IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 January 2023, accepted 31 January 2023, date of publication 6 February 2023, date of current version 24 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3243114

RESEARCH ARTICLE

Secure PIN-Entry Method Using One-Time PIN (OTP)

FARID BINBESHR[1,2], LIP YEE POR[1], (Senior Member, IEEE), M. L. MAT KIAH[1], (Senior Member, IEEE), A. A. ZAIDAN[3], (Senior Member, IEEE), AND MUHAMMAD IMAM[4]

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[2]Department of Computer Science, College of Computers and Information Technology, Hadhramout University, Al-Mukalla, Yemen
[3]SP Jain School of Global Management, Sydney, NSW 2141, Australia
[4]Interdisciplinary Research Center for Intelligent Secure Systems, Department of Computer Engineering, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Corresponding authors: Farid Binbeshr (farid@hu.edu.ye) and Lip Yee Por (porlip@um.edu.my)

This work involved human subjects or animals in its research. The authors confirm that all human/animal subject research procedures and protocols are exempt from review board approval.

ABSTRACT The regular PIN-entry method has been still the most common method of authentication for systems and networks. However, PINs are easy to be captured through various attacks, including shoulder-surfing, video-recording, and spyware. This could be attributed to the involuntary nature of entering the original PIN during authentication. In this paper, we employ an indirect input method that utilizes the addition mod 10 and a mini-challenge keypad in order to produce a one-time PIN (OTP) that obscures the original PIN. The results of our user study manifest that the proposed PIN-entry method provides better security than the existing PIN-entry methods while maintaining an acceptable level of usability. Moreover, the user feedback fully support the use of the proposed PIN-entry method in critical-security situations.

INDEX TERMS PIN entry, password authentication, OTP, shoulder surfing, observation attack, video recording, spyware attack.

I. INTRODUCTION

Personal Identification Number (PIN) entry, or regular PIN-entry, is an example of knowledge-based authentication in which users enter shared secrets of either 4-numeric or 6-numeric password to prove their identities [1]. It is still the most popular method of authentication for systems and networks. The popularity of the regular PIN-entry method comes from being easy to use and remember [2].

In regular PIN-entry method authentication, users need to type in their original PINs each time they login into a system. However, revealing the original PIN during login may make it susceptible to be attacked. For example, adversaries may shoulder surf the authentication session to obtain the PIN. They may use a video-recording device to record a user while performing authentication and later reproduces the PIN. It is also possible that the adversaries might install spyware at the compromised device and capture the user input (e.g., PIN) and screen content [3]. These examples highlight the problem of the regular PIN-entry method and signify the need to enhance its security.

Many PIN-entry methods have been proposed in the literature to solve the aforementioned problem. They can be classified into direct and indirect input methods according to whether a user enters the original PIN or not [4]. Direct input methods ask users to reveal the original PIN during authentication as the regular PIN-entry method does. However, these methods try disguising the observer from capturing the original PIN through gaze input [5], [6], [7], [8] and visual distraction [9], [10], [11], [12], [13], [14]. Despite reducing the shoulder-surfing effect, direct input methods are still vulnerable to video-recording and spyware attacks. Indirect input

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

methods prevent users from entering the original PIN during authentication through a challenge-response approach. That is, a challenge is sent to the user, and then the user finds out and enters the response based on their knowledge of the challenge and the original PIN. The indirect input methods can be categorized into audio-based [15], [16], [17], haptic-based [18], [19], [20], and visual-based [21], [22], [23], [24], according to the channel through which the challenge is sent. Nonetheless, these indirect input methods either provide no protection against video-recording and spyware attacks or hamper the PIN-entry method's usability [25]. Therefore, the development of a secure and usable PIN-entry method against such attacks would be promising.

In this paper, we employ a challenge-response approach that utilizes the addition mod 10 and a challenge keypad in order to produce a one-time PIN (OTP) that obscures the original PIN. To simplify the login process and maintain regular PIN-entry compatibility, the visual channel used to enter the response is used to transfer the challenge through the challenge keypad. Besides, a user needs only to remember the PIN digits to identify the challenge digits. The main objective of the research is to develop a secure PIN-entry method and evaluate its feasibility in preventing shoulder-surfing, video-recording, and spyware attacks. The key contribution of this research is to provide a compatible and usable PIN-entry method resistant to shoulder-surfing, video-recording, and spyware attacks. We can therefore indicate that the proposed PIN-entry method could be utilized by users to secure a variety of everyday-life and critical applications and services. For example, the proposed PIN-entry method can be used as an alternative to the regular PIN to unlock smart device screens, withdraw cash from ATMs, make payments at POS systems, and open electronic doors. The proposed PIN-entry method enjoins the user to enter an OTP to thwart the threat of shoulder-surfing and recording attacks that arise when observing or capturing the user's PIN directly or through a recording tool when he is with-drawing cash from an ATM, unlocking his device in public, or logging from an internet cafe machine.

This paper is organized as follows. Section II-B presents the literature review. Section III explains the proposed approach. The evaluation analysis of the proposed PIN-entry method is described in Section IV. Finally, Section V concludes this paper and suggests future work.

II. LITERATURE REVIEW

A. PIN AUTHENTICATION ALTERNATIVES

There are several alternatives to personal identification number (PIN) authentication that can be used to verify a user's identity, including biometric authentication, token-based authentication, one-time password (OTP) authentication, and security question authentication.

In the token-based authentication system, a token or an object such as a key card, RFID card, bank card, or smart card is used as an instrument for an authorized verification. Token-based authentication provides an additional layer of security, as the token is typically only valid for a limited period of time. However, it may require the user to possess a separate device, such as a security token, to generate the authentication code, which may be less convenient for users. Furthermore, if a user has obtained a valid token, the user can immediately gain access to a particular system, even if the user is not an authorized user. As a consequence, a biometric authentication system has been proposed to address the limitations of the token-based authentication system.

Biometric authentication involves the use of personal and physiological characteristics of an authorized user, such as a fingerprint, speech, facial recognition, or iris scan, to verify the user's identity. This method can be more secure than token-based authentication systems because biometric data is unique to each individual and difficult to replicate. However, biometric authentication is still not widely adopted due to some major drawbacks, such as the exorbitant development cost that is required for setting up and maintaining such a system. Moreover, most biometric authentication systems suffer from slow performance and often produce a high, unreliable rate during the identification process [26]. For instance, most voice authentication schemes produce high error rates when tested in a noisy environment, while facial recognition schemes are still sensitive to variations in lighting conditions during verification, and fingerprint readers can be defeated by fake fingerprints [27]. Furthermore, biometric authentication systems may not be suitable for individuals with disabilities.

An OTP is a password that can only be used once on a computer or other digital device for a single login session or transaction. OTPs are immune to replay attacks, so they cannot be used against them. This means that even if a potential intruder records an OTP that has already been used to log into a service or complete a transaction, they will be unable to use it again because it is no longer valid after being used once. Because they are only valid for a single transaction, OTPs add an extra layer of security. They may, however, necessitate the use of a separate device, such as a phone, to receive the OTP, which may be inconvenient for users. It is possible that some of the emailed OTPs will arrive late or in the spam folder. If a user loses or misplaces their physical token, they will lose access to their OTP. It is possible that cellular network traffic is not always encrypted, which allows out-of-band networks to monitor the data. OTPs obtained via SMS, for example, are more likely to be hacked because they can be hacked via wireless infiltration and malware.

Security questions are a type of authentication method in which users must answer questions in order to be authenticated. Setting up security questions is a very simple process. Most of the time, a drop-down menu of questions is presented, and a user needs to select a few of them and then provide an answer. Because the information is already in the user's head, no additional tools or devices are required. However, many security question answers are easily accessible. In public records or on social media, people can find information such as your father's or mother's middle name, your favorite place

or color, and so on. Social engineering techniques, such as phishing emails or phone calls, can also inadvertently reveal this sensitive information.

In conclusion, despite the availability of other forms of authentication, PINs continue to be a popular and effective method of accessing bank accounts, unlocking smartphones, and logging into computer systems. This is because they are convenient and cost-effective.

