Smart Home Multi-Factor Authentication Using Face Recognition and One-Time Password on Smartphone

https://doi.org/10.3991/ijim.v15i24.25393

Tok Yen Xin, Norliza Katuk(✉), Ahmad Suki Che Mohamed Arif
Universiti Utara Malaysia, Kedah, Malaysia
k.norliza@uum.edu.my

Abstract—Recently, the adoption of smart home technology has been on the rise and becoming a trend for home residents. The development of Internet-of-Things (IoT) technology drives the smart home authentication system with biometric systems such as facial recognition, fingerprint, and voice control techniques. In the context of homeowners, security is always the primary concern. However, conventional home security and the existing smart home security system have some limitations. These techniques use single-factor authentication, which provides limited protection for home security. Therefore, this project proposed a design for smart home multi-factor authentication using facial recognition and a one-time password sent to smartphones for a home security system. Rapid application development was the methodology for conducting this study. A usability evaluation suggested that the proposed smart home multi-factor authentication is acceptable, but some usability issues can be improved in the future.

Keywords—security, biometric system, smart home, authentication, smartphones

1 Introduction

At present, smart home technology is increasingly gaining popularity among homeowners due to the features offered by the system [1, 2], including security protection and comfort. Moreover, it allows residents to remotely manage and control their houses [3, 4] using mobile devices such as smartphones and tablets [1]. Nevertheless, home security protection such as door locks and surveillance cameras is always the main priority for homeowners to ensure the residents' privacy and safety from intrusions. However, unlike smart home systems, the conventional door locking system such as key and padlock on the grill door has low-security protection [5]. It is also inconvenient and inefficient because the resident needs to use a physical key for every identification process. Moreover, the system can be compromised easily and thus increase the rate of home burglaries through doors and windows. In addition, the careless attitude of residents who do not close the door and windows when nobody is at home is also a safety threat. Thanks to smart home technology that can address the problems in conventional door locking.

Home authentication systems are one of the components in smart home technology that controls the residents' entrance to the house [1]. It comprises the authentication mechanism and door security system, which only allows the access of authorised residents [6]. The advances in Internet-of-Things (IoT) and cloud computing technologies have increased the maturity and usability of smart home technology to a reasonable level. A smart home authentication system includes smart cards, biometrics, passwords, and radio frequency identification (RFID) sensor [7]. The use of a biometric-based door lock is highly reliable because it identifies an individual using their biological characteristics. These characteristics are unique for every people and cannot be duplicated easily. Further, the security of the smart home authentication system can be increased by applying more than one authentication technique, which is called multi-factor authentication. For example, the prevalent use of smartphone technology [1, 8] can be utilised with biometric authentication to strengthen the security system. In addition, combining personal identification numbers (PINs) or passwords sent to residents' smartphones during the authentication process can provide higher security protection than the traditional lock.

Therefore, this study intends to propose and design a smart home multi-factor authentication system using face recognition and one-time password (OTP) sent to residents' smartphones. It is a multi-factor authentication system that can provide double protection to smart home residents by enhancing entrance control to their houses. First, the study identified the system's requirements and then developed a prototype to demonstrate the design. Finally, the prototype was tested for its usability. It works as a smart door system integrated with a microcontroller. Facial recognition technology is the primary authentication system, combined with OTP. The system is beneficial to home residents because it enhances home security to a large extent and improves the convenience for the smart home resident. Furthermore, it makes life easier as residents only need to scan the face and input the OTP for entering their house. Overall, the advancement in IoT on the smart home authentication system has impacted society in changing a better-quality lifestyle and improving the user experience on the home security system today.

2 Background and related studies

This section described the background of smart homes, biometric systems, and the OTP approach. Besides, the related studies investigated the implementation of face recognition systems in various areas. Smart home technology is also referred to as home automation, enabling the residents to manage their homes remotely through Internet-connected devices such as smartphones or tablets [1, 9]. The concept of a smart home was introduced by Nikola Tesla in 1898 with the invention of remote controls [10]. The first smart automation system was developed in 1966 that allowed users to create shopping lists and control room temperature and home appliances [10]. Today, the smart home is integrated with the IoT and cloud computing technology that could increase security. Therefore, it can provide home residents with a comfortable, convenient, secure, and high-quality home environment. The general idea of a smart home system [6] is demonstrated in Figure 1.

