A Study on Using Emojis in a Shoulder Surfing Resistant Authentication Method

Mohamed Mahrous Amer, Yvonne Hwei-Syn Kam, and Vik Tor Goh

Abstract While images or emojis offer good memorability when used in an authentication method, inherently graphical data are highly susceptible to shoulder surfing attacks. An authentication system incorporating emojis was proposed and designed, which offers resistance to shoulder surfing attacks. The proposed system implements emojis in place of numerics in the reference method, DragPIN, and adds cue questions. The methods are compared in terms of performance and memorability, through user testing. The proposed authentication system was found to be successful at resisting shoulder surfing attacks. After 4–6 weeks, memorability was also higher in the proposed method compared to the reference method.

Keywords Graphical authentication system · PIN · Password · Emoji · Shoulder surfing

1 Introduction

User authentication systems must consider human factors such as ease of use and accessibility. Traditionally, alphanumeric passwords are perceived to have memorability predicaments. Graphical passwords use pictures instead of texts and are easier to remember than text-based passwords [1]. They provide a mechanism offering more user-friendly passwords. An advantage of graphical passwords is that they are easy to recall compared to alphanumeric passwords. However, while images or emojis might offer great memorability, inherently graphical data are highly susceptible to shoulder surfing attacks. Designing an effective graphical user authentication challenge scheme has been an ongoing subject of research for more than a decade. The

M. M. Amer · Y. H.-S. Kam (✉) · V. T. Goh
Multimedia University (MMU), 63000 Cyberjaya, Selangor, Malaysia
e-mail: hskam@mmu.edu.my

M. M. Amer
e-mail: 1151102010@student.mmu.edu.my

V. T. Goh
e-mail: vtgoh@mmu.edu.my

H. Kim and K. J. Kim (eds.), *IT Convergence and Security*, Lecture Notes in Electrical Engineering 782, https://doi.org/10.1007/978-981-16-4118-3_7

challenge is managing the tradeoffs between the competing requirements of usability, memorability, and security.

2 Literature Review

Graphical passwords can offer advantages with regards to memorability and safety. The memorability can be explained by a hypothesis called the pictorial-superiority effect. The pictorial-superiority effect is a hypothesis that claims that a person can more easily recall graphical data than a text [1]. In an attempt to mitigate the risks associated with the vulnerabilities of Graphical authentication systems towards shoulder surfing attacks, Srinivasan proposed DragPIN [2]. Two schemes were created; manual and auto sliding. The proposed system revolves around a four-by-ten grid Personal Identification Number (PIN) entry scheme with characters that move automatically or manually. This system uses a four-digit PIN.

Figure 1 illustrates the DragPIN scheme. It has a manual and auto-sliding variant. The login process of the manual variant is initially commenced by mentally choosing an alphabet letter. Users must then use either the left or right arrow keys to move the alphabets in the left or right direction by remembering the digits of the PIN so that the chosen alphabet on the Nth row is located on a column number equal to the Nth PIN. For example, let the PIN be 5269. In Fig. 1, 'E' is the chosen letter which the user moves until it is aligned with each of the PIN digits. The automatic variant auto slides the rows and the user has to click at the right time to select the PIN digit. The advantage of DragPIN is that it is shoulder surfing resistant, especially its auto-sliding variant. The display in its auto-sliding variant does not directly correspond to the fixed password making it more difficult to reconstruct or deduce the fixed PIN from the result. In contrast, the password candidates of some shoulder-surfing resistant schemes can reduce radically after one observation [3].

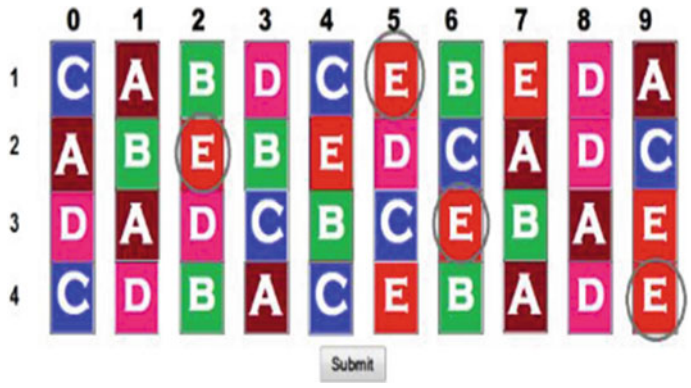


Fig. 1 Screenshot of DragPIN scheme [2]