B. RELATED WORK

This section provides a literature review of the PIN-entry methods resistant to shoulder-surfing, video-recording, and spyware attacks. These methods either employ a direct or indirect input way of entering the original PIN.

1) DIRECT INPUT METHODS

The previous research has shown that direct input methods attempt to disguise the observer from obtaining the original PIN through visual distraction or gaze input approaches. Visual distraction methods endeavor to distract observers visually by using a cursor camouflage [9], [10], by presenting a random-digit keypad [11], [12], and by input distraction ways such as aligning PIN digits together [13] or tapping the appropriate number using a deep or shallow pressure [14]. Visual distraction methods can provide varied protection against shoulder-surfing attack; however, they are vulnerable to spyware or video-recording attacks or both as the attacker can recover the original PIN directly from the recording tool regardless of the visual distraction tactics.

Gaze input methods [5], [6], [7], [8], [28] employ the eyes to enter the PIN in order to minimize the effect of shoulder-surfing attack. These PIN-entry methods are highly resistant to shoulder-surfing attack. They may further reduce the threat of video-recording attack. However, they are susceptible to spyware attack because users still reveal the original PIN during the authentication process. Furthermore, the application of gaze interaction methods is too limited because these methods fail to meet high accuracy, cost, and user experience requirements [29].

2) INDIRECT INPUT METHODS

The idea of indirect input methods is to prevent users from exposing the original PIN during each authentication attempt to thwart the adversary. The challenge-response approach is the typical example of indirect input methods in which a challenge is sent to the user through the audio, haptic, or visual channel. Then, the user needs to enter a response according to the received challenge and the original PIN.

Several studies have employed audio-based [15], [16], [17] and haptic-based [18], [19], [20] challenge-response methods to defend shoulder-surfing, video-recording, and spyware attacks. In audio-based and haptic-based methods, the challenge is sent through an audio channel and a haptic channel, respectively. The user then needs to provide the response based on the received challenge and the original PIN. These PIN-entry methods can provide high resistance against shoulder-surfing, video-recording, and spyware attacks as long as the channel that transfers the challenge is secure. Audio-based and haptic-based methods require an additional channel (audio or haptic) in addition to the visual one that is used to enter the response. However, requiring an additional channel may harm the acceptance and adoption of such methods as it contradicts the compatibility condition of the PIN-entry method [30]. We are not going to elaborate more on these methods as this paper focuses on visual-based challenge-response methods.

Visual-based challenge-response is a unimodal method in which the same visual channel is used to transfer the challenge and deliver the response. Thus, this could give such method more preferences than bimodal challenge-response methods (i.e., audio-based and haptic-based). For example, a visual-based challenge-response method has been proposed by [21], to resist shoulder-surfing attack. This method is similar to the cognitive trapdoor game method [24] in which it asks users to enter colors instead of the 4/6-numeric PIN to disguise user input. In other words, users of these methods must enter the background colors (black or white) that are assigned to each PIN number. The proposed method, however, does not mitigate the video-recording attack. More precisely, the attacker can easily narrow down the possible PINs by analyzing the recorded authentication sessions. Moreover, the proposed method may hamper usability by requiring multiple rounds to input PIN digits.

Lee [31] presented a challenge-response method where its layout comprises an array of digits (0-9), juxtaposed with an array of 10 objects. In the first round, a user identifies the session decision key, which is the object aligned with the first digit of the PIN. For subsequent rounds, the user aligns the session decision key to each PIN digit. Assume the user's PIN is 1234, and the object that is aligned to the first digit in the first round (i.e., 1) is ◯. For the second round, the user needs to rotate the object array so that the second PIN digit (i.e., 2) is aligned with the session decision key (i.e.,◯). The same process applies to entering the third and fourth PIN digits. Although the developed method is effective against shoulder-surfing attack, it is susceptible to video-recording attack with two recorded sessions. A usability limit of this method is the requirement of multiple rounds to enter the PIN. AlignPIN [32] is a challenge-response indirect input method to resist repeated shoulder-surfing attack. A user needs to align each PIN digit with each challenge digit in each row of a random 4×10 grid of cells to perform authentication. To illustrate, each grid cell has four digits: one static digit and three other digits chosen at random. Each row has a unique occurrence of each static digit $(0, 1, 2, \ldots, 8, 9)$. During the registration process, a user must register a reference cell (row, column) that will be used to recognize the challenge digits when logging in. So, the user should use the arrow keys to align the first PIN digit with the first challenge digit in the first row. Then, he should repeat the same process for the remaining PIN digits in order to login. AlignPIN provides

high resistance against shoulder-surfing attack. However, it is still prone to video-recording attack where an attacker can recover the original PIN through two recorded sessions. Moreover, AlignPIN is not compatible with the regular PIN-entry method with respect to the interface layout and the memorized information.

Zezschwitz et al. [23] proposed an indirect input PIN entry method named SwiPIN that assigns a simple random touch gesture to each digit on the keypad in order to resist the shoulder-surfing attack. These random gestures are UP, DOWN, RIGHT, LEFT, and TAB. To perform authentication, a user needs to draw the gestures that are assigned to his PIN digits. The authors have conducted a security and usability evaluation of the SwiPIN. Even though the evaluation results showed that SwiPIN performs fast regarding login time, it is susceptible to shoulder-surfing attack. In particular, an attacker needs to recognize the gestures drawn by the user to break the PIN.

Kwon and Na [22] proposed a visual-based indirect input method named SteganoPIN to resist video-recording attack. SteganoPIN consists of two numeric keypads, random (permute) and standard. The random keypad is used to derive the new OTP. It permutes the 10 numeric keys randomly for each session. However, this keypad is hidden by default, and it appears in a small circular touch area when a user puts a cupped hand on this circle. The standard keypad is used to key in the OTP. The user first locates the original PIN in a random keypad and subsequently maps the key locations into the standard keypad for OTP derivation. The user then enters the OTP on the standard keypad. Thus, the use of OTP resists the shoulder-surfing attack. SteganoPIN is secure against video-recording attack if a user correctly uses the system.

III. THE PROPOSED PIN-ENTRY METHOD

The proposed PIN-entry method employs an indirect input way of entering the PIN using the challenge-response approach. The challenge-response approach utilizes the addition mod 10 formula with a mini-challenge keypad in order to produce an OTP that obscures the original PIN. The employment of the addition mod 10 produces equally likely OTP digits so as to remove any correlation between authentication sessions and thus resist shoulder-surfing and recording attacks. The challenge is sent to the user through the challenge keypad. The user then computes the response (i.e., OTP) based on the received challenge and the original PIN. The principle of the proposed PIN-entry method is to create an OTP per each authentication session based on the addition mod 10 formula that takes two parameters, the original PIN P and the challenge R, as shown in equation 1.

$$OTP = (P + R) \mod 10 \tag{1}$$

A. CHALLENGE KEYPAD

Challenge keypad is a mini random digits keypad that is used to locate the challenge digits. It can be aligned to a key location within the regular keypad as shown in Figure 1. The challenge, R, is a random number composed of the same length of digits as the original PIN. The R digits are reordered for each authentication session by the user. To derive R, a user needs to map the PIN key locations on the challenge keypad. To illustrate, suppose the user's PIN is 1234 and Figure 1 represents the challenge keypad sent by the server. The user needs to map his PIN key locations (i.e., 1234) on the challenge keypad (seen in Figure 1) in order to derive R digits (i.e., 7, 5, 1, 3). R digits should be ordered according to the key locations of the PIN digits on the regular keypad layout (i.e., 1, 2, 3, . . . , 9, 0) to avoid sessions correlation and thus make it difficult for an attacker to predict the original PIN. For example, suppose the user creates a PIN of 1472. As in Fig 1, the R digits are 7, 3, 6, and 5. We can notice that the digit 5 of the R digits results from mapping the digit 2 (fourth digit) of the PIN with its key location on the challenge keypad. The sequence of the R digits needs to be rearranged in ascending order based on the key locations of the PIN digits on the regular keypad layout (i.e., 1, 2, 3, . . . , 9, 0) to prevent the correlation between the authentication sessions. Therefore, the digit 5 of the R needs to be placed before the digits 3 and 6 because digit 2 precedes digits 4 and 7 of the PIN on the regular keypad layout. Therefore, R is 7536. We remark that users need only to remember their original PIN to know the challenge. This is a strength point of the proposed PIN-entry method in which it maintains the regular PIN compatibility.