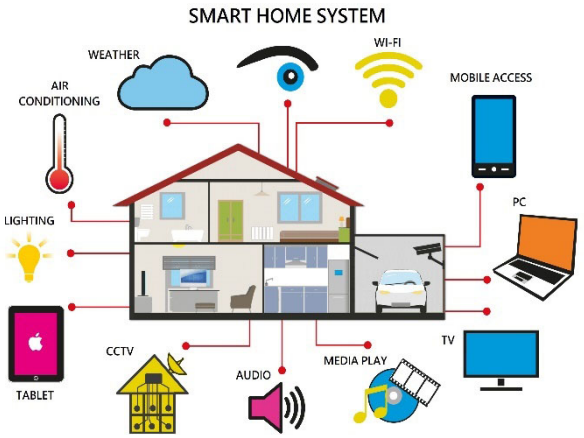

Fig. 1. The components of a smart home system [6]

Multi-factor authentication systems use biometric features with other types of authentications methods such as PINs, passwords, OTPs, and smartcards [11]. Biometrics can be categorised into two types, which are physiological biometrics and behavioural biometrics. The physiological biometric include face recognition, fingerprint, hand gesture, and deoxyribonucleic acids (DNA). On the other hand, behavioural biometrics include signature and voice recognition [12]. Fingerprint, facial recognition, and voice recognition would be the most familiar biometrics in our daily lives beyond the application of smart homes. For example, the banking sector used fingerprint recognition to increase the transaction security on the automated teller machine (ATM). Moreover, the biometric system is used along with the PIN to form double protection of smartphones. Other than PINs, OTPs are also frequently used in multi-factor authentication. It is a set of numerical or alphanumerical codes generated for every transaction or authentication and valid only once [13]. For example, OTP is often used in Android apps. A server generates a random number of OTP and sends it to the user's smartphone via a short message service (SMS) or push notification [14]. Developers suggest six OTP rules for secure implementation. First, the system must guarantee randomness in generating an OTP for authentication [15]. Second, it must generate at least six digits of the OTP. Third, the system must limit the attempts for OTP validation. Next, OTP is only used once for every authentication process. Then, OTP should only be valid for a limited time. The sixth rule is that the OTP value can be renewed if it expires. Finally, the OTP should be more reliable than the password to protect against replay attacks [14].

Facial recognition is gaining attention as an authentication method in various domains, including smart home environments, due to efficient recognition devices and algorithms. For example, Sandar and Oo [16] proposed a face-recognition door lock system using Raspberry Pi and GSM modules. The authentication process started when the camera detected and recognised the face. Then, the user must enter the password, and the correct password will unlock the door. On the other hand, if the incorrect passwords were input more than three times, the GSM module sends the alert message to the admin user. It also used the Haar cascade classifier for face detection because of the high detection accuracy. Furthermore, the local binary pattern histogram in OpenCV

was used for face recognition because it is more flexible to recognise the side face. It is an instance of multi-factor authentication that is more secure and suitable for homes, banks, or other public areas.

Manjunatha and Nagaraja [17] proposed a home security system using face recognition and an intruder detection system with automated alerts. The system captures an image of an intruder using a web camera and sends it to the homeowner through an email. At the same time, an SMS alert is sent to them. Utilising the intruder alert system with email and SMS makes the system more secure to protect the house from unauthorised people. The user can notice the intruder and react when they receive the notification immediately. Aishwarya [18] proposed an android based real-time smart door lock system with image detection and voice recognition. The system was integrated with IoT and used smartphones to control the door. First, the camera detects the face image and sends it to the user application for image verification. Then, the authorised voice command is used as an input to unlock the door. In addition, the OTP is generated and send to the registered mobile number for every registration process. In this system, the convolutional neural network of deep learning was implemented to train and recognise the images and the authorised user's voice. The multi-layered network increased the model accuracy during the recognition process. However, voice recognition would not be as necessary as the user can control the door using smartphones. Another possible way could be clicking on the smartphone notification to make the authentication process more convenient.

Face recognition and OTP have been implemented in the banking sector for ATM transactions [19]. First, the user inserted the ATM card into the machine. Then, the user can choose either face recognition or OTP mechanism for authentication. The advantage of the system is that the cardholder can assign other people to make a transaction on the ATM while necessary. In addition, iris recognition technology can be implemented to allow the system to work more accurately at night. Manish et al. {Manish, 2020, Card-Less ATM Transaction using Biometric and Face Recognition–A Review.} proposed a card-less ATM transaction with a biometric system. The user can start the transaction immediately with fingerprint recognition and the OTP approach without an ATM card. It provided more convenient and comfortable ways for the user to make a transaction. In addition, both studies by Singh et al. [19] and Manish et al. [20] aimed to prevent card fraud activities because only the authenticated person is allowed to make the transaction. Varshitha and Shivanand [21] proposed an Android-based voting system using face recognition and OTP. There are three steps of authentication for valid voters. The first step is to login into the application to verify users' personal information on the smartphone. Then, the face recognition process is executed to authenticate the voter's identity. The last step is that the voter received the OTP on the smartphones and entered the OTP. The voter is allowed to vote if the correct OTP is verified. The user status is changed to yes after voted. It indicated that one voter could vote only once and thus avoid the duplication of votes. The voters can vote using smartphones, which is more convenient and time-saving than the traditional systems.

3 Methodology of the study

The study adopted the rapid application development (RAD) [22, 23] methodology. It consists of four phases requirement planning, user design, construction, and cutover, as demonstrated in Figure 2. The requirement planning involved gathering the

information and identifying the user requirements to develop the multi-factor authentication for a smart home. The requirements for this system were gathered by analysing documents and conducting a survey using social media networks to random homeowners in Malaysia in January 2021. The result of the survey was analysed to understand the design and the functions that the system needs. Finally, the requirements were documented and demonstrated using a use case diagram, flow chart, and circuit diagram to construct a user design. The user design process is iterated and conducted in parallel with the construction of the prototype. The prototype construction process is also iterated to reflect changes in the user design [23].

