BIOMETRIC IRIS RECOGNITION AND TWO-FACTOR AUTHENTICATION FOR LOGIN SYSTEM

Noor Shakirin Binti Shaari
Malaysian Institute of Information Technology
Universiti Kuala Lumpur
50250 Kuala Lumpur
MalaysiaShakirin.shaari@s.unikl.edu.my

Dalilah Binti Abdullah
Malaysian Institute of Information Technology
Universiti Kuala Lumpur
50250 Kuala Lumpur
Malaysiadalilah@unikl.edu.my

ABSTRACT- Traditional username and password authentication were easily compromised and had caused a breach of data. Research shows that two-factor authentication and biometrics applied to web systems is a more secure method compared to the traditional username and password when used appropriately. The project was to implement a secure login authentication mechanism for the inventory system in two different environments, the desktop environment, and the mobile browser environment. The stated mechanism is biometric iris detection and two-step authentication using one-time password (OTP).

KEYWORDS- *Authentication; Iris detection; Two-factor authentication; One-time password*

I. INTRODUCTION

Authentication is one of the most important parts of any system. Appreciated as the first and the last line of defenses in the majority of cases, authentication systems can usually prevent the kleptomaniac from unauthorized accessing users' data. With the rapid development of the Internet and mobile devices, authentication systems have been widely used in Internet service access and mobile device access for protecting user devices, contents, and accounts [1].

Today, users and operators can exploit technologies to share and adjust confidential data from a long-distance or to execute critical commands in real-time. Traditionally, users' authentication is based on pairs of username and password and performed as a single-occurrence process, only at the login phase. The used of username and password can be compromised and had caused a breach of data in the system.

The purpose of this research project is to study the mechanism of secure system login for the inventory system. The secure mechanism of system login is designed to minimize the damages that result from the repudiation. There were two main designs in the project, the first part is user login using biometric iris detection and the second part is user login using two-factor authentication by one-time password (OTP). Biometric iris detection was designed to be used in the desktop environment while two-factor authentication using one-time password (OTP) was designed to be used in the mobile browser environment.

II. LITERATURE REVIEW

The traditional text-based password is still used in many websites and applications which are vulnerable to different kinds of attacks. Biometrics is a great approach to be used in the validation of users in a web system because the cost to forge any physical or behavioral human trait is too high. The study stated that two-factor authentication and biometrics applied to web systems is a more secure method compared to the traditional username and password when used appropriately [2].

A. Biometric iris detection framework

The study states that the iris recognition system is made up of various steps, which are also known as stages in the personal authentication or recognition process [3]. The stages consist of four stages which are segmentation, normalization, feature extraction and template matcher. The segmentation or iris localization process is the first stage. In this stage, the iris area is segmented or segregated from the eye by completing a pupil separation procedure and then roughly determining two circular borders, the pupillary or inner border and the sclera or outer border.

The second stage is the normalization method, which transforms the segmented iris area to have fixed dimensions, making feature extraction and matching easier. Inconsistencies in the segmented iris region's proportions across eye images are related to its functionality, for example, the size alteration to let light into the eye, resulting in pupil dilation. As a result of the normalization method, any two isolated iris regions with constant dimensions will have the same spatially located features.

The final stages in the system are the feature extraction and the iris template matching stage. A biometric template is developed at the end of the feature extraction stage, which is subsequently used for template matching. An iris code, an iris signature, or a decision tree could all be

biometric templates. These templates are then matched using one of several available matching procedures, which aids in determining the degree of resemblance between two separate iris templates. When two different templates belonging to the same eye are matched, a range of values known as "intra class variations" results. Additionally, when the templates come from different eyes, the range of values is referred to as "inter class variations." Based on these two variations, it is possible to determine if the templates belong to a sane or two separate iris or irises [3].

B. Two-factor authentication using one-time password (OTP)

The research has showed that two-factor authentication solutions are separated into two categories, tokens that are supplied to customers to use when logging in and infrastructure or software that detects and authenticates access for users who use their tokens correctly. Authentication tokens can be found in software in the form of mobile or desktop programs that produce personal identification number (PIN) for authentication. These authentication codes, also known as one-time passwords (OTP), are often produced by a server and may be verified by an authentication device or app [4].

One Time Passwords based on Short Message Service (SMS) is the most basic approach for producing one-time codes [5]. In this technique, the one-time code is created on the server and communicated over the network by SMS to the registered mobile number. Authentication happens when the server recognizes that the user has entered a valid login code. The user's phone number must be registered with the provider that offers SMS OTP for authentication. When a user attempts to connect to his account using a username and password, the user will receive a unique code on his phone number, which he must enter to gain access to his account. The OTP can be delivered to the user through text message or by an automated call via text-to-speech conversion. Furthermore, OTP is limited to a very short length of time and will expire automatically [5].