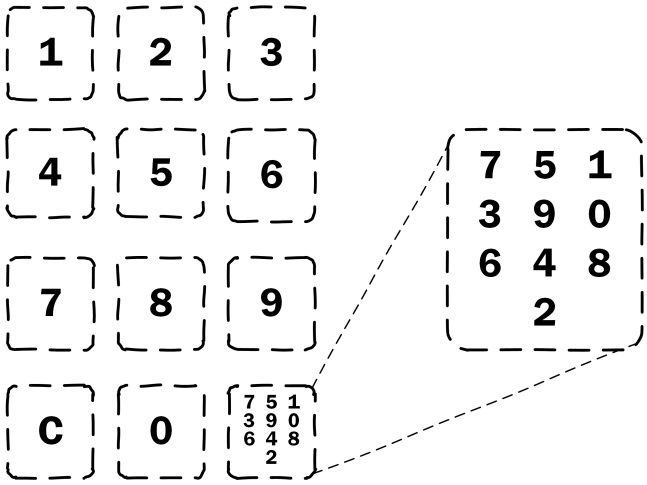


FIGURE 1. Challenge keypad incorporated within regular keypad.

B. HOW THE PROPOSED PIN-ENTRY METHOD WORKS?

1) REGISTRATION PHASE

In this phase, the user registers a username and creates a PIN password (4 digits). We go with a 4-digit PIN to keep our method simple. The registration process is assumed to be secure.

2) LOGIN PHASE

At this phase, the user has to provide their username (i.e., ID) and the *OTP* to login into the system. Fig 2 shows how the

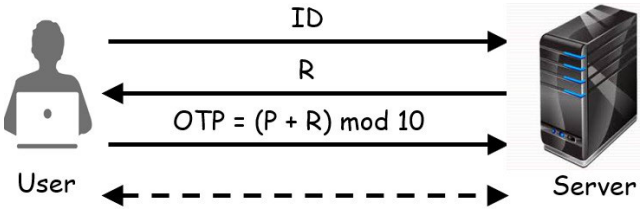


FIGURE 2. Login Phase.

user login into the system. First, the user types in the username. Then, the server sends R in the form of the challenge keypad. Finally, the user must calculate the OTP and send it to the server. For instance, let Fig 1 represents the keypad sent by the server for authentication. Suppose P is 1472, then R is 7536 and OTP is 8908. To illustrate, the first OTP digit results from adding the first P digit to the first R digit using mod 10 (i.e., $1 + 7 \bmod 10 = 8$). The user needs to repeat this step to produce the remaining OTP digits.

Identifying the challenge digits becomes easy when a user memorizes the PIN digit key locations. For the user's PIN digits of 1472, the corresponding digits on the challenge keypad are 7365, as seen in Fig 3a. To get the challenge digits, the user must rearrange the PIN digits in sequential order (1,2,3, …, 9, 0), as depicted in Fig 3b. The user can easily memorize the the order of the PIN digits by the time. So, the new order of 1472 PIN digits is 1247, and the corresponding challenge digits are therefore 7536.

Likewise, the server calculates otp_server and granting access to the user if there is a match, as described in Algorithm 1. At first, otp_server is calculated based on the R that is sent to the user and the stored P. The server grants access to the user only if otp_server matches the OTP that is taken as input from the user.

Algorithm 1 Login Procedure at Server

```
Input  : OTP as an array of 4 elements
Output: Grant access or wrong password
Initialize: otp_server = [], X = 0;
for i = 0 to 3 do
    otp_server[i] = (P[i] + R[i])  mod 10;
end
for j = 0 to 3 do
    if otp_server[j] = OTP[j] then
        X ← 1;
    else
        X ← 0;
        break;
    end
end
if X == 1 then
    grant access;
else
    wrong password;
end
```

If the user enters a wrong PIN many times (i.e., violate the threshold), the system asks the user to attempt authentication after a certain time. If the user failed again, the system would lock the account. The user then needs to contact the system administrator for the procedures required (e.g., requesting a security code through email or phone number) to unlock their account. The reason for locking the user's account is to avoid guessing attack. In fact, entering a wrong password many times is a sign of the attack. The recovery phase is similar to traditional password-based authentication, where the user resets the password if it is forgotten.

IV. EVALUATION AND ANALYSIS

In this section, we present the threat model and describe the user study conducted to evaluate the security and usability of the proposed PIN-entry method. We also provide the security and usability analysis of the proposed PIN-entry method and compare it to other PIN-entry methods.

A. THREAT MODEL

1) SHOULDER-SURFING ATTACK

In this type of attack, the attacker uses his naked eye to capture the authentication session data. Shoulder surfing is a potential threat of PINs in crowded and public places such as trains, airports, and markets. To evaluate the proposed PIN-entry method against this attack, users type in their PINs in a semi-public environment. The attacker stands in the user's vicinity and can observe the authentication session multiple times.

2) VIDEO-RECORDING ATTACK

In this attack, we employed a camera device to record the user's authentication session multiple times. Later, the attacker watches these recordings and reproduces the original PIN.

3) SPYWARE ATTACK

To evaluate the proposed PIN-entry method against this attack, the attacker has access to all information exchanged during the authentication session, including user input and screen content.

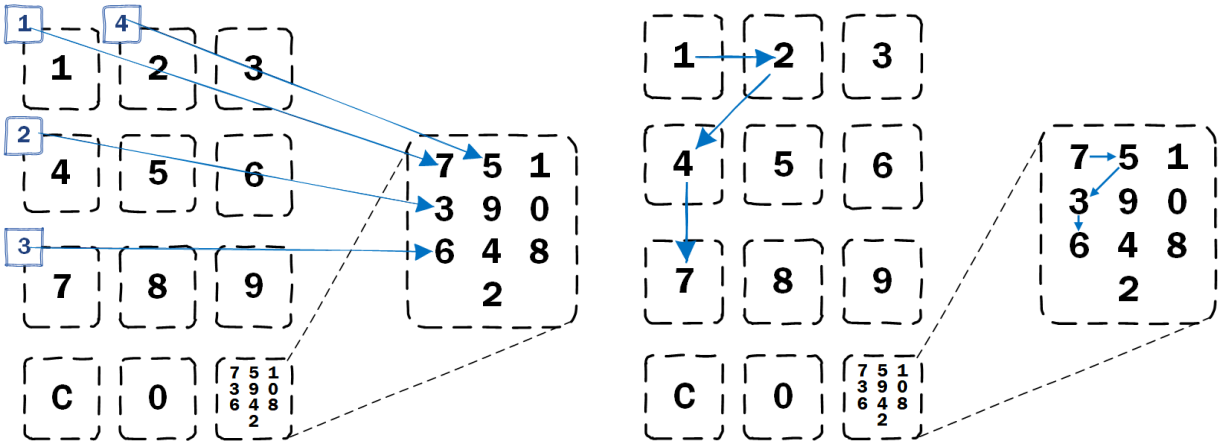
4) GUESSING ATTACK

A guessing attack is an attempt to login with the most common PINs (dictionary attack) or every possible PIN combinations (brute-force attack). The purpose of analyzing the guessing attack is to measure the security level of the proposed PIN-entry method when an attacker has no knowledge of it. We assume the attacker has access to the device and can manually guess the 4-digit PIN using both attacks.

B. USER STUDY

1) DESIGN

We conducted a 2×2 within-subject design study to evaluate the security and usability of the proposed PIN-entry method. The independent variables are PIN type (easy and hard) and



(a) Matching challenge digits of the PIN 1472

(b) Reordering challenge digits

FIGURE 3. How to locate challenge digits.

TABLE 1. PIN types and patterns.