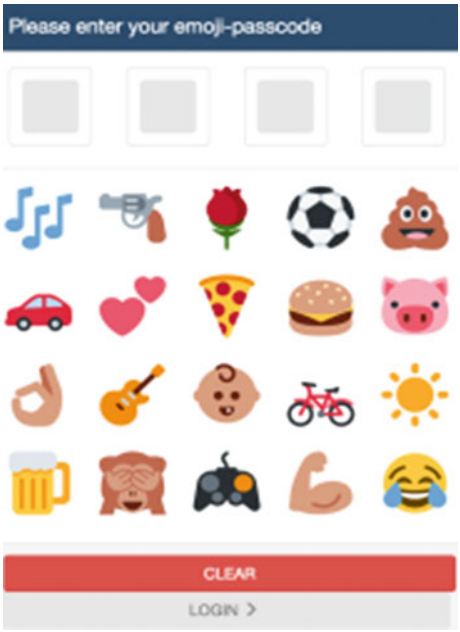


Fig. 2 Screenshot of EmojiAuth system [4]

While DragPIN achieved sufficient results in ensuring the resistance to shoulder surfing attacks, it may lack the ease of memorability, as common with methods that use alphanumeric passwords. This could be enhanced by using images rather than digits. Emojis are said to be familiar to users and can be expressed into memorable stories [4]. EmojiAuth [4] is an emoji-based authentication method. Figure 2 below demonstrates the login interface of the system. It is vulnerable to shoulder surfing because a potential shoulder surfer could watch the user as he/she selects the icons to enter his/her emoji password.

A highly effective approach to resisting shoulder surfing is by creating a secret channel between the system and the user to send information, which can cue the user in entering their session password. These channels could be, for example, audio [5], tactile [6], etc. A downside is that additional hardware or capabilities are needed to achieve these secret channels. Binbeshr et al. [7], suggested that future research should focus on methods that do not require an additional channel and/or hardware to ensure its acceptance and adoption.

Table 1 lists the advantages and disadvantages of related works. The methods [5] and [6] both require additional channels and thus additional hardware. Both DragPIN [2] and the methods in [3] and [8] are resistant to shoulder surfing without requiring additional hardware. The auto sliding variant implemented by DragPIN has the advantage where the displayed state does not directly correspond to the fixed password, which makes it more shoulder-surfing resistant. In [3], the fixed password can be deduced after multiple observations. In [8], intersection attacks on multiple observations can also narrow down candidates.

Table 1 Advantages and disadvantages of reviewed systems

Paper	Advantages	Disadvantages
Srinivasan [2]	Resistant to shoulder surfing attacks The display does not directly correspond to the fixed password (auto-sliding variant)	Numbers are not as memorable as pictures
Salman et al. [3]	Resistant to shoulder surfing attacks	Vulnerable to intersection attack, with multiple observations
Kasat and Bhadade [8]	Resistant to shoulder surfing attacks	Vulnerable to intersection attack, with multiple observations
Rajarajan et al. [5]	Resistant to shoulder surfing attacks	Additional hardware/capabilities needed (earphones)
Ku and Xu [6]	Resistant to shoulder surfing attacks	Additional hardware/capabilities needed (vibration)
Golla et al. [4]	Memorable and easy to use	Not resistant to shoulder surfing attacks

To summarise, DragPIN proposed a graphical authentication system for resisting shoulder surfing attacks. However, it uses numbers, which are not as memorable as pictures. EmojiAuth proposed a very easily memorable and useable system. But it is not resistant to shoulder surfing attacks. Both these methods came with their associated disadvantages. Therefore a proposed system using emojis instead of digits in DragPIN can achieve memorability and resistance to shoulder surfing attacks while solving both systems' disadvantages, while not losing their particular advantages.

3 Methodology

Both DragPIN and EmojiAuth methods were implemented to better understand their workings. A prototype of DragPIN was created as a proof of concept. As illustrated in Fig. 3, a signup page that allows a user to register a 4-digit pin and a username were created. The login scheme proposed in DragPIN was also implemented. The interface allowed users to sign in using the manual and automatic variants shown in Fig. 4.