III. PROPOSED METHODOLOGY

The main objectives of the project are to study the mechanism of secure system login for the inventory system and to design a secure mechanism of system login to minimize the damages that result from the repudiation. There were two main parts in the project, the first part is user login using biometric iris detection and the second part is user login using two-factor authentication. Biometric iris detection designed to be used in the desktop environment while two-factor authentication using one-time password (OTP) was designed to be used in the mobile environment. For the first part which is biometric iris detection, the module was developed by using Python language in an integrated development environment named PyCharm. The second part which is two-factor authentication using one- time password (OTP), the module was developed by using Twilio cloud API, Database Management System, MySQL. The language was all integrated into one web server entitled Xampp Server.

A. Block diagram

The figure below shows the block diagram process of image acquisition in iris detection. During the enrolment process, there were four stages before the image went to a database. The four stages stated were segmentation, normalization, feature extraction and enrolment. In the segmentation stage, the iris area is segmented or segregated from the eye by completing a pupil separation procedure and then roughly determining two circular borders, the pupillary or inner border and the sclera or outer border. The second stage is the normalization method, which transforms the segmented iris area to have fixed dimensions, making feature extraction and matching easier. The final stages in the system are the feature extraction and the enrolment iris template matching stage. A biometric template is developed at the end of the feature extraction stage, which is subsequently used for template matching. These templates are then matched using one of several available matching procedures, which aids in determining the degree of resemblance between two separate iris templates. The extracted features then sent to the database. During the verification process, all three stages were the same as the enrolment process except the last stage was the comparison of the iris stored in the database.

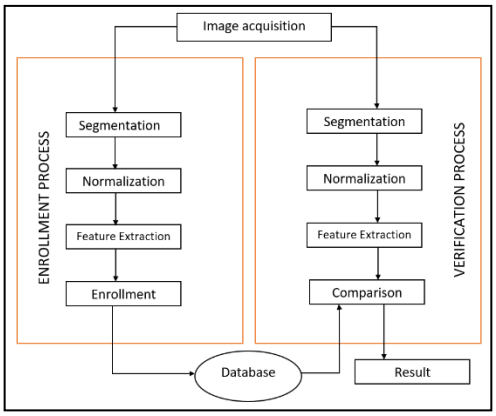

Fig 1: Block Diagram of Iris detection

B. System Architecture

The Figure 2 below shows the architecture of 2FA using SMS-based OTP for mobile browser environment. During the login process, the user has to insert their registered username and password that were stored in the database. If the username and password were not valid it will revert to the login page. If the username and password were valid, the web server will prompt for OTP to service API which is the Twilio service. Twilio API service will send the OTP which is six digits code to the user's registered phone number. In this process, a user has to insert a valid OTP code for successful authentication. Failed authentication due to invalid OTP code will revert the process to the login phase of username and password.

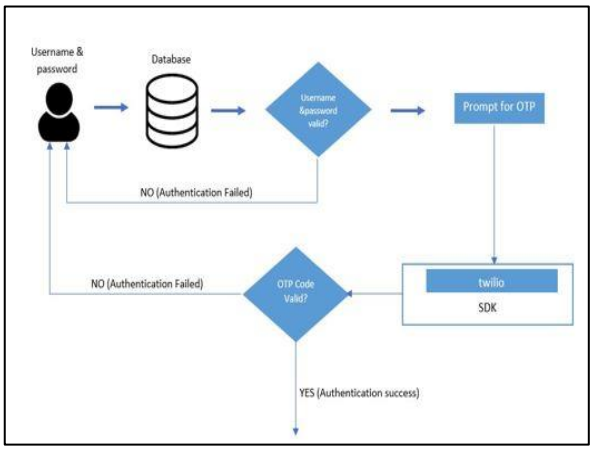

Fig 2: System Architecture of 2FA

IV. RESULT AND DISCUSSION

The testing is executed to determine each function of a system by giving adequate input and comparing the output to the functional requirements. This testing checks the user interface, APIs, database, security, client-server communication and other functionality of the application under test. For biometric iris detection the testing consists of two parts which is user registration and user verification in desktop environment. For two-factor authentication using OTP in mobile browser environment consists of login authentication and OTP code authentication

A. User's registration for iris detection

The system will automatically detect the user's eye and captured it when a user clicked the register button as shown in figure 3 below. To get an accurate result of the data captured, the user must not wear any type of glasses or any contact lens. As the user clicks on the register button, a box of the registration form will appear so that the user can insert the ID number, name, age and gender. The captured iris and the information inserted will be stored in the database.