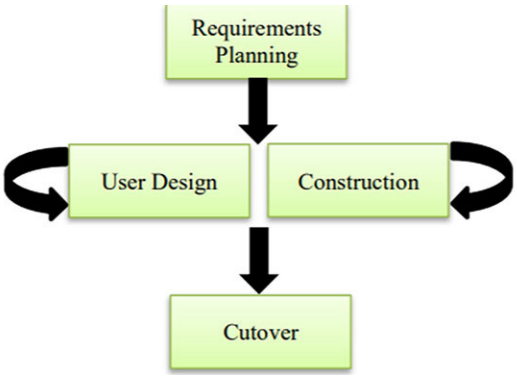

Fig. 2. The flow of RAD methodology [23]

The software and hardware architecture, including the programming language used and the database storage, were specified during the prototype construction phase. RAD emphasises the prototype's iterated development in obtaining the system's requirements so that the entire development process is faster and more flexible [23]. During the cutover phase, users were involved in evaluating the system functionalities and performance. A post-task questionnaire [23] containing the demographic information and the system usability scale (SUS) [24–27] were used to evaluate the usability of the proposed design. The description of the post-task questionnaire is summarised in Table 1. Selected respondents were also interviewed for further feedback and identifying issues. Finally, the user's issues were addressed to enhance the system's usability. Thus, it helps to improve the users' satisfaction and produces a more reliable multi-factor authentication for the smart home.

Table 1. The content of the post-task questionnaire

Section	Topic
A	▪ Demographic and background information on home security and face recognition technology today. ▪ Closed-ended question. ▪ The total number of questions is 8.
B	▪ After each task is demonstrated, the respondents self-rated their opinions using the System Usability Scale (SUS) [24–26]. ▪ A 5-point Likert Scale is used. ▪ The total number of questions is 13.
C	▪ Interview questions. ▪ The total number of questions is 5.

4 The design of smart home multi-factor authentication

The design and development of the smart home multi-factor authentication are described in this section. Two steps were involved in the requirement gathering process. The first step was analysing documents and information from Internet resources. The relevant contents were searched using the keywords and documented to construct the requirements in developing the smart home multi-factor authentication. The second step was conducting a survey on a social media platform like Facebook and WhatsApp. A survey questionnaire was created based on the information collected from the analysed documents in the first step of the requirement gathering process. A total of 100 respondents participated in this survey to provide their opinion regarding the face recognition system. Most of the respondents were students aged between 21 to 30. 57.7% of the respondents were familiar with face recognition technology, and 53.8% were satisfied with today's face recognition application. The survey result was then transformed into a list of requirements specifications, as shown in Table 2. The requirements consist of three major requirements, 'Configure', 'Register', and 'Authenticate'. The priority of the requirement is indicated by M (Mandatory), O (Optional), and D (Desirable).

Table 2. The requirements for the proposed smart home multi-factor authentication system

No.	Requirement Description	Priority
1	**CONFIGURE**	
1.1	An admin user shall be set up.	M
1.2	The camera and microcontroller are connected to electricity.	M
1.3	The system shall be initiated with at least one user is registered.	M
1.4	Users shall be taught how to use the system.	D
2	**REGISTER**	
2.1	The system shall allow a new user to register their personal information, including the phone number, face image (maximum to 5 images), and a set of PINS for backup.	M
2.2	The system shall be able to store information in a database.	M
2.3	The system shall be able to allow registration to a maximum of 10 users.	M
3	**AUTHENTICATE**	
3.1	The system shall be able to detect the face appear on the camera.	M
3.2	The system shall be able to match the face detected with the registered face image in the database.	M
3.3	The system shall recognise the user's face if only one face is detected at the same time.	M
3.4	The system shall be able to display a message when the face recognition process is successful.	M
3.5	The system shall send the OTP to the user's phone through a text message after face recognition success.	M
3.6	Users can enter OTP on the keypad.	M

(Continued)

Table 2. The requirements for the proposed smart home multi-factor authentication system *(continued)*

No.	Requirement Description	Priority
3.7	The system shall be able to verify the OTP input by the user.	M
3.8	The system shall be able to notify if the user correctly inputs the OTP.	M
3.9	The system shall be able to notify if incorrect OTP is input by the user.	O
3.10	The system shall be able to display an alert message if incorrect OTP attempts more than three times.	O

The requirements are then translated to a use case diagram, one of the behavioural diagrams in UML, as shown in Figure 3. The diagram describes the interaction between the user and admin user with the smart home multi-factor authentication system. First, the admin user handles the 'Configure' use case. Meanwhile, the user and admin user execute the use case of 'Register' and 'Authenticate'. 'Authenticate' use case allows the system to recognise the user's face image and verify OTP. However, the process of face recognition and generate OTP must be executed before the verification of OTP. In addition, the user can receive an unsuccessful message during the failure of the face recognition and OTP verification process.