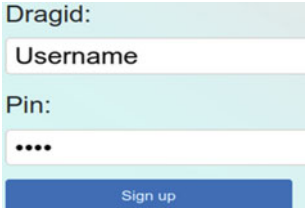


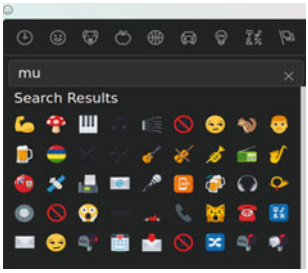
Fig. 3 DragPIN prototype
Sign up page

Fig. 4 DragPIN prototype (DragPIN auto sliding variant shown)

Figure 4 shows our implementation of the DragPIN interface. The login process of the manual variant was as described in Sect. 2. The auto sliding (or automatic) variant automatically slides the rows and the user has to click at the right time to select the PIN digit. The login process of the automatic scheme is commenced similarly by mentally choosing an alphabet letter then pressing the start button. This is followed by clicking the Spacebar once when they see their preferred alphabet appearing at the same column as their first PIN digit. The first row continues to slide, however. The user needs to press the Enter key to stop the sliding of the first row and to begin the sliding of the second row. The slipping of the second row then begins. The process is repeated for the four digits of the PIN. Then a prototype for EmojiAuth was created. The signup page allowed users to register a username and an emoji password. A login page (Fig. 5) allowed the user to input his/her previously registered username and emoji password using an online rendered emoji keyboard (shown in Fig. 6) or the emoji keyboard available on most smartphones.

Fig. 5 EmojiAuth prototype sign in

Fig. 6 Emoji Keyboard



3.1 Proposed Method Design

The proposed system was designed as a web application. To achieve better memorability, emojis are implemented rather than the PIN digits in DragPIN. The user only submits four emojis for each of the two passwords needed to register. Therefore, the system randomly generates six more decoy emojis from Unicode 'version six' to allow for $4 + 6 = 10$ emojis to be placed as table column indexes which are only generated by the system once and stored. For a particular user, the same set of emojis is shown at every login. To achieve memorability and usability, cue questions were added to the method, which was not in DragPIN. Cue questions are used to provide a cue for the particular password expected during authentication. Shoulder surfing resistance is enhanced as there are two cue questions, where the attacker may not be challenged with the same cue question as the one observed. Figure 7 below further illustrates the proposed usage of cue questions. The cue question is created by the user and ideally ultimately creates a virtual mental channel in which the system would seem to communicate details about the password to the user. Each user is required to register two cue questions associated with two passwords consisting of four emojis each, as shown in Fig. 7 below. For each login session, the column indexes are rendered by the system along with a random cue question allowing users to login using either the first or second emoji password.

Users are then expected to submit their username in the form shown in Fig. 8 below as the first part of a two-part login process. During this phase, Cross-site request forgery (CSRF) tokens are generated and passed with the form to the user. Those tokens get checked as well as the requested username. A CSRF token is a unique secret value generated by the server-side application. This token is sent to the client so that it would be checked after being sent back in a subsequent HTTP request made by the client. An example of the usage of CSRF tokens in the proposed system is shown in Fig. 9.

