Asian Journal of Research in Computer Science

9(2): 59-69, 2021; Article no.AJRCOS.69289
ISSN: 2581-8260

Smart Android Graphical Password Strategy: A Review

Guhdar Yousif Izadeen[1*] and Siddeeq Y. Ameen[1]

[1]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.

Authors' contributions

This work was carried out in collaboration between both authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v9i230220
Editor(s):
(1)Dr. G. Sudheer, GVP College of Engineering for Women, India.
Reviewers:
(1) Mishall Al-Zubaidie , Thi-Qar University, Iraq and University of Southern Queensland, Australia.
(2) Radael de Souza Parolin, Federal University of Pampa, Brazil.
(3) LIENOU Jean-Pierre , The University of Bamenda, Cameroon.
Complete Peer review History: http://www.sdiarticle4.com/review-history/69289

Review Article

Received 25 March 2021
Accepted 03 June 2021
Published 03 June 2021

ABSTRACT

In recent years, when users across the world have embraced smart devices in greater numbers owing to recent advances and appealing applications, they have also become a target for criminals who are zealously attempting to breach protection. As a result, a significant number of attacks have been observed on these systems. As a result, several password-based authentication mechanisms have been proposed to counteract these attacks. Among them, the graphical password scheme is more consistent with smart devices, which are highly graphic-oriented. However, current graphical password schemes are vulnerable to a variety of assaults, including shoulder surfing, smudging, intersection attacks, and reflection attacks. Thus, the paper aims to review recent published papers on android smart phone graphical password and identify used techniques. Moreover, the paper analyzes results to give better understanding for users of such devices to protect their devices from unauthorized access and attacks.

Keywords: Android; smart devices authentication; graphical password; Information security; attacks.

1. INTRODUCTION

Password protection analysis is an essential aspect of machine and accessible security. Passwords have shown to be a challenging to be chosen by humans and not much used in password schemes, as the method of utilizing mnemonic or randomly created passwords

**Corresponding author: E-mail: guhdar.youcif@dpu.edu.krd;*

usually means that people choose passwords [1-5]. With the launch of smartphones and tablets, the unlock authentication options used to lock and unlock mobile devices have become extremely relevant in terms of information protection as shown in Fig. 1. There are two major dominant smartphone systems, iOS and Android, each with a native solution to unlocking. Although secondary and knowledge-based authentication, including fingerprints or face recognition, are essential, passcode-based authentication is still the primary means for mobile device security. The iPhone's most popular passcode-based authentication mechanism is via a PIN that consists of at least of 4-digit complexity (last updates may require a 6-digit). After its introduction, Android has provided a broader range of unlock authentication methods, such as text-based passwords, PIN, facial recognition, and, most notably for this article, the graphical password pattern. Android unlocks has been shown to be effective in many situations and after it became broadly implemented, it has been analyzed by many applications in various contexts. In the first case, studies of unlock style authentication [5-10].

The iPhone's most popular passcode-based authentication mechanism is via a PIN consisting of at least 4-digit complexity (last updates may require a 6-digit). After its introduction, Android has provided a broader range of unlocking authentication methods, such as text-based passwords, PIN, facial recognition, and, most notably for this article, the graphical password pattern. Android unlocks be effective in many situations, and after they became broadly implemented, many applications have been analyzed in various contexts. In the first case, studies of unlock style authentication [7-13] showed that Android patterns remain reasonably common as an option of authentication. Various experiments [14-22] have also looked at how people select graphical login patterns on their Android devices. If there are some adjustments to the device [15, 23-25], some examples include changing the contact points, and password meters are indicators of strategies to influence preference [2,26-28] demographic considerations in the collection [10, 29, 30]. The paper includes a detailed overview and categorization of methods and strategies for compilation in other taxonomy documents. It provides owners of those systems with a clearer view of protecting their appliances from unwanted entry and attacks [2, 15, 21, 31].