PIN Type	PIN Pattern	Example
Hard	Four distinct digits	2345
	Three distinct digits	2321, 2231
Easy	Two distinct digits	2121, 2211
	Three identical digits	2212, 2221
	Four identical digits	2222

PIN system (regular and proposed). We categorize PINs into hard and easy according to the number of distinct/identical digits. The hard PIN has at least three distinct digits, while the easy PIN has at most two. Table 1 presents the details of PIN types and patterns. We counterbalanced the order of the conditions to reduce the learning effect. Participants were given three attempts per authentication session.

2) PARTICIPANTS

We recruited 30 participants (9 females) to conduct this study. For a comparative user study, a sample size of 30 participants can provide significant results. For instance, Alroobaea and Mayhew [33] suggest that a group size of 12 to 25 participants typically provides valid results. Six and Macefield [34] found that a sample size of greater than or equal to 20 participants is valid for comparative studies or for studies that seek statistically significant findings. Moreover, it was extremely difficult to obtain larger sample size during the Covid-19 pandemic. The participants have different levels of education, including elementary and secondary school, undergraduate, and postgraduate. They were aged between 11 and 38. All participants had experience with the regular PIN-entry method. It is deemed appropriate for studying this type of population as they often experience a variety of situations with regular PIN. Table 2 shows the demographic information of the participants.

3) PROCEDURE

The user study was proceeded in three phases: training, testing, and feedback. The training phase was started by explaining the purpose of the study and the procedures and task scenarios for each PIN-entry method. The next step was to provide free training for participants until they were ready for the test. Prior to the test, participants were asked to fill out a basic demographic information form in order to attain a sufficient context of the study.

TABLE 2. Participants demographic information.

Demographic	Number	Percent
Gender		
Male	21	70%
Female	9	30%
Age		
Minimum	11	
Maximum	38	
Median	25	
Education		
Elementary & secondary	4	13%
Undergraduate	5	17%
Postgraduate	21	70%
PIN usage		
Yes	30	100%
No	0	0

In the testing phase, each participant was asked to enter two PINs (easy and hard) using each PIN-entry method 10 times. We marked each login as successful if the participant passed the test within three trials. For later analysis, the PIN-entry time and error rate were logged. The user study was concluded with the feedback phase. In this phase, participants were asked to fill out a questionnaire.

A pilot study was conducted to find the most appropriate attackers for conducting the attacks. First, the participants were surveyed about their familiarity with PIN-entry methods, shoulder-surfing, and recording attacks. Then, those who reported their familiarity were tested. Only two of them were found capable of conducting and implementing all the

TABLE 3. Level of resistance of a PIN-entry method against shoulder-surfing and recording attacks [4].

Level of resistance	Criterion
High	Fully resistant to multiple observed/recorded sessions
Moderate	Partially resistant to multiple observed/recorded sessions
Low	Resistant to only single observed/recorded sessions
Vulnerable	Not resistant to any observed/recorded sessions

attacks. The two attackers were free to move in order to find the best position to perform the shoulder-surfing attack. To implement the video-recording attack, all login sessions were recorded using a camera. For spyware, the attackers have access to the recorded videos and the user input (i.e., OTP). The attackers had full control of the recorded videos for the purpose of guessing the original PINs. All attacks were based on three views followed by three guesses per each view.

C. SECURITY ANALYSIS

This part analyzes the security of the proposed PIN-entry method against shoulder-surfing, video-recording, spyware, and guessing attacks, in addition to a custom scenario of PIN length and challenge digits distribution. We analyzed the security of the proposed PIN-entry method according to the level of resistance it provides against these attacks, as described in Table 3. The level of resistance against attacks has been categorized into vulnerable (not resistant to any session), low (resistant to a single session), moderate (partially resistant), high (fully resistant), as described in [4]. The attack results show that the regular PIN-entry method is vulnerable to shoulder-surfing attack because users directly reveal their PINs without any protection. So, the attackers did not perform further testing on other attacks (i.e., video-recording and spyware) for the regular PIN because they succeeded to recover all the participants' PINs through the shoulder-surfing attack.

1) SHOULDER-SURFING ATTACK

The attackers failed to recover all hard and most easy PINs entered through the proposed PIN-entry method, as shown in Fig 4. The proposed PIN-entry method is a type of indirect input method that uses the concept of OTP. That is, an OTP is entered by the user for each authentication session. As a result, the attackers found it difficult to reveal the original PINs even though they captured the OTP. It was also difficult to capture the OTP and the challenge keypad simultaneously. However, they were able to recover 16.67% of the easy PINs. Indeed, all these recovered PINs are composed of four identical digits. Thus, the attackers needed one to three captured authentication sessions to recover these PINs, as shown in Figure 5. It was easy for them to recover such PINs as there were only 10 possibilities of the four identical digits, i.e., attackers could narrow down the possibilities after each trial. Overall, the proposed PIN-entry method with a hard PIN type offers a high level of resistance against shoulder-surfing attacks, while its resistance is only modest with an easy PIN type.

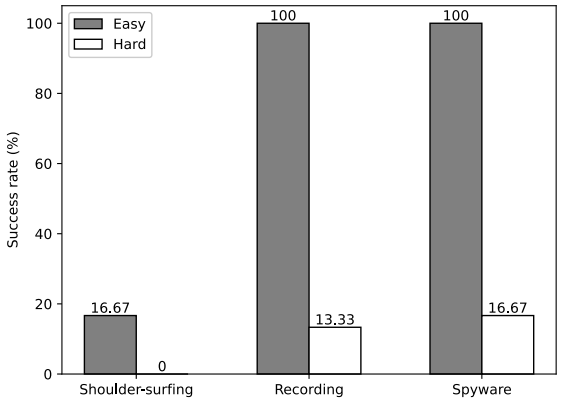


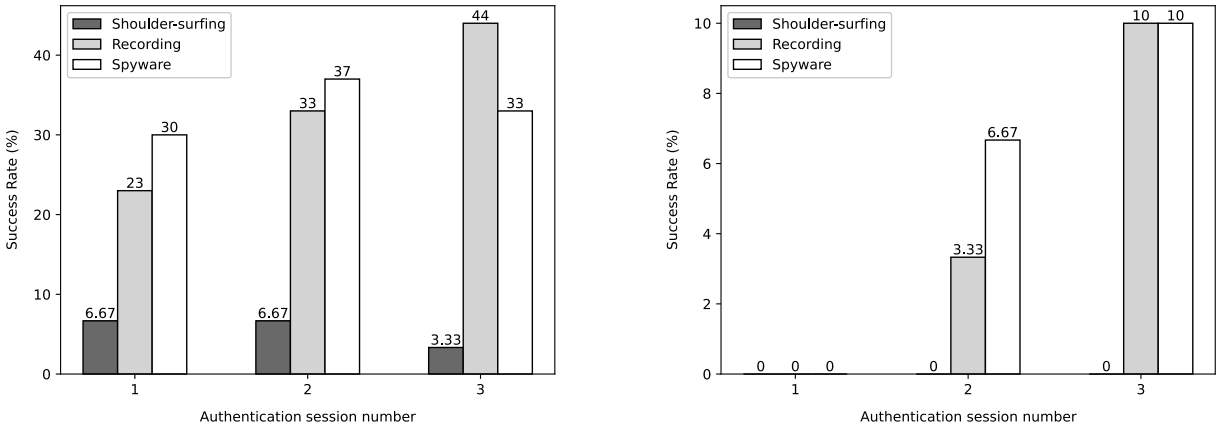
FIGURE 4. Attack success rate for easy and hard PINs of the proposed PIN-entry method.

2) VIDEO-RECORDING ATTACK

Video-recording attacks failed in most hard PIN cases, while they were successful in all cases of easy PINs, as presented in Figure 4. This means that, when used with a hard PIN type, the proposed PIN-entry method provides a moderate level of protection against these types of attacks; however, when used with an easy PIN type, it is vulnerable to such attacks. The attackers failed to recover most hard PINs because the proposed PIN-entry method produces different, equally likely OTP digits per authentication session. For example, the digit 1 in the OTP could be 1+0, 9+2, 8+3, 7+4, or 6+5 or vice versa.

