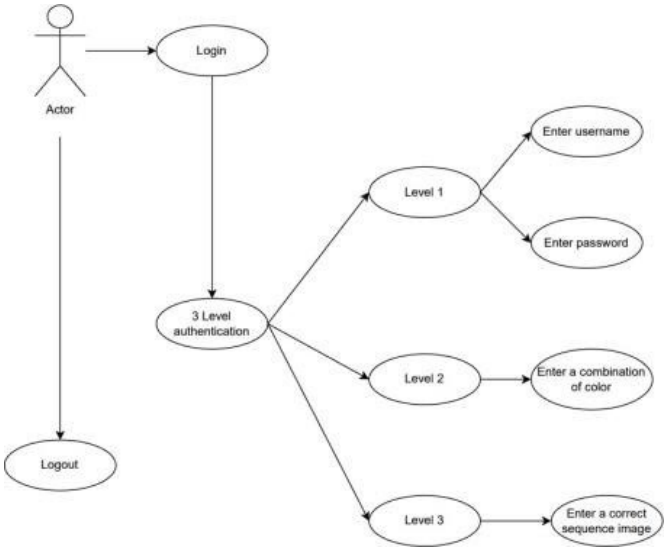

Figure 2: Use Case Diagram

IV. RESULT AND TESTING

In this chapter, testing and results will be fully described and explained. It will include an explanation of system testing, system functionality testing, security testing, and overall testing. Testing and result are important elements before the developer can publish to the public use for them to use the system or the software.

Table 1: Script Insertion

SQL Injection (Script Insertion)	
Description	To test the SQL Injection for Script Insertion vulnerability at the login page.
Precondition	Users need to have access to the input box in the web browser (username and password)
Input definition	• Insert script (‘ OR ‘1’=1) in the username and password box. • Insert script (‘ OR ‘1’=’1--) in the username and password box.
Expected result	User cannot get access to the account.

Table 2: Brute Force Attack

Broken Authentication (Brute Force Attack)	
Description	To test the strength of passwords in Online Shopping Systems by doing brute force attacks using the burp suite community edition.
Precondition	Setup proxy with port 8080 at burp suite community edition.
Input definition	Password that the user wants to use must contain a combination character (e.g., a – z, A – Z, 0 – 9, and a special character).
Expected result	A complex password prevented the payload from guessing and brute-forcing the password.

Table 3: Anti – CSRF Token

Broken Authentication (Anti – CSRF Token)	
Description	By using a csrf token, developer cannot prevent attackers from gaining access to an account by stealing the token or generating an unpredictable token.
Precondition	User password (text-based, colour code, and graphical)
Input definition	• A user enters the information at first authentication. • The user enters the information at the second authentication. • Users enter the information at third authentication.
Expected result	Attacker cannot use another token except the csrf token that generates at the first session.

Table 4: Encryption

Sensitive Data Exposure (Encryption)	
Description	By encrypting the database, users are guaranteed that their data is protected from unauthorized access. As a result, attackers or malware would not be able to access sensitive information until they gain access to the database.
Precondition	User password (text-based, colour code, and graphical)
Input definition	• The user clicks the “Register” button. • The user enters all the information needed. • The user opens the pickle file that contains the database for the users.
Expected Result	Users will see an encrypted password, not in plain text.

V. CONCLUSION

In the past ten years, there has been an increase in interest in switching from text-based passwords to other authentication methods, such as graphical passwords. We conduct a thorough online survey of the current authentication methods as part of this project. The main defense of colour-coded and graphical passwords is that they are simpler to remember than text-based passwords, but there are few user studies that provide strong evidence for this claim. Using multiple authentications makes it more challenging to crack using conventional attack techniques like brute force attacks, dictionary attacks, and spyware, according to research by Sayli Chavan et al. [7]. Next, we review and assess the success of our project objectives:

A. Review of Research Objectives

1. Objective 1

   Studying how text-based passwords, colour-code, and graphical passwords work can help users improve their security levels. The objective is achieved whereby the combination of text-based passwords, colour codes, and graphics that can help secure the system are studied.

2. Objective 2

   To develop the layer of system security by implementing more than one-factor authentication. The objective is achieved. The development of an online shopping system is completed at the end of this project. Three types of multifactor authentication are applied [5].

3. Objective 3

   To implement another type of authentication that can be used in the system to ensure that it is compatible with current technology. The objective is achieved. A colour code and graphical password are implemented as another type of authentication.

B. Recommendation

It is advised to add a few more features to this system for improvement:

1. Use a user interface to implement graphical password authentication.
2. Using graphical password authentication is advised because it is simpler to remember, more practical, and more secure than conventional authentication techniques.
3. To increase the system's level of authentication so that big businesses can use it to protect their systems because it is more economical and secure.
4. It is suggested that the following researcher also include some colour recognition in addition to improving the image marking pattern.
5. Multifactor authentication will be globally useful once it is integrated into software, databases, and applications.

ACKNOWLEDGMENT

All glory belongs to the All-Powerful, Compassionate, and Merciful Allah. This study is a component of the undergraduate capstone project for the University of Kuala Lumpur. The author wants to thank his parents, other family members, friends, and everyone else who has supported him in making this small project a success.

REFERENCES

[1] Ese, M. (2015). THREE -LEVEL PASSWORD AUTHENTICATION. European Journal of Computer Science and Information Technology

[2] M. Manjunath, K. Ishthaq Ahamed & Suchitra. Security Implementation of Security System Using 3 – Level Authentication. European Journal of Computer Science and Information Technology

[3] Kamble, N., & Dharani, J. (n.d.). Implementation of Security System Using 3-Level Authentication. In IJEDR1402039 International Journal of Engineering Development and Research

[4] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., & Swanstrom, R. (n.d.). Picture Password: A Visual Login Technique for Mobile Devices

[5] Partheeban, N. (2020). THREE LEVEL PASSWORD AUTHENTICATION SYSTEM 1 RAHUL CHOURASIA, 2. International Journal of Creative Research Thoughts

[6] B. O. ALSaleem and A. I. Alshoshan, "Multifactor Authentication to Systems Login," 2021 National Computing Colleges Conference (NCCC)

[7] Sayli Chavan, Shardul Gaikwad, Prathama Parab, Govind Wakure; Graphical Password Authentication System

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

[9] Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-points.

[10] Chen, Y. L., Ku, W. C., Yeh, Y. C., & Liao, D. M. (2013, February). A simple text-based shoulder surfing resistant graphical password scheme. In *2013 International Symposium on Next-Generation Electronics* (pp. 161-164). IEEE.

[11] S. R. Bandre, "Design and implementation of smartphone authentication system based on Color-Code," 2015 International Conference on Pervasive Computing (ICPC), 2015