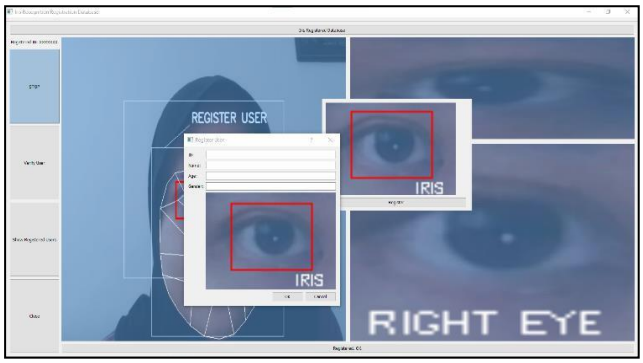

Fig 3: user registration

B. User verification for iris detection

For verification process, a panel of the face and eye detection will capture the user's face and eye. When the verify button is clicked by the user, the user needs to insert the correct ID number so that the user's information panel will pop out for verified iris as shown in figure 4 and 5 below.

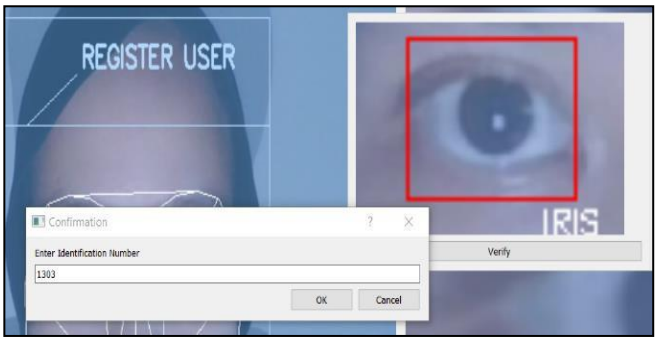

Fig 4: verify by ID Number

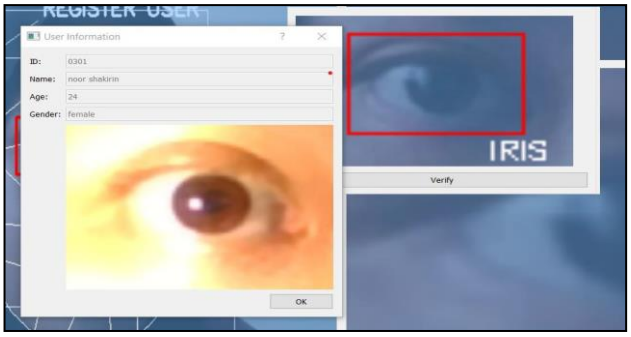

Fig 5: verified user

C. Login authentication

During login authentication a user needs to inserts the correct username and password for the OTP code to be sent to the registered phone number. As shown in figure 6, an OTP code were sent by cloud API service (Twilio) to the user's registered phone number.

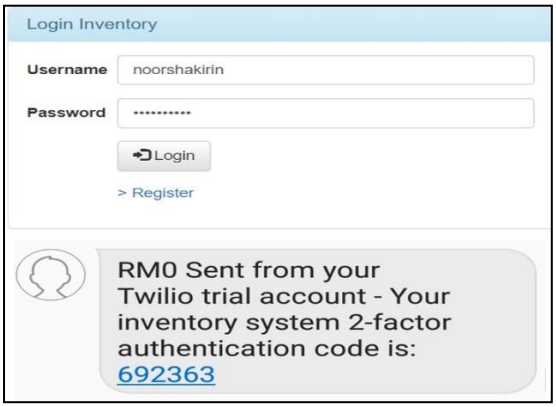

Fig 6: verified user

D. OTP code authentication

The cloud API service (Twilio) were integrated with the inventory system. Cloud API service (Twilio) received a request to send the OTP code to the registered phone number in the database. When the user inserts the correct username and password it will be directed to the OTP authentication page for the user to insert the six digits code as shown in figure 7.