However, the figure shows that the attackers succeeded in recovering some of the hard PINs entered through the proposed PIN-entry method. In some cases of such PINs, the produced OTP contains two identical digits, according to the R digits distribution. Thus, this helps the attackers predict the pattern of the original PIN and start narrowing down the possibilities. In the other cases, the random distribution of R digits helps the attackers narrow down the possibilities of the PIN digits after each trial. This occurs with the help of expecting that the first R digits are located at the beginning of the challenge keypad, whereas the last R digits are located at the end of the challenge keypad. The R digits, as we know, are the same PIN digits but ordered according to the key locations of the PIN digits on the regular keypad layout (i.e., $1, 2, 3, \ldots, 9, 0$). Thus, the attackers could narrow down the possibilities of the PIN digits over the trials based on the recorded OTPs and the expected R digits.

For easy PINs, the attackers succeeded in recovering all the participants' PINs because the produced OTP pattern helped them predict the PIN pattern. In fact, all easy PINs (except for the four-identical digits) are composed of only two distinct digits. Therefore, the produced OTP is always composed of two distinct digits. Hence, attackers need only to assume the correct pair that matches all OTP digits to recover



(a) Easy PINs (b) Hard PINs

FIGURE 5. Success rate of shoulder-surfing, video-recording, and spyware attacks over three captured authentication sessions.

the participant's PIN with the help of the recorded challenge keypad.

Remarkably, the attackers failed to detect all easy PINs and any hard PINs from the first recorded authentication session, as illustrated in Figure 5. The figure shows that attackers needed three recorded authentication sessions to recover all easy PINs and some hard PINs. This implies a positive correlation between the number of recorded sessions analyzed by the attackers and the attack success rate. It is noteworthy to mention that despite the difficulty of recording the authentication session multiple times, the attackers failed to recover most of the hard PINs entered through the proposed PIN-entry method.

3) SPYWARE ATTACK

Fig 4 shows that the proposed PIN-entry method with a hard PIN type offers a modest level of resistance to spyware attacks; however, it is vulnerable with an easy PIN type. Spyware attackers succeeded in recovering all easy PINs because the produced OTP pattern reveals the victim's PIN's pattern. Unlike easy PINs, attackers failed to recover most hard PINs due to the difficulty of identifying the PIN pattern or digits. Similar to video-recording attack, attackers needed more than one captured session to recover all easy PINs and some hard PINs, as shown in Fig 5.

4) GUESSING PIN

To evaluate the proposed PIN-entry method against guessing attack, we need to compute the PIN space ($digit\ space^{PIN\ length}$). Since the proposed PIN-entry method is the same as the regular 4-digit PIN, the possible PIN combinations are 10^4 (10000). The success probability of both guessing attacks (brute force attack or dictionary) is too low ($\frac{1}{10000}$). However, an attacker may repeat the same PIN to increase their opportunity to login since the PIN is dynamic and just four digits. Mathematically, the probability of matching the user's PIN increases by trials. This attack can be limited by allowing only three continuous failed login attempts, as in the case of the regular PIN-entry method. Also, we can mathematically point out the success probability of shoulder-surfing and recording attacks against a PIN-entry method as reported in [35] and [20]. For a challenge-response method, Lee et al. [20] proved that the success probability of guessing, shoulder-surfing and recording attacks are same ($\frac{1}{10000}$ for a 4-digit PIN) when the adversary has no access to the challenge, and all possible responses are equally likely. To some extent, this is applicable to our proposed PIN-entry method. The concise details to mathematically evaluate the success probability of these attacks against both PIN types of the proposed method are left for future work.

We can extend our statistical analysis to describe the success probability of these attacks. Theoretically, the probability of an attacker successfully shoulder-surfing, video-recording, or spying against a one-time 4-digit PIN can be represented by the following formula:

$$P(\text{success}) = \frac{1}{N}$$

where N is the number of possible 4-digit PINs. In this case, N is equal to 10000, since there are 10000 possible 4-digit PINs ranging from 0000 to 9999.

Therefore, the probability of an attacker successfully shoulder-surfing against a one-time 4-digit PIN is $\frac{1}{10000} = 0.01$, or 1%. This probability can be considered to be very low, since the attacker would need to be in the right place at the right time and be able to correctly guess the PIN from the small number of digits that they can see. The success probability against the regular PIN is 1 because the attacker is assumed to observe the entered PIN.

D. CUSTOM SETTINGS

The previous section shows that the video-recording and spyware attacks are successful against some of the hard PINs entered through the proposed PIN-entry method. It is argued that this results from the random distribution of the R digits. That is, the random distribution of R digits helps the attackers to correlate the OTP digits after each trial to narrow down the PIN digit possibilities. So, a custom setting of R digits

distribution was created to test if the proposed PIN-entry method is capable of resisting these attacks. R digits were deliberately distributed in this setting to prevent any correlation between authentication sessions. The attackers were allowed to watch three recorded authentication sessions of 10 hard PINs each. They were allowed three guesses per PIN. The results of this custom setting found that the attacker failed to recover any of the hard PINs due to the equally likely OTP digits. That is, the proposed PIN-entry method with the hard PIN type is highly resistant to video-recording and spyware attacks. The nonrandom distribution of R digits eliminates the correlation between the authentication sessions and leads to narrowing down the PIN digit possibilities. Therefore, the random distribution of R digits helps the attackers to narrow down the PIN digits over trials.

One limitation of the proposed PIN-entry method is the weak resistance of the easy PINs against video-recording and spyware attacks. In the user study, the 4-digit PIN was employed to keep the method simple. Therefore, all easy PINs (except for the four-identical digits) are composed of only two distinct digits. As a result, the generated OTP pattern helps the attackers predict the PIN pattern and recover it. So, another custom setting of a 6-digit PIN is created so as to check if the PIN length affects the PIN type security (easy and hard) of the proposed PIN-entry method. The attackers were allowed to watch three recorded authentication sessions followed by three guesses. The results of this custom setting are summarised in Table 4. It is noted that the attackers succeeded to recover all PINs: two PINs in one recorded session, eight PINs in two recorded sessions, and two PINs in three recorded sessions. The proposed PIN-entry method requires attackers to assume the correct pair(s) (PIN digit(s), challenge digit(s)) that matches all OTP digits in order to recover the victim's PIN using the recorded challenge keypad. The probability of assuming the correct pair(s) using the 6-digit PIN is higher than the 4-digit PIN. Thus, the success in recovering two digits (a pair) of the 6-digit PIN can easily help the attacker to narrow down the possibilities and recover the PIN digits. Overall, the attack success rate is positively correlated with the PIN length.

E. USABILITY ANALYSIS

Usability is a key factor to consider when designing a secure PIN-entry method. Therefore, we analyzed the relative usability of the proposed PIN-entry method in terms of PIN-entry time, error rate, and learning effect and compared it to the regular PIN-entry method. A paired sample t-test was used to measure the effect of the PIN type as well as the PIN systems. A $p < 0.05$ is used for statistical significance level.

1) PIN-ENTRY TIME

We measured the PIN-entry time as the time a user takes to enter the 4-digit PIN. Fig 6 shows the average PIN-entry time for easy and hard PINs of the proposed and regular PIN-entry methods. We can notice that the average PIN-entry time of the proposed PIN-entry method is significantly longer than the regular one regardless of the PIN type ($p < 0.05$). This longer time of the proposed PIN-entry method results from OTP derivation. It is also noted that users took less time to enter their easy PINs (5.56s) using the proposed PIN-entry method than the hard ones (8.18s). This is attributed to the easiness of locating and calculating the repeated digits an easy PIN contains. The t-test analysis shows a significant effect of the PIN type (easy or hard) on PIN-entry time ($p = 0.023$). With respect to the regular method, the study results reveal no significant difference between easy and hard PINs on pin-entry time ($p = 0.73$).

TABLE 4. Recording attacks against 6-digit PINs entered through the proposed PIN-entry method.