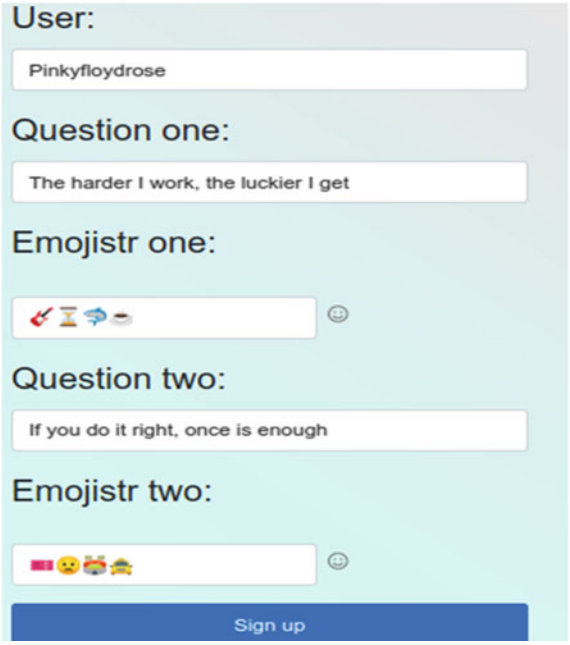


Fig.7 Proposed method Sign up page

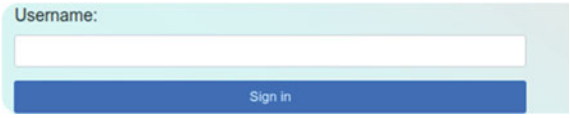


Fig. 8 Proposed method Sign-in page

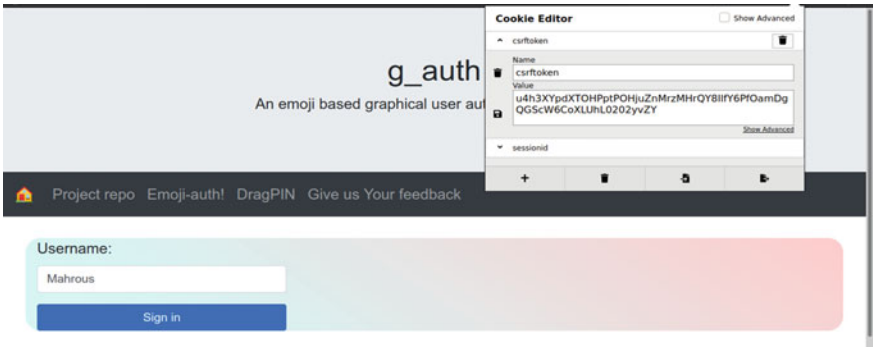


Fig. 9 CSRF token

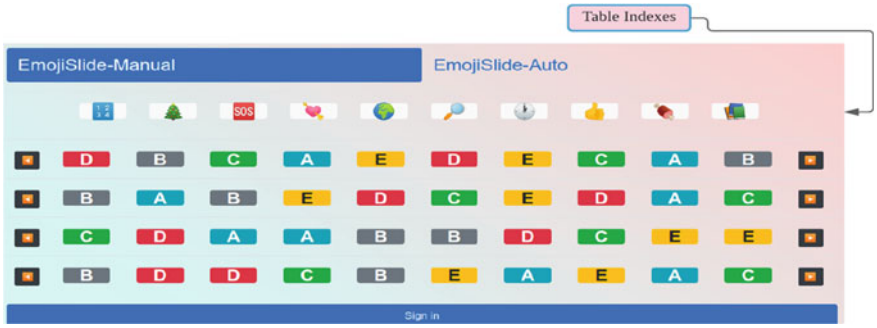


Fig. 10 Proposed manual implementation

3.2 Authentication

During authentication, a user may choose to authenticate via the manual or the automatic scheme. If the manual scheme shown in Fig. 10 is chosen, the user needs to mentally pick a color or a character to represent his marker. The user's four emoji password could be for example 🔢, 👆, 🕐, 🆘. The icons may look slightly different on different platforms. The arrows located at both ends of each row move the chosen color/letter under the first emoji in the password. The process is repeated for the remaining three emojis in the password. In Fig. 10, the chosen letter was 'D' and this letter was aligned to the emojis in the password.

Otherwise, if the automatic scheme (Fig. 11) is chosen, similar to the manual variant, firstly the user needs to pick a color or a character to represent his marker. Secondly, the user's four emoji password (e.g. 🔢, 👆, 🕐, 🆘) is then mapped by allowing the first row to shift until the chosen color/letter is in the required position. The "space" key is pressed to record that entry and the process can be commenced in the second row by pressing the "enter" key to stop the existing row from shifting and begin shifting the second row. The same technique is constant throughout the rest of the rows thus the process is repeated for the remaining emojis in the password. In Fig. 11, the chosen letter was 'B' and the user pressed the "enter" key after the row had slid past the password emoji. That is the reason the letter 'B' is no longer under the corresponding emojis. This misalignment resists shoulder surfing.

3.3 User Test Study

In the first phase, we invited participants to a google meet that was being recorded for later evaluation on the ability of this scheme to resist shoulder surfing. Initially, the motives behind the system were briefly explained. A test user was then created while explaining each field on the sign-up page. The participant (or user) then attempted to log in using the test user account, using each of the implemented schemes in both

Fig. 11 Proposed automatic implementation

DragPIN and EmojiSlide (our proposed method). This enabled the users to fully understand the login process associated with both schemes of the authentication systems. Next, users were instructed to register. The users had to create two cue questions and their corresponding emoji passwords. Some users resorted to creating an emoji password that resembled a story. They then attempted to authenticate. Participants were given only 3 consecutive attempts to log in. None of the users failed 3 consecutive attempts. Users registered and logged in using both schemes. In both, the time needed for the users to successfully authenticate was recorded. An understanding of what users thought of the system was reached by allowing the users to answer a quick survey upon completion of the experiment. To test for shoulder surfing resistance, in the first phase, shoulder surfing was carried out on the user login video recordings. Four "shoulder surfers" were first subjected to a demo round in which each created a user and tried logging in to gain an understanding of each of the schemes. Each shoulder surfer was then given the video recordings of the logins performed by the users, to attempt a shoulder surfing attack. In the second phase, users from the first phase were tasked to log in again, to test for memorability of the emoji passwords vs PINs. This phase was held from four to six weeks after the initial tests.