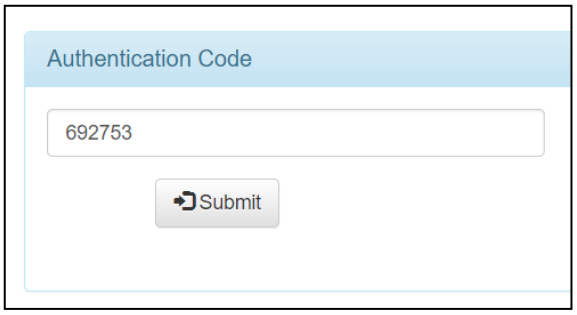

Fig 7: OTP authentication code

E. Functional testing results

Based on the results of the functional testing of biometric iris detection and two-factor authentication, the analysis concludes that the application performed under the design specifications and project objectives. The result of the testing applied to the system has shown to be successful except for the integration of biometric iris detection with the inventory system. The system was failed to integrate with the inventory system as it should be. The system still in need of improvement so that it can be the best and successful system. Table 1 and Table 2 below lists the activities of biometric iris detection and two-factor authentication respectively, that have been carried out in response to the outcome

TABLE I. 2FA USING OTP FUNCTIONAL TESTING

Description	Expected result	Actual result	Remarks
User registration for iris.	A panel of the face and eye detection will capture the user's face and eye.	The user's face and eye detected by the system. User cannot wear glasses to pass the result.	PASS
User verification for iris.	A panel of the face and eye detection will verify the user's face and eye. The user information panel will pop out for verified iris.	The user information panel pop out when the user is verified.	PASS
Different iris verification for a different ID number.	A message of "iris does not match with database" will pop out.	The message pops out if a different user tried to enter a different ID number.	PASS
Face and iris verification using photo.	The system should be an error to detect the iris.	The iris cannot be detected by using photo.	PASS
Integrate to the inventory system.	A verified user's iris will be directed to log in to the inventory system.	The iris detection is not integrated into the inventory system.	FAIL

TABLE II. IRIS DETECTION FUNCTIONAL TESTING

Description	Expected Result	Actual Result	Remarks
User registration.	All user information data will be sent to the database.	PASS	All functions working well.
User login.	An OTP code will be sent to the user's registered phone number for matching username and password.	PASS	
OTP authentication submission.	A correct OTP code will prompt the user to the system dashboard	PASS	
Web server request and receive OTP code from cloud API (Twilio).	Cloud API (Twilio) received a request and sent the OTP code to the webserver.	PASS	

V. CONCLUSION

The project that was undertaken to develop a biometric iris detection and two-factor authentication login was for the inventory system. The necessary measures and processes were followed to guarantee that the project's development satisfied the project requirements as well as the purpose and objectives as defined earlier in the project. In a conclusion, the project developed considered to be functional well except there was only one limitation to the project. The modules are operating systematically, as the project met the initial purpose, objectives, and scopes established during the initial phases of the system development. During the development of biometric iris detection, the system was supposed to be integrated with the inventory system, however, there was a

problem that makes the system unable to be integrated. This flaw is hoped to be improved in future studies.

REFERENCES

[1] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification ", Telematics and Informatics, vol. 35, no. 5, pp. 1491–1511, Aug. 2018, doi: 10.1016/j.tele.2018.03.018.

[2] A. I. Silva, P. S. Neto, and N. P. Carvalho, "An application of biometrics in the web regarding health insurance", RECIIS, vol. 4, no. 5, Dec. 2010, doi: 10.3395/reciis.v4i5.333en

[3] Nithya, A. A., & Lakshmi, C. "Iris recognition techniques: a literature survey". International Journal of Applied Engineering Research, 10(12), 32525-32546,2015.

[4] "What is Two-Factor Authentication (2FA) and How Does It Work?", SearchSecurity. https://searchsecurity.techtarget.com/definition/two-factor- authentication (accessed Jun. 02, 2021).

[5] N. Kaur and M. Devgan, "A Comparative Analysis of Various Multistep Login Authentication Mechanisms", *IJCA*, vol. 127, no. 9, pp. 20–26, Oct. 2015, doi: 10.5120/ijca2015906472.

[6] Tellini, N., & Vargas, F. (n.d.). *"*Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a Digital Assessment Platform",2017.

[7] Singh, D., & Verma, A. "Inventory Management in Supply Chain. Materials Today": Proceedings, 5(2), 3867–3872, 2018. doi: 10.1016/j.matpr.2017.11.641.

[8] Silva, A. I., Neto, P. S., & Carvalho, N. P. "An application of biometrics in the web regarding health insurance". RECIIS, 4(5),2010. doi: 10.3395/reciis.v4i5.333en

[9] Schiavone, E., Ceccarelli, A., & Bondavalli, A. "Continuous Biometric Verification for Non-Repudiation of Remote Services". Proceedings of the 12th International Conference on Availability, Reliability and Security, 1–10, 2017. doi: 10.1145/3098954.3098969

[10] Rahman, A. S. A., & Masrom, S. "Non-repudiation in order, delivery and payment process for a sustainable online business". 2010 International Symposium on Information Technology, 1099–1103, 2010. doi:10.1109/ITSIM.2010.5561515