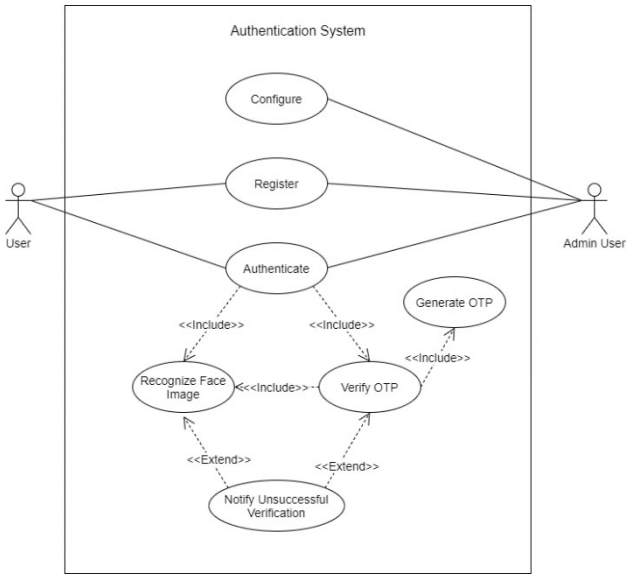

Fig. 3. The use case diagram for the proposed smart home multi-factor authentication system

The process of the smart home multi-factor authentication system is described in the flow chart in Figure 4. It allows the user to understand the operations of the system quickly.

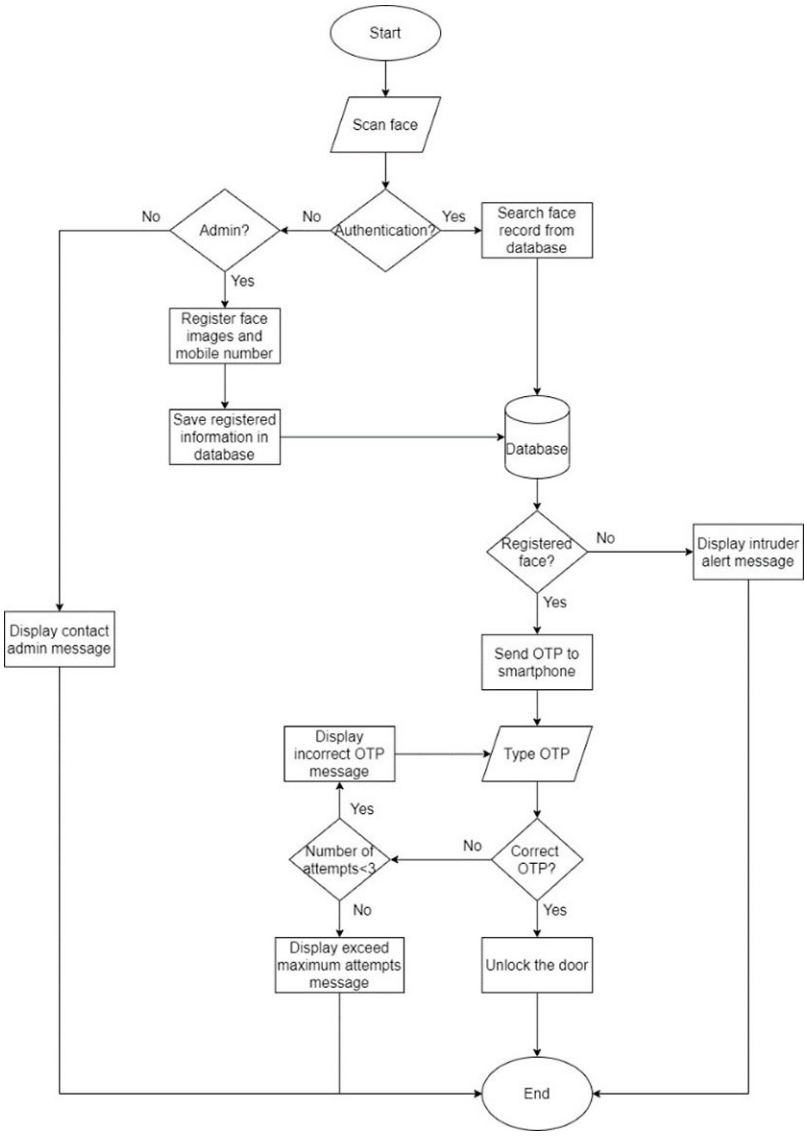

Fig. 4. The flow chart of the proposed smart home multi-factor authentication

Figure 5 demonstrates the circuit diagram of the system. The hardware components used are the Arduino UNO, 3×4 Membrane keypad, 16×2 LCD, ESP32 camera, a breadboard, batteries, relay module, 12V solenoid lock and SIM900a GSM module. These components are connected to the computer and configured on Arduino Studio.