4 Results

There were 30 participants in the study. The age groups of the participants who participated are shown in Fig. 12. Most of them (76.7%) were between 20 and 30 years old. Table 2 below summarises the different aspects of the participants that contributed to this study. A note about the 26.7% of participants who claimed to be computer savvy. They were faster and tried to protect their identity by using a variation of less commonly used emojis that did not relate to their cue question at the first glance.

Each of the participants attempted to login to two methods with two variants each (EmojiSlide Manual, EmojiSlide Automatic, DragPIN Manual, and DragPIN Automatic). Table 3 shows the average time needed for the participants to login using each of the schemes, with the two variants each. When comparing the login time

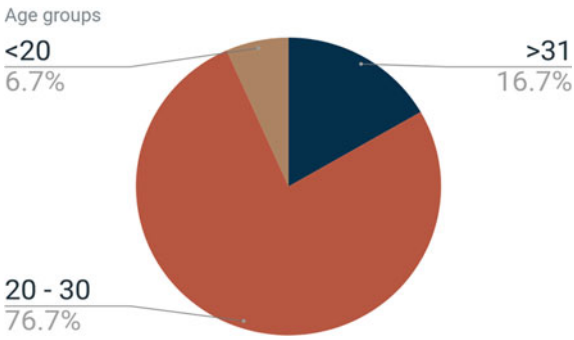


Fig. 12 Age groups of users

needed for DragPIN vs EmojiSlide, users took less time to login using EmojiSlide. Results also showed that the automatic variants required more time than the manual variants. Users were requested to rate their trust in the system as being shoulder-surfing resistant by the question shown in Fig. 13. The figure shows that 76.7% of participants felt that they can trust this system to resist shoulder surfing. 23.3% of participants were unsure and none (0%) of the participants answered no to this question.

The shoulder surfers described trying to observe the users' passwords as an "excruciating task". They also commented that reversing the recorded videos or slowing the playback did not help much in identifying the password. This was especially true for the automatic variants. None of them were able to get any full PIN or emoji password. They were only able to get a maximum of two emojis right, from three users, which was due to those users pointing their cursor at their desired emoji. None of the participants took more than three tries to log in to both the proposed system and DragPIN implementations. Most were in the DragPIN auto variant during phase 1, where three participants took three tries to log in. The proposed system has a higher average partial success rate and higher memorability as apparent in Fig. 14. The partial success rate is calculated as such: for each participant, if a successful login is made in one attempt, the success rate is 100%, if in two attempts, the success rate is 1/2 or 50% and if in three attempts, the success rate is 1/3 or 33.33%. The average partial success rate is taken as the average across all participants. After 4–6 weeks, during the phase 2 evaluation, the partial success rate of the proposed system was still higher compared to DragPIN. The percentage of decline was also smaller. User testing of the proposed scheme showed that users were able to enter their graphical passwords with high accuracy. Enhanced memorability was also achieved by implementing emojis in DragPIN schemes.

Table 2 Summary of the participants

	Males	Females	Graduates/Employed	Undergraduates	Computer savvy users	Average computer users	Non-frequent computer users
Percentage (%)	66.66	33.33	26.67	73.33	26.66	53.33	20

Table 3 Average login time

Parameters	DragPIN manual	DragPIN automatic	EmojiSlide manual	EmojiSlide automatic
Average login time (s) seconds	19.3	30.1	16.7	29.5