2. SMART ANDROID AUTHENTICATION SECURITY

An authenticator is a device used to verify a user's identification or conduct automated authentication. Through proving that he or she has ownership and control of an authenticator, an individual may authenticate to a computer device or program. The authenticator is, in the most basic situation, a generic password. The group that has to be validated is the complainant in the NIST Digital Identification Guidelines, whereas the party who verifies the claimant's identity is referred to as the verifier. The verifier may infer the claimant's identity if the claimant effectively demonstrates ownership and control of one or more authenticators to the verifier using a defined authentication procedure [32-36].

2.1 Smart Android Graphical Pattern Password

A template lock enables the phone to be unlocked only after the correct pattern is mapped out on a three-by-three rectangle, as shown in Fig. 1. When a user becomes used to this natural and automatic lock, it becomes a straightforward way to enter a handset, and if all nine dots in the pattern are used, there are nearly 400,000 available access codes [37]. Unfortunately, there are some areas where the pattern lock falls short. When the pattern is recreated successfully, it is possible to access the device. Fig. 1 shows an illustration of appropriate strokes from the upper left corner.

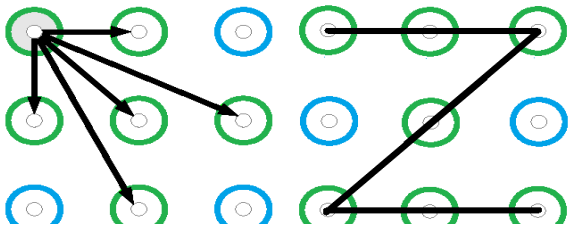

Fig. 1. Touchpoints that can be reached in a 3x3 pattern Unlock from the top left touch spot

2.2 Methods for Graphical Passwords

Graphical password strategies have been proposed to address shortcomings of traditional text-based password techniques since images are more straightforward to recall than texts. Some current graphical passwords are as follows [38]. Graphical password techniques demonstrate that the techniques can be grouped into four categories. A Recognition-based technique: Users pick pictures, icons, or symbols from a picture set in this group. Upon authentication, users need to remember their pictures, symbols, icons chosen during registration between a series of photographs [39];

a. Recognition-Based Method: Users can choose icons or pictures from a collection of images presented at the graphical user interface in this technique. Users select their photos at the time of authentication from a list of chosen images at the time of signup [40, 41].

b. Pure Recall-Based Method: Users are required to write their codes without any clues or reminders. Even though this method is more efficient and straightforward, people cannot recall their passwords [42].

c. Cued Recall-Based Method: Users are sent reminders or hints throughout this technique. Users may use prompts to help them remember their passwords or help them type or pick their passwords more accurately. This approach is similar to recall-based systems but with the use of cues.

d. Hybrid Method: Authentication is done with a mixture of two or more schemes. This method eliminates the issues associated with other schemes, such as spyware, shoulder surfing, and so on [43].

Fig. 2 illustrates different methods types of the graphical password [39].

2.3 Unlock Choices for Android Smartphone Authentication

a. Password: A well-thought-out password, the old classic in protection, may be a potent security mechanism, but a password with no work placed into it may just as quickly be a significant security danger. Despite this, the best protection mechanism possible for a user's mobile device is a password (or its cousin, the passcode). However, one big drawback with the password: entering it each time the phone has to be accessed easily becomes cumbersome and awkward.

b. PIN Number: A PIN code, like a password, is a surprisingly secure authentication method since the standard 4-digit alternative has over 10,000 possible variations. While a 16-digit PIN is admittedly challenging to recall, an Android computer may be covered by a 16-digit PIN, taking the total amount of valid codes to 10 quadrillion. The PIN, though, has a flaw in that many people can yield to the lure of creating an oversimplified PIN that could be estimated very quickly.

c. Fingerprint Scanner: For exemplary purposes, this method of unlocking a mobile device has quickly become the preferred method: not only is it secure, but it is also relatively easy. However, even this approach has shortcomings. E.g., the fingerprint scanner is not often placed in the most comfortable location on the handset. Furthermore, gloves render this process difficult to use.

d. Facial Recognition: Under the current state of affairs, this is likely to become the preferred means of verifying user identification to gain access to a phone shortly. However, in their current form, these approaches are not yet reliable enough to securely authenticate items like transactions and other financial tasks, but that is changing.