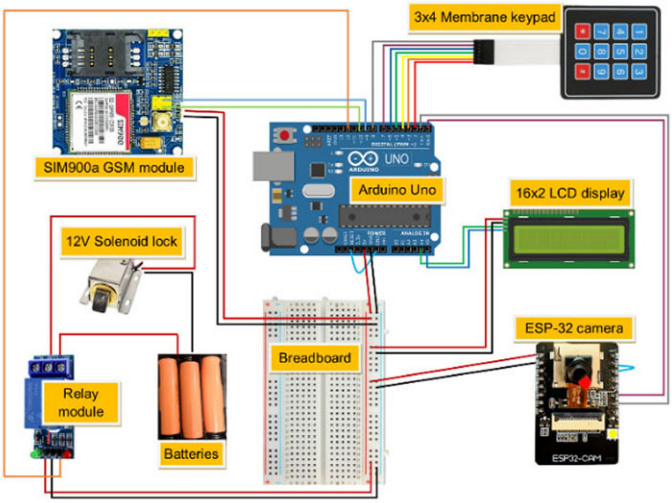

Fig. 5. The circuit diagram for the proposed smart home multi-factor authentication system

The hardware components are configured in a casing, as shown in Figure 6. The white box indicates the door locking system, and the solenoid lock demonstrates the door lock in the resident's house.

Fig. 6. The hardware components configured in a box

5 Evaluation

Multi-factor authentication recognises authorised users according to their biometric characteristics and is combined with other authentication factors like smart cards, passwords, PINs or OTP [11]. Thus, it increases the system's security by making it difficult for criminals to steal identities or pretending to be someone else. However, usability

has been the main challenge of multi-factor authentication. It is always the tradeoff of security and vice versa [11]. In other words, increasing the security of a system through authentication would also increase users' steps to authenticate themselves, reducing its usability. On the other hand, usability ensures users use the authentication system in the most efficient way [28]. Therefore, efficiency is essential for an authentication system's usability [29]. Kaur and Mustafa [29] suggested the following characteristics that can represent it (1) users' effort to authenticate themselves, (2) time to authenticate an authorised user, (3) memorability of the authentication methods and (4) learnability of using the authentication system.

In evaluating the usability of the multi-factor authentication using face recognition and OTP on a smartphone, the study qualitatively analysed the system based on these usability features.

1. Users' effort to authenticate themselves involves three steps, facing the camera to detect the face image, opening the text message on the smartphone, and keying the OTP on the keypad.
2. Time to authenticate an authorised user would vary depending on the quality of the Internet connection for sending the OTP to the user's smartphone. Currently, it uses the cellular network to connect to the Internet. So, for example, users would receive the OTP on their smartphone within 3 seconds within an excellent GSM network connection.
3. Memorability of the authentication methods would be the most valuable part of the system as it does not require users to memorise another set of passwords or PINs. Therefore, there is no risk of a forgotten password or PIN.
4. Learnability of using the authentication system is very simple. The authentication system has an LCD screen that displays messages during the authentication process. First, it asks the authorised users to face the camera and then checks their phone for the OTP and finally key in the OTP.

The qualitative analysis of the multi-factor authentication using face recognition and OTP on a smartphone demonstrates that the proposed authentication system meets usability features. Nevertheless, it depends highly on the Internet connection to send the OTP to the authorised users' smartphones.

An evaluation was conducted to assess the system's usability and performance through a one-to-one session with 30 respondents. During the evaluation, the researchers met the respondents face-to-face or through the Zoom meeting platform. In addition, a post-task questionnaire (as described in Table 1) was distributed to the respondents at the end of the evaluation session.

The respondents consisted of 18 males and 12 females. 76.7% of them were between 21–30 years old. 60% of the respondents were students, 26.7% worked in the private sector, and 13.3% were self-employed. Regarding the type of door lock used in the respondent's house, 73.3% of them used the key and padlock on the grill door, 16.7% used the passwords or PINs, and the other 10% used the access card to unlock the door. In terms of attitude towards home security, 53.3% of the respondents were moderate conscious of their home security which they always lock the door. 43.3% were very conscious and always double-locked the door, and the other 3.33% of respondents

were relaxed and sometimes forgot to lock the door. Next, most respondents used the face recognition application to unlock their smartphones or tablets and the temperature scanner at the shopping malls. Ten respondents never used the face recognition application in their daily life. A minority of the respondents had used the face recognition application, including unlocking the door, attendance system in school or workplace, airport boarding, and border check-in. Besides, 50% of the respondents believed that face recognition could provide better home protection. On the other hand, 26.7% of the respondents claimed that it is less secure than the other door locking system, and the other 23.3% of them were not sure regarding the security protection by the face recognition. In short, a few people doubted the security protection provided by facial recognition technology.

As mentioned in Section 3, SUS was the primary tool used to evaluate the usability of the proposed design. It used a five-point Likert scale, as shown in Table 3. The points were used in the calculation of the final SUS score.