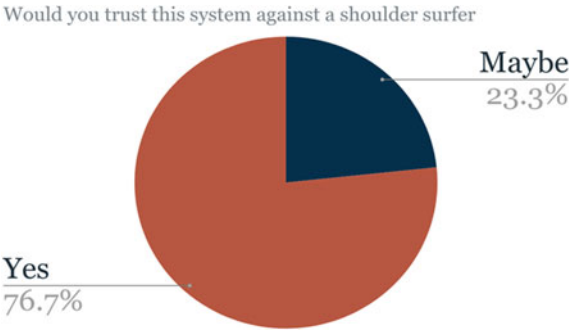


Fig. 13 Users' trust in the proposed system to resist shoulder surfing

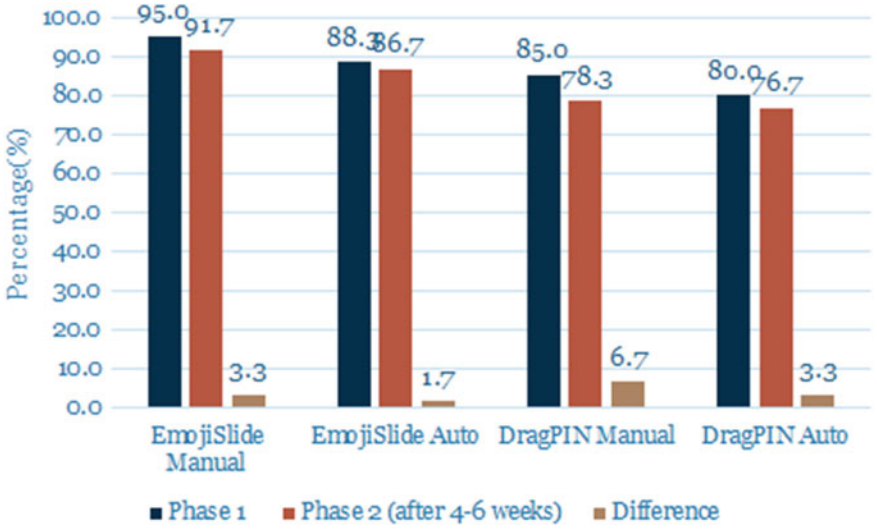


Fig. 14 Average success rate (including partial fails) in EmojiSlide and DragPIN during phase 1 and phase 2

5 Conclusion

In this paper, a graphical authentication method was proposed where it was shown to be shoulder surfing resistant as well as memorable. The proposed system implements emojis in place of numerics in the reference method, DragPIN, and in addition, implements cue questions that aid memorability while improving theoretical shoulder surfing resistance. A user study was carried out and participants demonstrated the features of high usability and security in the proposed method. Memorability was tested by having the same participants log in using the methods, four to six weeks after the initial phase. The result showed a higher partial success rate for the proposed method compared to the DragPIN implementation. The proposed method (both manual and auto-sliding variants) showed resistance to shoulder surfing in a recording-based shoulder surfing experiment, where none of the shoulder surfers managed to obtain the passwords.

Acknowledgements This work was supported by the Malaysian Ministry of Higher Education, Fundamental Research Grant Scheme (FRGS) [grant number FRGS/1/2015/ICT04/MMU/03/6]; and Multimedia University IR Fund [grant number MMUI/210071-IR Fund].

References

1. Paivio A, Csapo K (1973) Picture superiority in free recall: imagery or dual coding?. Cogn Psychol 5(2):176–206
2. Srinivasan R (2018) DragPIN: a secured PIN entry scheme to avert attacks. Int Arab J Inf Technol 15(2):213–223
3. Salman M, Li Y, Wang J (2019) A graphical PIN entry system with shoulder surfing resistance. In: 2019 IEEE 4th international conference on signal and image processing (ICSIP). IEEE, pp 203–207
4. Golla M, Detering D, Dürmuth M (2017) EmojiAuth: quantifying the security of emoji-based authentication. In: Proceedings of the usable security mini conference (USEC)
5. Rajarajan S, Kalita R, Gayatri T, Priyadarsini PLK (2018) Spinpad: a secured pin number based user authentication scheme. In 2018 international conference on recent trends in advance computing (ICRTAC). IEEE, pp 53–59
6. Ku W, Xu H (2019) Efficient shoulder surfing resistant PIN authentication scheme based on localized tactile feedback. In: 2019 6th IEEE international conference on cyber security and cloud computing (CSCloud)/ 2019 5th IEEE international conference on edge computing and scalable cloud (EdgeCom), pp 151–156
7. Binbeshr F, Kiah MM, Por LY, Zaidan AA (2020) Systematic review of PIN-entry methods resistant to shoulder-surfing attacks. Comput Secur 102116
8. Kasat OK, Bhadade US (2018) Revolving flywheel pin entry method to prevent shoulder surfing attacks. In: 2018 3rd international conference for convergence in technology (I2CT). IEEE, pp 1–5