e. Smart Lock: Safety capabilities are available on several phones today, depending on alternate authentication forms. Whenever the gadget is held, body tracking holds it free - independent of who has it. It is also possible to teach a computer to confide in specific locations, computers, and faces. Another choice is to open the user's telephone using Google Assistant by saying "Yes, Google." These characteristics are, however, not so well for user safety and are primarily for convenience. As previously reported, Users with more modern mobile devices may also choose a biometric, such as a fingerprint or facial recognition. However, since they must also choose a PIN or pattern in this environment, we place the

biometric options above the primary options. Furthermore, an intruder targeting an authentication scheme is likely to concentrate on knowledge-based attacks—that is, attacks that can be guessed or enumerated—which means that the user's option of authentication secrets is still essential. The graphical login pattern is not the only way to secure users. A variety of experiments have looked at consumer preference for PINs and passwords [44].

From 2017 to 2021, a variety of reports on the mobile device accessing actions have been released. According to these studies, users consider patterns as more stable and less error-prone than PINs in entry, but in fact, the reverse is also accurate. In general, these findings indicate that more research into Android's graphical password scheme is essential. Even though certain users think other options are safer, this alternative is expected because of the users' belief that it safeguards their phones from unauthorized users [45].

2.4 Protection of Android Smartphone Graphical Password

In a recent study, it was said that it is possible to calculate a graphic password by analyzing the movement of the fingers when drawing a pattern (key) captured on video. It should be noted that the video can be made at a distance of two meters from the user, for example, in public places. Users can check the fingerprints left by the owner on the device screen, but this is ineffective as a rule since users usually have to deal with many paths Fuzzy or worn out [46]. To maintain the Security of the graphic password, cases such as using further intersections, which will select variations that can help confuse the intruder, turning off the "display pattern" option in the operating system settings in the Android OS. After lines, this function is disabled. The between the points will not be visible on the device screen, and turning off the device screen at the moment are recommended. A visual password is entered, preventing an intruder from eavesdropping on a user's password [47].

3. LITERATURE REVIEW

Graphical passwords are security mechanisms that rely on expertise. Many general suggestions and implementation guidance have resulted from thorough research into the effects of various factors on knowledge-based authentication, with a particular emphasis on text passwords. Rather than repeating those, we would concentrate on similar work that is closely related to graphical passwords. Furthermore, it can be divided into four types as shown following:

3.1 Graphical Password for Childs

[48] They investigated graphical passwords as a child-friendly solution for user authentication. They assessed the usability of three versions of the Pass Tiles graphical password system for children and the similarities and disparities in performance and preferences between children and adults when utilizing these systems. Children were the most effective at remembering passwords that included pictures of particular items. Both children and adults choose graphical passwords to their current systems, but their password memorization methods vary significantly. Based on their findings, they made suggestions for developing more child-friendly authentication systems. Also, [49] They

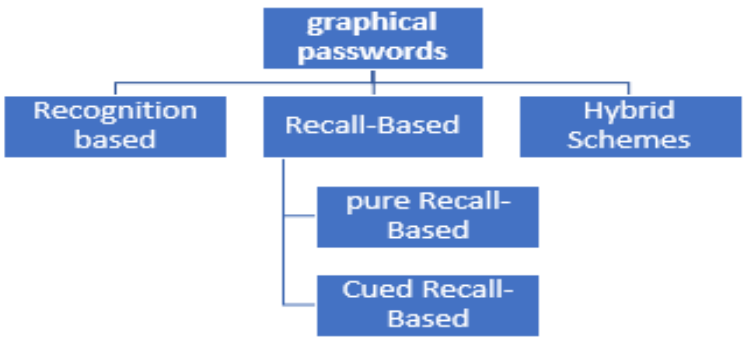

Fig. 2. Categorization of authentication methods for the graphical password

suggested Graphical Password Authentication for Child Personal Storage Program, an application that would offer personal storage for children to save their notes in softcopy formats. The suggested system's use of graphical password protection is meant to encourage children to use passwords to protect their files in a fun way. The proposed framework was created using the Android mobile application platform, and the project's approach was Object-oriented Mobile Application Development. The technical specifications of the proposed framework were introduced based on user requirements, and the programming interfaces were also implemented based on user characteristics. The project's value lies in raising children's understanding of the importance of safe file storage. Children who will use graphical passwords while they are young will benefit in the future, and it will make sense to preserve their privacy by putting up a password. In terms of information protection, the suggested scheme mentions authentication, anonymity, and availability as qualities that would be accomplished.