Table 3. The 5-points Likert scale is used in SUS

Agreement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Points	1	2	3	4	5

The respondents were divided into two groups according to their prior experience using face recognition technology in their daily lives. Group A comprised twenty respondents who had prior experience in using facial recognition technology. On the other hand, Group B comprised ten respondents with no experience of using facial recognition systems. The formula to calculate the final score of SUS [27] is defined in Equations (1–3).

$$Total\ score = \sum_{i=1}^{5} N_i \times S_i \tag{1}$$

where,

N_i = *Number of respondents checked the scale*

S_i = *Points for each agreement*

Deduct one from **the total score for each respondent for every odd-numbered question.**

$$Final\ score = Total\ score - (1 \times n\ respondents) \tag{2}$$

Deduct five from **the total score for each respondent for every even-numbered question.**

$$Final\ score = (5 \times n\ respondents) - Total\ score \tag{3}$$

The responses and scores of Group A and B are shown in Tables 4 and 5, respectively. The formula to calculate the SUS total score [27, 30] can be referred to as the agreement chosen by the respondents with the corresponding point in Table 3. Finally, the complete result is shown in Table 6.

Table 4. The self-rated responses of Group A

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
1	4	4	0	7	5	65
2	0	3	3	8	6	77
3	0	0	0	13	7	87
4	0	0	1	5	14	93
5	0	0	2	11	7	85
6	0	2	3	9	6	79
7	0	3	5	9	3	72
8	3	11	3	3	0	46
9	0	1	1	12	6	83
10	0	1	3	12	4	79

Table 5. The self-rated responses of Group B

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
1	1	1	3	3	2	34
2	0	5	3	1	1	28
3	0	0	1	6	3	42
4	0	1	2	4	3	39
5	0	0	1	6	3	42
6	0	4	3	3	0	29
7	0	1	0	6	3	42
8	3	3	2	2	0	23
9	0	0	1	7	2	41
10	1	0	3	3	3	37

Table 6. The final SUS score for two groups of respondents

Question	Group A (n1 = 20 respondents)		Group B (n2 = 10 respondents)	
	Total Score	Final Score	Total Score	Final Score
1	65	45	34	24
2	77	23	28	22
3	87	67	42	32
4	93	7	39	11
5	85	65	42	32
6	79	21	29	21
7	72	52	41	31
8	46	54	23	27
9	83	63	41	31
10	79	21	37	13
Total		418	Total	258
SUS score (Total * 2.5 / n1)		52.25	SUS score (Total * 2.5 / n2)	64.50

Table 7 illustrated the guideline for the SUS score in which the higher score indicates the system' better usability, and it is recommended to use.

Table 7. The guideline of the SUS score

SUS Score	Grade	Rating
>80.3	A	Excellent
68 – 80.3	B	Good
68	C	Pass
51 – 68	D	Poor
< 51	E	Awful

The overall SUS score for the group A respondent is 52.25, and group B respondents are 64.50. As referred to the SUS score guideline in Table 7, both scores were classified as poor and below the passing SUS score, 68. Thus, the scores reflected that the system is acceptable, but some usability issues can be improved in the future. Besides, the SUS score for the respondents in group B is greater than that in group A. It indicated that the respondents with zero experience on the facial recognition system are more satisfied with the system's usability than the respondents with facial recognition experience. However, the result might be inaccurate due to the different number of respondents in each group. The larger number of respondents in group A could have made the result more reliable and closer to the expected value. Thus, increasing the number of respondents for further analysis could reveal more information on the usability issue of the system.

Apart from that, 50% of the respondents agreed, and 23.3% strongly agreed that this smart home multi-factor authentication system would be an alternative to a conventional home locking system. However, 3.3% and 10% of the respondents strongly disagreed and disagreed that this system would replace the conventional system. The other 13.3% of them were not sure about this statement. In short, most respondents agreed that this system would be an alternative to traditional home locking systems. Furthermore, 93.3% of the respondents rated the positive comments (agree and strongly agree) that they were satisfied with the overall ease of use of the system. In comparison, there are 6.7% of the respondents rated neutral. Therefore, the conclusion is that the respondents were satisfied with the usability of this system. Moreover, 60% and 36.7% of the respondents agreed and strongly agreed that they were satisfied with the time to complete the process. Meanwhile, there were 3.33% of them rated neutral. Therefore, it proved that the respondents were satisfied with the convenience of the system.

5.1 Analysis of the interview

The interview session was transcribed and analysed based on the two groups of respondents as mentioned above. Overall, the respondents' experience with this system was excellent and enjoyable, but there would be some displeasure due to the online evaluation. It is also beneficial of experience sharing for the respondents who had never used face recognition technology. Besides, the respondents with zero experience of

the facial recognition system were more concerned about the dependent factors that would affect the system's usability, such as the unstable internet connection, the electrical blackout issues, and the quality of the hardware components. For example, the Internet connection issue connecting the camera to the WiFi during the configuration step. For offline testing, the camera can quickly connect to the WiFi. However, it took longer to connect the camera with the WiFi while the online testing was conducted. The assumption can be made that the online meeting software had consumed a considerable amount of internet bandwidth and thus influenced the speed of the Internet. Meanwhile, the feedback provided by the respondents with experience with face recognition technology demonstrated that they were more concerned about the security issues and the improvement that can be made to this system.