PIN digits	Pattern	Attack status	No. of required recorded sessions
555555	1 distinct digit	Pass	One
333333	1 distinct digit	Pass	One
449499	2 distinct digit	Pass	Three
991991	2 distinct digit	Pass	Two
770977	3 distinct digit	Pass	Two
128222	3 distinct digit	Pass	Three
019112	4 distinct digit	Pass	Two
832818	4 distinct digit	Pass	Two
953192	5 distinct digit	Pass	Two
665498	5 distinct digit	Pass	Two
152698	6 distinct digit	Pass	Two
380791	6 distinct digit	Pass	Two

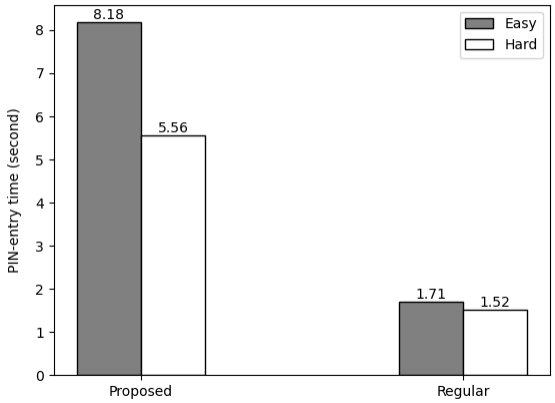


FIGURE 6. PIN-entry time for easy and hard PINs of the proposed and regular PIN-entry methods.

2) ERROR RATE

The error rate was classified into basic and critical. We measured the basic error rate as the number of failed login attempts for successful authentication sessions. The critical error rate was measured as the entirely failed authentication sessions. Participants were asked to enter their PINs 10 times with three attempts per entry. Fig 7 shows the results of the basic error rate of the easy and hard PINs of the proposed and regular PIN-entry methods. The results show that the proposed PIN-entry method is more error-prone than the regular one for both PIN types. These erroneous login attempts

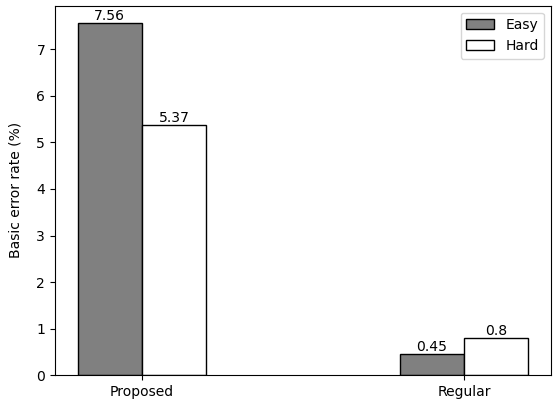


FIGURE 7. Basic error rate for easy and hard PINs of the proposed and regular PIN-entry methods.

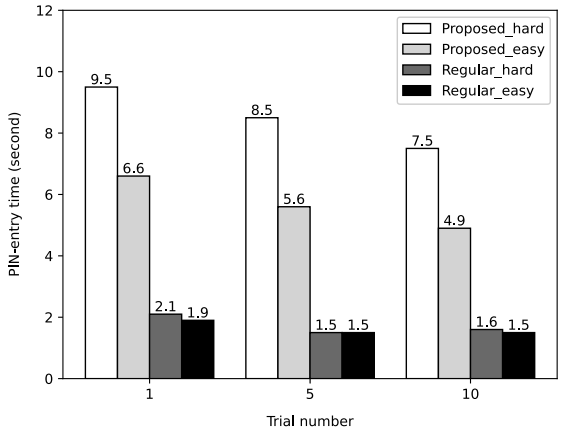


FIGURE 8. Variations in PIN-entry time over 10 trials using easy and hard PINs of the proposed and regular PIN-entry methods.

of the proposed PIN-entry method stems from deriving and entering the OTP in one attempt. Nonetheless, participants could perform 10 successful logins in 10 attempts with more than 90%. The t-test results show no significant effects of PIN type on the basic error rate for both PIN systems. For critical error rate, none of the participants failed any authentication session (i.e., all three attempts) for either method.

3) LEARNING EFFECT

We measured the learning effect among participants through the variations of the PIN-entry time over 10 trials. Fig 8 reveals a learning effect for both types of the proposed PIN-entry method in which the average PIN-entry time decreases with successive runs. This is because participants become familiar with the mechanism over time. The average PIN-entry time for both types of the regular method is relatively stable over time.

Multiple t-tests were performed to evaluate the statistical significance of differences in study outcomes among participants of different genders, ages, and educational levels. For example, two-sample t-tests (paired) were performed to determine if there is a significant difference between the average login times for males and females for easy and hard PINs. The sample data consisted of 21 males and 9 females for both PIN types. For easy PINs, the t-test yielded a p-value of 0.5012, which is greater than the significance level of 0.05. Therefore, it cannot be concluded that there is a significant difference between the means of the two groups. For hard PINs, the t-test yielded a p-value of 0.0563, which is also greater than the significance level of 0.05. A two-sample t-test was performed to determine if there is a significant difference between the average error rates of males and females for hard and easy PINs. The significance level for the test was set at 0.05. The t-test results show that there is no significant difference in error rates between males and females for hard PINs ($p = 0.1996$), but there is a significant difference for easy PINs ($p = 0.0734$). Furthermore, the t-test results revealed that the use of the proposed PIN authentication method varied significantly based on education and age in some instances but was not statistically significant in others. Overall, it is important to note that having a larger sample size would likely increase the accuracy of the t-test results, as it would provide a more representative sample of the population.

F. USER FEEDBACK

Participants were asked to evaluate the proposed PIN-entry method in terms of ease of use, usage, and security through a questionnaire. Figure 9 illustrates the questionnaire results using a 5-point Likert scale with a rating from 1 (strongly disagree) to 5 (strongly agree). Even though most participants considered that the regular PIN-entry method is more convenient than the proposed one, they agreed that the proposed PIN-entry method is easy to use. This result goes in line with the reported results of the user study regarding PIN-entry time, error rate, and learning effects in section IV-E. In the case of usage, most participants fully supported the use of the proposed PIN-entry method in critical-security situations, whereas they had different views regarding daily use. This indicates a clear inclination towards the proposed PIN-entry method. For security, all participants perceived the proposed PIN-entry method to resist shoulder-surfing and recording attacks (video and spyware). They also perceived that the proposed PIN-entry method is more secure than the regular one. This observation supports our previous findings in section IV-C, which shows that the proposed PIN-entry method (hard PIN) is secure against such attacks, and it outperforms the regular method.

G. COMPARISON WITH RELATED WORK

Table 3 shows a security and usability comparison of our proposed PIN-entry method with the regular PIN, LIN_4, SteganoPIN, and TTU. We compared our proposed PIN-entry method with the regular 4-digit PIN-entry method because it is still in use for most forms of user authentication. The other PIN-entry methods are the most relevant and best performing PIN-entry methods in terms of security and usability that employ the concept of OTP according to our systematic review [4]. The level of resistance against attacks has been categorized into vulnerable (not resistant to any session), low

TABLE 5. Comparison of PIN-entry methods.

PIN-entry Method	Security				Usability		
	SSA	Recording	Spyware	Guessing	PIN-entry Method	Error (basic)	Error (critical)
Regular	Vulnerable	Vulnerable	Vulnerable	$\frac{1}{10^4}$	1.62	0.63%	0
LIN_4 [31]	Moderate	Low	Low	$\frac{1}{10^3}$	8.9	N/A	0
SteganoPIN [22]	Moderate	Moderate	Vulnerable	$\frac{1}{10^4}$	5.7	1.1%	0
TTU [30]	Moderate	Moderate	Vulnerable	$\frac{1}{10^4}$	10.42	11.95%	9
Proposed (hard)	High	High	High	$\frac{1}{10^4}$	8.18	7.56%	0