3.2 3D Graphical Password

[39] They proposed a new authentication scheme based on 3D graphical keys, which they tested to make mobile devices safer. This authentication mechanism enables users to communicate with 3D artifacts in a simulated world, with their behavior being recorded and used to generate unique passwords. They created a basic research application based on previous studies of the 3D password scheme to construct their own 3D password. Also, [50] described that the 3D password is a multifactor authentication system that can merge many authentication techniques into a single 3D virtual world. The user will browse and communicate with different things. The series of behaviors and experiences inside the 3D world creates the user's 3D password. The 3D Password is the strongest tool for having encryption since it can be used with any mixture of passwords. It is more powerful than other authentication methods, because it is a highly reliable authentication scheme. Furthermore, it explains how the intruder can obtain awareness of the most probable assaults. Shoulder surfing assaults are still feasible and successful against 3D passwords.

3.3 Map-Based Graphical Password

In reference [51], they showed that graphical passwords (GPs) might be a viable solution to traditional authentication schemes. Map-based GPs (geographical passwords), which enable users to choose one or more locations on a map for authentication, have been designed to provide an expansive password room. PassMap, for example, allows users to select two locations as their keys, while GeoPass only requires users to select one. According to some tests, using just one location as a password is insufficiently safe, while using two positions reduces device usability. They performed a study to see if users might choose between two PassMap locations and discovered that users could choose between identical locations due to time constraints. They developed CPMap, a click-points map-based GP scheme that enables users first to pick a position on a world map and then click a point or an item on a picture related to that location. They performed a second usage analysis of up to 50 users to investigate the success of CPMap. It has been discovered that our scheme will provide consumers with positive outcomes in terms of protection and usability.

In reference [52], they suggested a new password scheme for mobile Android devices that is map graphical-based. This algorithm benefits from allowing for randomization and selection order, making it less susceptible to brute-force and shoulder-surfing assaults. For mobile Android application, this algorithm enhanced the map graphical-based password authentication scheme. As a result, the device has been changed and rendered safer. This approach is appropriate for software locks on mobile devices. When a user inputs his or her graphical password, the device obtains the period and all protection features, so consumers are not burdened in any way. When a user successfully authenticates via the graphical password, he or she is allowed to connect to the device through this system. However, the proposed modified implementation must be tested to see how effective it can be when used in other operating systems or indifferent job environments.

3.4 Various Types of Graphical Password

Forman, T., & Aviv, A [29] suggested utilizing Double Patterns (DPatts) as an extension of Android patterns. Users access their phones by entering two patterns in series and superimposed. They performed an online survey in which 634 people choose DPatts from three different treatments: power, first pattern blocklist, and absolute, DPatt blocklist. It was discovered

that, when compared to standard Android patterns, DPatts significantly improve Security. After 30 tries, a hypothetical intruder guessing an unknown DPatt based on any training data will only guess 5.3 percent of the DPatts in the training range, opposed to 23.6 percent of Android trends. Just 1.9 percent and 0.9 percent of DPatts in the rst-pattern blocklist and complete DPatt blocklist, respectively, suggest that block listing may be a feasible choice for further enhancing protection.

Moreover, [53] They created an Android program. It includes all of the information about how to use the Multi-level Locking Application. They split the support manual into three parts based on three modules. The expression "multi-level" refers to various levels of protection (types of locks) that can be accessed at the user's discretion. Android is an advanced, adaptable stage that was designed to be incredibly accessible. Android apps use cutting-edge hardware and programming and adjacent and served details, exposed during the process, to convey progression and motivating force to customers. There is also a built-in protection mechanism supported by Android, such as a pin code, a pattern password, an image password, and so on.