6 Conclusion and future works

This research proposed a design of a smart home multi-factor authentication system using face recognition and OTP. The proposed design was implemented using an ESP32 camera, 3×4 keypad, 16×2 LCD and GSM module programmed on an Arduino microcontroller. Meanwhile, the relay module and the solenoid lock indicated the door lock in the house. The proposed design was tested to detect and recognise the face image on the camera. Then, an OTP sent to the user's smartphone is used to verify to unlock the door. The major limitation of the multi-factor authentication using face recognition and OTP on a smartphone is that it highly relies on the Internet connectivity used for the system. In the context of this study, it uses a GSM module for the Internet connection. However, it can be replaced with a home WiFi module for more reliable Internet connectivity in its actual implementation.

Nevertheless, the evaluation of the proposed design suggested that it can be further improved in several ways to expand the functionalities. First, it should allow several sample images taken during the enrollment process; hence, it could increase the classifier accuracy to identify and recognise the user's face. Second, a simple interface should be developed to allow a smooth enrollment process. It would allow the system to function more efficiently and provide explicit instruction to the user than a serial monitor. Next, an alert system using a suitable notification mechanism can be implemented when the camera detects an intruder's face image. Furthermore, an LED can also be added to indicate a successful face recognition process instead of relying on the message displayed on the LCD. Moreover, additional devices like lightning and tablet can be added to improve the system's user experience.

7 Acknowledgement

The authors thank the Ministry of Higher Education Malaysia for funding this study under the Fundamental Research Grant Scheme (Ref: FRGS/1/2018/ICT03/UUM/02/1, UUM S/O Code: 14208), and Research and Innovation Management Centre, Universiti Utara Malaysia for the administration of this study.

8 References

[1] N. Katuk, K. R. Ku-Mahamud, N. H. Zakaria, and M. A. Maarof, "Implementation and recent progress in cloud-based smart home automation systems," in *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2018, pp. 71–77. https://doi.org/10.1109/ISCAIE.2018.8405447

[2] N. Wei, A. Baharudin, L. A. Hussein, and M. Hilmi, "Factors affecting user's intention to adopt smart home in Malaysia," *International Journal of Interactive Mobile Technologies,* vol. 13, pp. 39–54, 2019. https://doi.org/10.3991/ijim.v13i12.11083

[3] T. K. Ghazali and N. H. Zakaria, "Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment," *Journal of Computers (Taiwan),* vol. 29, pp. 189–208, 2018.

[4] A. Aziz, M. H. A. Wahab, A. Mustapha, and M. F. M. Mohsin, "Design and development of smart home security system for disabled and elderly people," *Journal of Telecommunication, Electronic and Computer Engineering,* vol. 9, pp. 135–138, 2017.

[5] S. Elly, "Traditional vs modern: the better security systems". [Online]. Available: https://www.asmag.com/showpost/25806.aspx [Accessed: July 1, 2021].

[6] Visioforce Automation Systems, "Smart Home". [Online]. Available: http://visioforce.com/smarthome.html [Accessed: July 1, 2021].

[7] O. Eseosa and U. Roland, "Access control using smartcard and passcode," *IOSR Journal of Electrical and Electronics Engineering,* vol. 4, pp. 29–34, 2013. https://doi.org/10.9790/1676-0452934

[8] N. Katuk, N. Zakaria, and K. R. Ku-Mahamud, "Mobile phone sensing using the built-in camera," *International Journal of Interactive Mobile Technologies*, vol. 13, pp. 102–114, 2019. https://doi.org/10.3991/ijim.v13i02.10166

[9] A. Hayes, "Smart Home". [Online]. Available: https://www.investopedia.com/terms/s/smart-home.asp [Accessed: July 1, 2021].

[10] S. G. Gaurav, "*The Evolution of Smart Home Technology*". [Online]. Available: https://blog.bccresearch.com/the-evolution-of-smart-home-technology [Accessed: July 1, 2021].

[11] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography,* vol. 2, pp. 1–31, 2018. https://doi.org/10.3390/cryptography2010001

[12] Thales, "Biometrics: Definition, use cases and latest news". [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics [Accessed: July 1, 2021].

[13] K. Richards and I. Wigmore, "One-time password". [Online]. Available: https://searchsecurity.techtarget.com/definition/one-time-password-OTP#:~:text=A%20one%2Dtime%20password%20(OTP,or%20reused%20across%20multiple%20accounts [Accessed: July 1, 2021].