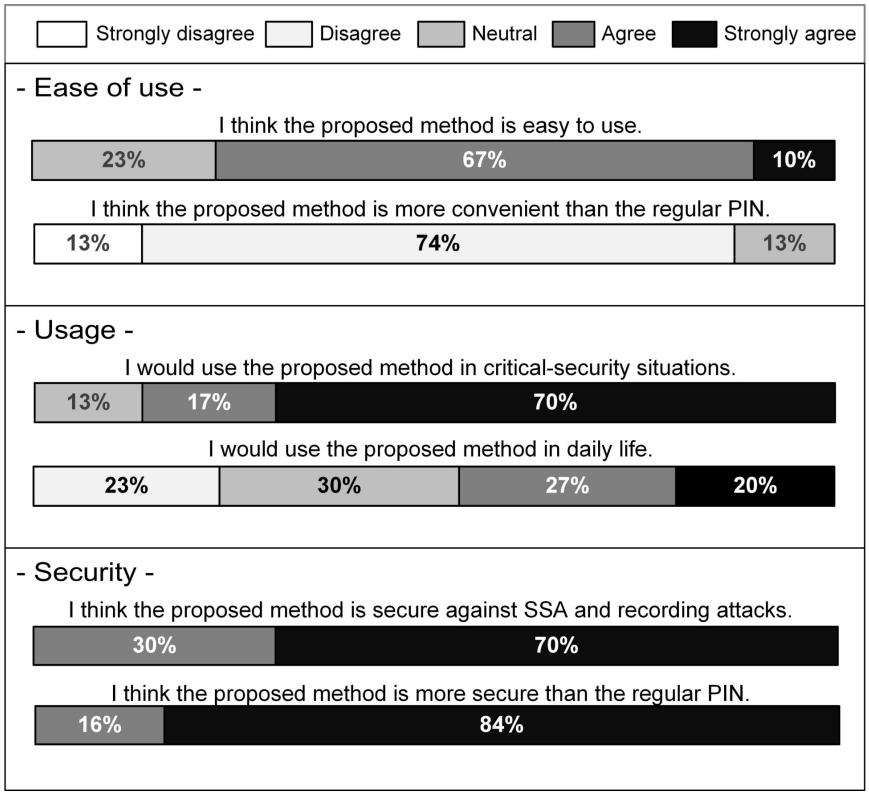


FIGURE 9. Participants' feedback of the proposed PIN-entry method in terms of ease of use, usage, and security.

(resistant to a single session), moderate (partially resistant), high (fully resistant), as described in Table 2.

The proposed PIN-entry method (hard) outperforms all other methods in terms of resisting shoulder-surfing, video-recording, and spyware attacks. This is because it drives users to enter an OTP for each authentication session. The employment of the mod 10 addition produces equally likely OTP digits. Besides, the nonrandom distribution of R digits eliminates the correlation between the authentication sessions, which leads to narrowing down the possibilities of the PIN digits. Thus, the attackers failed to recover any hard PINs.

It can be seen that StenagnoPIN and TTU are moderately resistant to both shoulder-surfing and video recording attacks. Indeed, these methods rely on the physical hand protection of the challenge. Therefore, improper user posture of the mechanism can reveal the PIN. Both StenagnoPIN and TTU are vulnerable to spyware attack because this type of attack cannot be defeated by physical protection. LIN_4 provides a moderate resistance against shoulder-surfing and low resistance against video recording and spyware attacks. The problem with this method is the correlation between the authentication sessions. The attacker needs only two captured sessions to identify the session key and then the original PIN. Shoulder-surfers may require multiple sessions to discover the PIN due to the limited cognitive capabilities of humans. The regular PIN-entry method is vulnerable to all three attacks because it does not provide any means of security. The likelihood of a guessing attack is $\frac{1}{10000}$ for all methods except LIN_4, which employs the first digit of the PIN to identify the session key. Regarding usability, the regular PIN-entry method outperforms all other methods due to the direct input of the PIN. Nonetheless, all methods except TTU match the condition of the secure human executable protocol in which users perform authentication within 10 seconds with at least a 90% success rate.

V. CONCLUSION

An indirect input PIN-entry method using OTP has been proposed to defeat shoulder-surfing, video-recording, and spyware attacks. The user study shows that the proposed PIN-entry method with the hard PIN type is immune to such attacks because of the employment of the OTP. The results of the custom settings illustrate that the random distribution of R digits assists attackers in narrowing down the PIN digits over trials, and the attack success rate is positively correlated with the PIN length. For usability, the proposed PIN-entry method maintains an acceptable level of usability with respect to PIN-entry time and error rate. The learning effects on PIN-entry time indicates that the proposed PIN-entry method could become more user-friendly by practice. User feedback supports our findings regarding the security and usability of the proposed PIN-entry method. Even though most participants considered that the regular PIN-entry method is more convenient than the proposed one, they agreed that the proposed PIN-entry method is easy to use. Moreover, they fully supported the use of the proposed PIN-entry method in critical-security situations, whereas they had different views regarding daily use. Comparing the proposed PIN-entry method with related work, it provides better security than all methods and an acceptable level of usability.

One limitation of the proposed PIN-entry method is the weak resistance of the easy PINs against recording attacks due to the limited number of distinct digits. In fact, all easy PINs (except the four identical digits) are composed of only two distinct digits. Therefore, the produced OTP is always composed of two distinct digits. Hence, attackers need only to assume the correct pair that matches all OTP digits to recover the victim's PIN with the help of the recorded challenge keypad. In future work, it may be desirable to develop a PIN checker to help users avoid easy PINs. Other points that we are interested in examining in the future work include the potential effect of elderly people and timing attacks on the proposed PIN-entry method's usability and security, respectively.

ACKNOWLEDGMENT

Farid Binbeshr would like to express his gratitude to the Hadhramout University and Hadhramout Foundation, Yemen, for their financial and administrative support.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surv.*, vol. 44, no. 4, p. 19, Aug. 2012.

[2] K. K. Greene, J. M. Franklin, K. K. Greene, and J. Kelsey, *Measuring the Usability and Security of Permuted Passwords on Mobile Platforms*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2016.

[3] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2006, p. 6.

[4] F. Binbeshr, M. L. Mat Kiah, L. Y. Por, and A. A. Zaidan, "A systematic review of PIN-entry methods resistant to shoulder-surfing attacks," *Comput. Secur.*, vol. 101, Feb. 2021, Art. no. 102116.

[5] A. T. S. Carneiro, C. E. L. Elmadjian, C. Gonzales, F. L. Coutinho, and C. H. Morimoto, "PursuitPass: A visual pursuit-based user authentication system," in *Proc. 32nd SIBGRAPI Conf. Graph., Patterns Images (SIBGRAPI)*, Oct. 2019, pp. 226–233.

[6] D. M. Ibrahim and S. Ambreen, "Gaze touch cross PIN: Secure multimodal authentication using gaze and touch PIN," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1, pp. 777–781, Oct. 2019.

[7] C. Kumar, D. Akbari, R. Menges, S. MacKenzie, and S. Staab, "TouchGazePath: Multimodal interaction with touch and gaze path for secure yet efficient PIN entry," in *Proc. Int. Conf. Multimodal Interact.*, Oct. 2019, pp. 329–338.

[8] S. M. H. Krishna, G. Pradyumna, B. Aishwarya, and C. Gayathri, "Development of personal identification number authorization algorithm using real-time eye tracking & dynamic keypad generation," in *Proc. 6th Int. Conf. for Converg. Technol. (I2CT)*, Apr. 2021, pp. 1–6.

[9] J. D. Still and J. Bell, "Incognito: Shoulder-surfing resistant selection method," *J. Inf. Secur. Appl.*, vol. 40, pp. 1–8, Jun. 2018.

[10] V. Sugumar and P. Soundararajan, "Cursor masquerade: Masking of authentic cursor using random numeric keypad and spurious cursors," in *Proc. 3rd Int. Conf. Adv. Electr., Electron., Inf., Commun. Bio-Informat. (AEEICB)*, Feb. 2017, pp. 80–84.

[11] M. M. Kabir, N. Hasan, M. K. H. Tahmid, T. A. Ovi, and V. S. Rozario, "Enhancing smartphone lock security using vibration enabled randomly positioned numbers," in *Proc. Int. Conf. Comput. Adv.*, Jan. 2020, pp. 1–7.

[12] G. Nandhini and S. Jayanthy, "Mobile communication based security for ATM PIN entry," in *Proc. Int. Conf. Comput. Netw. Commun. Technol.* Singapore: Springer, 2019, pp. 453–467.

[13] M. Guerar, M. Migliardi, F. Palmieri, L. Verderame, and A. Merlo, "Securing PIN-based authentication in smartwatches with just two gestures," *Concurrency Comput., Pract. Exp.*, vol. 32, no. 18, Sep. 2020, Art. no. e5549.