Further study in reference [54] created the Vibration-and-Pattern (VAP), a modern graphical authentication system for smartphones and tablets that incorporates vibration-code and pattern-lock techniques to include a safe password mechanism. They designed the device on the Android platform and performed a usability test with 95 people. The outcome suggests that their method is both dependable and convenient to use. They've also included a quick security audit of the device, which shows that it can withstand a variety of different attacks. It was, to their knowledge, it was the first application to incorporate pattern-lock and vibration-code in the graphical password to avoid well-known assaults. Furthermore, [26] demonstrated how users like to use images and emojis in a multimedia password authentication app. In general, mobile devices lack a two-factor authentication (2FA) approach. A preliminary analysis and a consumer study (N=30) were performed to explore usability and protection problems. Both experiments showed a mechanism for using the image dominance effect to improve graphical password memorability.

Another study in reference [27], proposed a multi-element graphical password protection model for mobile devices that is immune to spyware and shoulder surfing assaults. The proposed Coin Passcode platform reduces the complexity of previous graphical password templates, which serve as a quick passcode authentication framework for mobile devices. In comparison to current numerical and alphanumerical passwords, the Coin Passcode model has a strong memorability score, as tests show that humans recall graphics rather than phrases. According to the findings, the Coin Passcode can solve the latest shoulder-surfing and spyware assault vulnerabilities that occur in established smartphone device numerical passcode authentication layers.

On the other hand, in reference [55], they proposed EvoPass, an evolvable graphical password scheme. This type of access control did not asking users to alter their pass photos. Furthermore, EvoPass is resistant to shoulder surfing assaults (type of data theft where cybercriminals steal personal information or confidential information by peering over the target's shoulders). They used two metrics, Information Retention Rate (IRR) or Password Diversity Score (PDS), to generate a difficulty range with good usability and resilience to shoulder-surfing assaults. According to their findings, using edge detection as an image distortion feature in EvoPass increases its resilience to shoulder-surfing attacks instead of other graphical password schemes that do not have the feature. Furthermore, with the aid of IRR and PDS, a shoulder surfing intruder would require more observations of password entry to breach a target account in EvoPass than in any graphical framework with picture distortion. Especially with the time-evolving functionality, EvoPass will attain the same resistance to shoulder-surfing attacks as other graphical systems with fewer decoy images. Also, [23] proposed the "SysPal" method, which mandates the use of a limited number of randomly chosen points when choosing a pattern. Users have the option of using specific mandated points in whatever location they choose. They conducted a large-scale online study with 1,717 participants to assess the protection and usability of three SysPal policies, varying the number of mandatory points required (when choosing a pattern) from one to three. Compared to the current Android regulation, their findings show that the two SysPal rules that include using one and two points will help users choose slightly more stable patterns: 22.58 percent and 23.19 percent fewer patterns were cracked. However,

no statistically meaningful difference in template recall success rate was seen for those two SysPal policies (the percentage of participants who correctly recalled their pattern after 24 hours). Also, [56], they proposed an XML-based schema for representing graphical images. When a user loads a password image with a graphical design, the server processes the pattern and verifies it for validity using stroke duration and drift. Different types of graphic patterns may be created by applying various transformations to a graphic input pattern. These practices' extracted pixel values are saved in an XML pattern database. The server then uses LSB steganography to correct the pattern bits in the input image and returns it to the user as a password image. When a user enters a password image, the password pattern is extracted and mapped to an XML pattern database. The presented paradigm is implemented as both a mobile and desktop application. The approach is more successful than other picture password mappers, according to the comparative efficiency assessment. Since all of the detail from the query password pattern picture is removed, the password mapping accuracy is 100 percent.

4. ASSESSMENTS AND RECOMMENDATIONS

We reviewed all of the studies related to the graphic password and classified them as shown in Fig. 3. These classification for all reviewed papers depends on publication years, authors, used tools/techniques, and results. It is more convenient to use and less likely to be lost than the conventional phone lock scheme.