[14] S. Ma, R. Feng, J. Li, Y. Liu, S. Nepal, E. Bertino, R. H. Deng, Z. Ma, and S. Jha, "An Empirical Study of SMS One-Time Password Authentication in Android Apps," in *Proceedings of the 35th Annual Computer Security Applications Conference*, 2019, pp. 339–354. https://doi.org/10.1145/3359789.3359828

[15] S. Ma, J. Li, H. Kim, E. Bertino, S. Nepal, D. Ostry, and C. Sun, "Fine with "1234"? An analysis of SMS one-time password randomness in Android apps," in *2021 IEEE/ACM 43rd International Conference on Software Engineering*, 2021, pp. 1671–1682. https://doi.org/10.1109/ICSE43902.2021.00148

[16] S. Sandar and S. A. N. Oo, "Development of a secured door lock system based on face recognition using Raspberry Pi and GSM module," *International Journal of Trend in Scientific Research and Development,* vol. 3, pp. 357–361, 2019.

[17] R. Manjunatha and R. Nagaraja, "Home Security System and Door Access Control based on Face Recognition," *International Research Journal of Engineering and Technology*, vol. 4, pp. 437–442, March 2017.

[18] I. P. Aiswarya, "Real-time Smart Door Lock System using Image Detection and Voice Recognition," *International Research Journal of Modernization in Engineering Technology and Science,* vol. 2, pp. 393–407, 2020, https://irjmets.com/rootaccess/forms/uploads/real-time-smart-door-lock-system-using-image-detection-and-voice-recognition.pdf

[19] P. Singh, S. Shahin, Y. Kumar, and U. Chauhan, "ATM Plus with Face Recognition and OTP Mechanism," *International Research Journal of Modernization in Engineering Technology and Science,* vol. 3, pp. 659–662, 2021.

[20] C. M. Manish, N. Chirag, H. R. Praveen, M. J. Darshan, and D. K. Vali, "Card-Less ATM Transaction using Biometric and Face Recognition–A Review," *International Journal for Research in Applied Science & Engineering Technology,* vol. 8, pp. 1493–1498, 2020. https://doi.org/10.22214/ijraset.2020.30444

[21] K. S. Varshitha and N. Shivanand, "Android Mobile based Voting System through Facial Recognition," *JNNCE Journal of Engineering & Management,* vol. 4, p. 1, 2021. https://doi.org/10.37314/JJEM.2021.040201

[22] J. Martin, *Rapid application development*: Macmillan Publishing Co., Inc., 1991.

[23] N. Katuk, T. Jayasangar, and Y. Yusof, "Design and Development of Smart List: A Mobile App for Creating and Managing Grocery Lists," *Baghdad Science Journal,* vol. 16, pp. 462–476, 2019. https://doi.org/10.21123/bsj.2019.16.2(SI).0462

[24] J. Brooke, "SUS-A quick and dirty usability scale," *Usability evaluation in industry,* vol. 189, pp. 4–7, 1996.

[25] A. Bangor, P. T. Kortum, and J. T. Miller, "An empirical evaluation of the system usability scale," *International Journal of Human–Computer Interaction,* vol. 24, pp. 574–594, 2008. https://doi.org/10.1080/10447310802205776

[26] J. R. Lewis, "The system usability scale: past, present, and future," *International Journal of Human–Computer Interaction,* vol. 34, pp. 577–590, 2018. https://doi.org/10.1080/10447318.2018.1455307

[27] H. Alathas, "How to Measure Product Usability with the System Usability Scale (SUS) Score". [Online]. Available: https://uxplanet.org/how-to-measure-product-usability-with-the-system-usability-scale-sus-score-69f3875b858f [Accessed: July 1, 2021].

[28] S. Iqbal, M. Irfan, K. Ahsan, M. A. Hussain, M. Awais, M. Shiraz, M. Hamdi, and A. Alghamdi, "A novel mobile wallet model for elderly using fingerprint as authentication factor," *IEEE Access,* vol. 8, pp. 177405–177423, 2020. https://doi.org/10.1109/ACCESS.2020.3025429

[29] A. Kaur and K. Mustafa, "Efficiency—A Layered Model for Authentication," in *ICRITO 2020—IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, 2020, pp. 543–547. https://doi.org/10.1109/ICRITO48877.2020.9197960

[30] D. Derisma, "The Usability Analysis Online Learning Site for Supporting Computer programming Course Using System Usability Scale (SUS) in a University," *International Journal of Interactive Mobile Technologies*, vol. 14, pp. 182–195, 2020. https://doi.org/10.3991/ijim.v14i09.13123

9 Authors

Tok Yen Xin is a final year student at Universiti Utara Malaysia (UUM), pursuing a Bachelor of Science with Honours (Information Technology) and majoring in Data Science. She is interested in artificial intelligence applications and has worked on a face recognition system for her final year project (Email: tokyenxin@soc.uum.edu.my).

Norliza Katuk obtained her Doctoral degree in information technology from Massey University, New Zealand, in 2012. Currently, she is an associate professor at Universiti Utara Malaysia (Email: k.norliza@uum.edu.my).

Ahmad Suki Che Mohamed Arif received his PhD degree from Universiti Utara Malaysia. His research interests include video transmission over the Internet, network transport protocol, mobile computing, distributed systems, and network traffic analysis/engineering (Email: suki1207@uum.edu.my).

Article submitted 2021-07-10. Resubmitted 2021-10-03. Final acceptance 2021-10-10. Final version published as submitted by the authors.