[14] K. Krombholz, T. Hupperich, and T. Holz, "Use the force: Evaluating force-sensitive authentication for mobile devices," in *Proc. 12th Symp. Usable Privacy Secur. (SOUPS)*, 2016, pp. 207–219.

[15] S. Rajarajan, R. Kalita, T. Gayatri, and P. Priyadarsini, "SpinPad: A secured PIN number based user authentication scheme," in *Proc. Int. Conf. Recent Trends Adv. Comput. (ICRTAC)*, Sep. 2018, pp. 53–59.

[16] Y.-X. Dan and W.-C. Ku, "A simple observation attacks resistant PIN-entry scheme employing audios," in *Proc. IEEE 9th Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2017, pp. 1410–1413.

[17] T. Perković, M. Čagalj, and N. Saxena, "Shoulder-surfing safe login in a partially observable attacker model," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Springer, 2010, pp. 351–358.

[18] G. Dhandapani, J. Ferguson, and E. Freeman, "HapticLock: Eyes-free authentication for mobile devices," in *Proc. Int. Conf. Multimodal Interact.*, Oct. 2021, pp. 195–202.

[19] N. Chakraborty, S. V. Anand, G. S. Randhawa, and S. Mondal, "On designing leakage-resilient vibration based authentication techniques," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 1875–1881.

[20] M.-K. Lee, H. Nam, and D. K. Kim, "Secure bimodal PIN-entry method using audio signals," *Comput. Secur.*, vol. 56, pp. 140–150, Feb. 2016.

[21] O. K. Kasat and U. S. Bhadade, "Revolving flywheel PIN entry method to prevent shoulder surfing attacks," in *Proc. 3rd Int. Conf. Converg. Technol. (I2CT)*, Apr. 2018, pp. 1–5.

[22] T. Kwon and S. Na, "SteganoPIN: Two-faced human–machine interface for practical enforcement of PIN entry security," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 1, pp. 143–150, Feb. 2016.

[23] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "SwiPIN: Fast and secure PIN-entry on smartphones," in *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst.*, Apr. 2015, pp. 1403–1406.

[24] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, Oct. 2004, pp. 236–245.

[25] A. Souza, Ì. Cunha, and L. B. Oliveira, "NomadiKey: User authentication for smart devices based on nomadic keys," *Int. J. Netw. Manage.*, vol. 28, no. 1, p. e1998, Jan. 2018.

[26] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja, "Comprehensive study of biometric authentication systems, challenges and future trends," *Int. J. Adv. Netw. Appl.*, vol. 10, no. 4, pp. 3958–3968, 2019.

[27] T. Van Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices," *Comput. Secur.*, vol. 66, pp. 115–128, May 2017.

[28] I. Das, R. Das, S. Singh, A. Banerjee, M. G. Mohiuddin, and A. Chowdhury, "Design and implementation of eye pupil movement based PIN authentication system," in *Proc. IEEE VLSI Device Circuit Syst. (VLSI DCS)*, Jul. 2020, pp. 1–6.
[29] N. Li, Q. Wu, J. Liu, W. Hu, B. Qin, and W. Wu, "EyeSec: A practical shoulder-surfing resistant gaze-based authentication system," in *Proc. Int. Conf. Inf. Secur. Pract. Exp.* Melbourne, VIC, Australia: Springer, 2017, pp. 435–453.
[30] D. Nyang, H. Kim, W. Lee, S.-B. Kang, G. Cho, M.-K. Lee, and A. Mohaisen, "Two-thumbs-up: Physical protection for PIN entry secure against recording attacks," *Comput. Secur.*, vol. 78, pp. 1–15, Sep. 2018.
[31] M.-K. Lee, "Security notions and advanced method for human shoulder-surfing resistant PIN-entry," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 695–708, Apr. 2014.
[32] S. Jain, S. Dabola, S. Binjola, and R. Jindal, "AlignPIN: Indirect PIN selection for protection against repeated shoulder surfing," in *Proc. 11th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2021, pp. 594–599.
[33] R. Alroobaea and P. J. Mayhew, "How many participants are really enough for usability studies?" in *Proc. Sci. Inf. Conf.*, Aug. 2014, pp. 48–56.
[34] J. M. Six and R. Macefield, "How to determine the right number of participants for usability studies," UXmatters, San Francisco, CA, USA, Tech. Rep., 2016.
[35] X. Bultel, J. Dreier, M. Giraud, M. Izaute, T. Kheyrkhah, P. Lafourcade, D. Lakhzoum, V. Marlin, and L. Motá, "Security analysis and psychological study of authentication methods with PIN codes," in *Proc. 12th Int. Conf. Res. Challenges Inf. Sci. (RCIS)*, May 2018, pp. 1–11.

FARID BINBESHR received the bachelor's degree (scientific excellence) in computer science from Hadhramout University, Al-Mukalla, Yemen, in 2009, and the master's degree in computer networks from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in 2014. He is currently pursuing the Ph.D. degree with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. He is currently a Lecturer with the Department of Computer Science, College of Computers and Information Technology, Hadhramout University. His areas of research interests include computer networks and computer security.

LIP YEE POR (Senior Member, IEEE) received the Ph.D. degree from the University of Malaya, Malaysia, in 2012. He is currently an Associate Professor with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology (FCSIT), University of Malaya, Malaysia. He has been the few among the first to obtain funds from the IRPA, E-Science, FRGS, ERGS, PRGS, HIR, and IIRG from FCSIT. Beside collaborators from Malaysia, he has international collaborators from France, U.K., New Zealand, Turkey, Hong Kong, and China. He has also established his connection with his national and international collaborators with some industrial partners in Malaysia and other countries. He has published more than 60 academic papers in respectable journals. He was the first few pioneers who managed to publish within top 1% ranking ISI journals from FCIST. He received a very good number of citations in the Web of Science database. He was also the first few pioneers who successfully filed a patent in FCSIT. Until now, he has filed up to eight patents and all the patents were granted. In general, his research interests include bioinformatic (e.g. biosensors, pain research), computer security (e.g. information security, steganography, authentication (graphical password)), neural networks (e.g. supervised and unsupervised learning methods such as support vector machine, extreme learning machine), grid computing, and e-learning framework.

M. L. MAT KIAH (Senior Member, IEEE) received the Ph.D. degree in information security from Royal Holloway, University of London, U.K., in 2007. Since then, she has been an Active Researcher with the Faculty of Computer Science and Information Technology, UM, in her computer science field particularly in security. She was promoted to Professorship, in 2015. She is an Active Member of EC Council, Malaysian Society for Cryptology Research (MSCR), and Malaysia Board of Technologists (Ts.). Her main research interest includes the security aspect of computing and technology fields with variation of applications in multi and/or trans disciplinary projects. This is evidenced by her publications and research projects in which she is/was the principal investigator (PI) as well as a co-PIs. As a professional technologist (Ts.), keeping up with the current trend and demand of ever evolving computing technology field is crucial to ensure the quality and the impact of her research work. Her current research interests include cyber security, blockchain technology, the IoT, and health information exchange.

A. A. ZAIDAN (Senior Member, IEEE) received the B.Eng. degree (Hons.) in computer engineering from the University of Technology, Baghdad, Iraq, in 2004, the M.Sc. degree in data communications and computer network from the University of Malaya, Malaysia, in 2009, and the Ph.D. degree in artificial intelligence from Multimedia University, Malaysia, in 2013. He is currently working as a Full Professor in data science and artificial intelligence at the SP Jain School of Global Management, Sydney, Australia. His research interests include artificial intelligence and decision theory.

MUHAMMAD IMAM received the B.Sc. and M.Sc. degrees in computer engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, and the Ph.D. degree in electrical and computer engineering from Carleton University, Ottawa, ON, Canada, in 2013. Since then, he has been working as an Assistant Professor with the Computer Engineering Department, KFUPM. His research interests include system logic design, network security, computer networking, and communication network protocols. In August 2017, he was assigned as the Director for Business Incubator Program at the entrepreneurship institute.