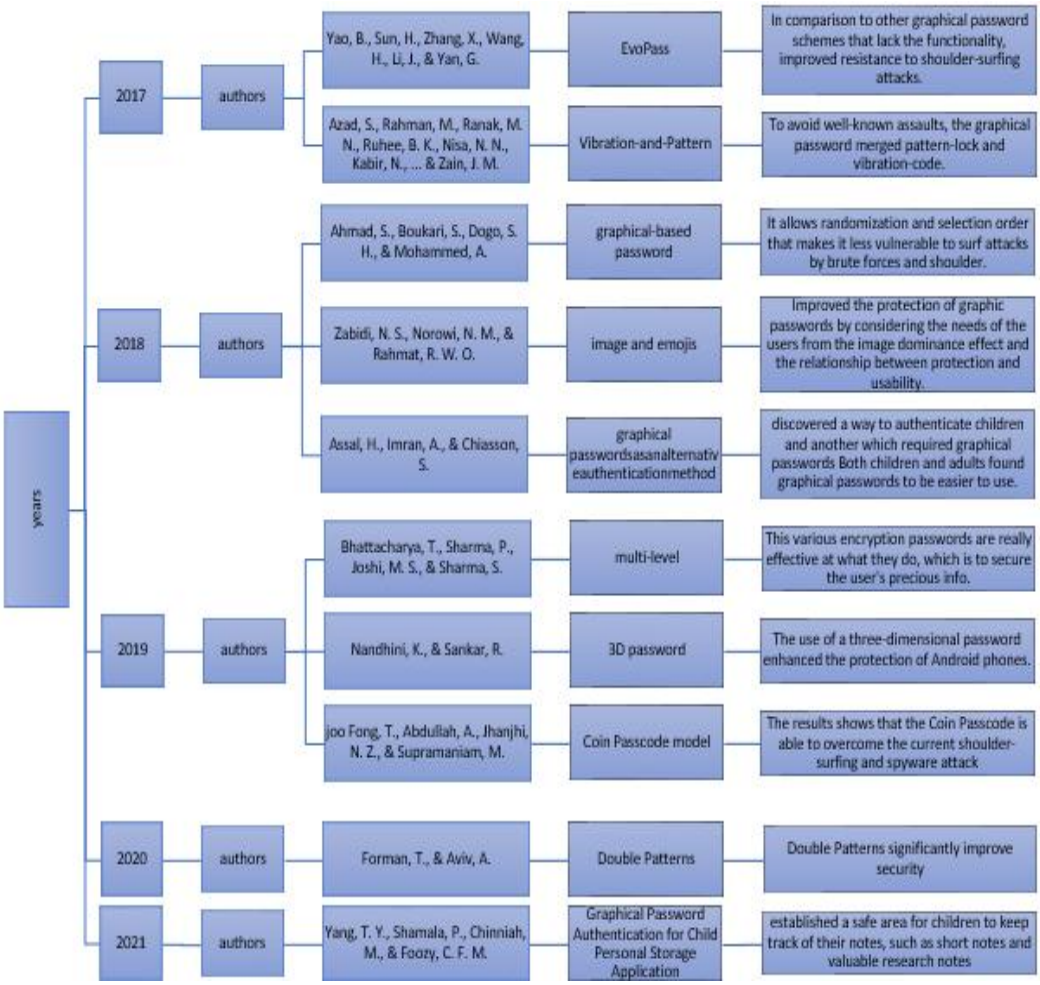

Fig. 3. Classification of reviewed graphic password

It often helps the user to create a pattern password for other applications. However, when not used in a private environment though, graphical passwords are more vulnerable to "shoulder-surfing attacks. The reason for that is that an unauthorized user can discover the password by observing the mobile screen while the user achieves entry. Since it uses icons instead of letters, numbers, or unique characters, attackers will see it. This will depend on the implementation, the types of icons used and how users communicate with them differ. Graphical passwords enable the user to pick images in a specific order or react to images in a specific order

.

5. CONCLUSION

While the graphical password strategy can transform how a typical consumer enters their password and how safe it can be, it is not without shortcomings and drawbacks. One of the drawbacks of using a graphical login scheme is the risk of shoulder surfing. A graphical password may be visually detected without a password field like an alphanumeric password, particularly in public spaces. An intruder can see the password is entered several times. They would quickly break it, which is a severe vulnerability. Another disadvantage to a graphical password scheme is that it is susceptible to guessing. If the user just registered a brief and predictable password, similar to an alphanumeric password, the likelihood of it being guessable will improve.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Kuo C, Romanosky S, Cranor LF. Human selection of mnemonic phrase-based passwords, In Proceedings of the second symposium on Usable privacy and security. 2006;67-78.
2. Michelle SK, Mazurek L. Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur, "Measuring Password Guessability for an Entire University; 2013.
3. RM. a. K. Thompson, Password security: A case history, Communications of the ACM. 1979;22:594-597, 1979.
4. Florian Schaub RD, Michael Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms; 2012.
5. Hassan RJ, Zeebaree SR, Ameen SY, Kak SF, Sadeeq MA, Ageed ZS*, et al.* State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions," Asian Journal of Research in Computer Science. 2021;32-48.
6. Yasin HM, Zeebaree SR, Sadeeq MA, Ameen SY, Ibrahim IM, Zebari RR*, et al.* IoT and ICT based Smart Water Management, Monitoring and Controlling System: A Review, Asian Journal of Research in Computer Science. 2021;42-56.
7. Serge Egelman SJ, Rebecca S. Portnoff, Kerwell Liao,Sunny Consolvo, and David Wagner, "Are you ready to lock?," presented at the Proceedings of the ACM 2014 SIGSAC Conference on Computer and Communications Security; 2014.
8. Marian Harbach ADL, Serge Egelman, "The anatomy of smartphone unlocking: A field study of android lock screens," presented at the Proceedings of the 2016 CHI conference on Human Factors in Computing Systems; 2016.
9. Marian Harbach, Alexander De Luca, Nathan Malkin, Serge Egelman. Keep on Lockin' in the Free World: A Multi-National comparison of smartphone locking. Presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems; 2016.
10. Hamed Z, Ahmed I, Ameen S. Protecting Windows OS Against Local Threats Without Using Antivirus" International Journal of Advanced Science and Technology. 2020;29(12s), SERSC:64-70.
11. Van Bruggen D, Liu S, Kajzer M, Striegel, A Crowell CR. D'Arcy J; 2013.
12. Emanuel von Zezschwitz, Paul Dunphy, Alexander De Luca. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services. August 2013;261–270.
13. Abdullah SMSA, Ameen SYA, Sadeeq MA, Zeebaree S. Multimodal emotion recognition using deep learning, Journal of Applied Science and Technology Trends. 2021;2:52-58.

14. Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, Can Yildiz. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. Presented at the Proceedings of the sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks; April 2013.
15. Adam DB, Aviv J, Ravi Kuber. Is bigger better? Comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock," presented at the Proceedings of the 31st Annual Computer Security Applications Conference; 2015.
16. Susanna Heidt, Adam J. Aviv. Refining graphical password strength meters for android phones. Presented at the In Poster Presented at the Twelfth Symposium on Useable Security and Privacy; 2016.
17. Marte L, Markus D, Lillian R. On user choice for android unlock patterns. Presented at the In European Workshop on Usable Security; 2016, January.
18. Youngbae S, Geumhwan C, Seongyeol O, Hyoungshick K, Jun HH. On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks. Presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems; 2015.
19. Chen Sun, Yang Wang, Jun Zheng. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. Journal of Information Security and Applications. 2014;19:308-320.
20. Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, Thorsten Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. Presented at the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications Security; 2013.
21. Emanuel von Zezschwitz, Malin Eiband, Daniel Buschek, Sascha Oberhuber, Alexander De Luca, Florian Alt, Heinrich Hussmann. On quantifying the effective password space of grid-based unlock gestures. Presented at the Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia; 2016.
22. Zeebaree S, Ameen S, Sadeeq M. Social media networks security threats, risks and recommendation: A case study in the kurdistan region, International Journal of Innovation, Creativity and Change. 2020;13:349-365.
23. Geumhwan Cho, Jun Ho Huh, Junsung Cho, Seongyeol Oh, Youngbae Song, Hyoungshick Kim. Syspal: System-guided pattern locks for android. Presented at the Symposium on Security and Privacy (SP), San Jose, CA, USA; 2017.
24. Harshal Tupsamudre, Vijayanand Banahatti, Sachin Lodha, Ketan Vyas. Pass-o: A proposal to improve the security of pattern unlock scheme. Presented at the roceedings of the 2017 ACM on Asia Conference on Computer and Communications Security; 2017.
25. Aziz ZAA, Ameen SYA. Air pollution monitoring using wireless sensor Networks, Journal of Information Technology and Informatics. 2021;1:20-25.
26. Nur Syabila Zabidi, Noris Mohd Norowi, Rahmita Wirza O. K. Rahmat. A usability evaluation of image and emojis in graphical password. International Journal of Engineering & Technology. 2018;400-407.
27. Teoh joo Fong, Azween Abdullah, Jhanjhi NZ, Mahadevan Supramaniam. The coin passcode: A shoulder-surfing proof graphical password authentication model for mobile devices. International Journal of Advanced Computer Science and Applications (IJACSA). 2019;10.
28. Amanuel SVA, Ameen SYA. Device-To-Device Communication For 5g Security: A Review, Journal of Information Technology and Informatics. 2021;1:26-31.
29. Tim Forman, Adam Aviv. Double patterns: A usable solution to increase the security of android unlock patterns. Presented at the In Annual Computer Security Applications Conference; 2020.
30. Abdullah DM, Ameen SY. Enhanced Mobile Broadband (Embb): A RevieW, Journal of Information Technology and Informatics. 2021;1:13-19.
31. Khalid LF, Ameen SY. Secure Iot Integration in Daily Lives: A Review," Journal of Information Technology and Informatics. 2021;1:6-12.
32. Gregory D. Moody, Mikko Siponen, Seppo Pahnila. Toward a unified model of information security policy compliance. MIS Quarterly; 2018.
33. Chen Wang, Yan Wang, Yingying Chen, Hongbo Liu, Jian Liu. User authentication on mobile devices: Approaches, threats and trends. Computer Networks; 2020.

34. BYOD and Increased Malware. Threats Help Driving Billion Dollar Mobile Security Services Market in; 2013.
35. Al Janaby AO, Al-Omary A, Ameen SY, Al-Rizzo H. Tracking and Controlling High-Speed Vehicles Via CQI in LTE-A Systems," International Journal of Computing and Digital Systems. 2020;9:1109-1119.
36. Hamed ZA, Ahmed IM, Ameen SY. "Protecting Windows OS Against Local Threats Without Using Antivirus," relation. 2020;29:64-70.
37. Jijo BT, Zeebaree SR, Zebari RR, Sadeeq MA, Sallow AB, Mohsin S. et al., "A comprehensive survey of 5G mm-wave technology design challenges," Asian Journal of Research in Computer Science. 2021;1-20.
38. Yahia HS, Zeebaree SR, Sadeeq MA, Salim NO, Kak SF, Adel AZ. et al. "Comprehensive Survey for Cloud Computing Based Nature-Inspired Algorithms Optimization Scheduling," Asian Journal of Research in Computer Science. 2021;1-16.
39. Zhen Yu, Ilesanmi Olade, Hai-Ning Liang, Charles Fleming. Usable authentication mechanisms for mobile devices: An exploration of 3d graphical passwords. The International Conference on Platform Technology and Service Jeju, Korea (South); 2016.
40. Ameen SY, Saud LJ. "Computing Nodes and Links Apperances on Geodsics in Netoworks Topologies Using Graph Theory," presented at presented at ECCCM 2011, January 30 – 31, 2011, University of Technology, Iraq; 2011.
41. a. B. W. Rong Yang. Position-independent multi-model method for mobile user behavior recognition. Information (Switzerland). 2017;7.
42. Alsuhibany SA. "Usability and shoulder surfing vulnerability of pattern passwords on mobile devices using camouflage patterns," Journal of Ambient Intelligence and Humanized Computing. 2020;11: 1645-1655.
43. Salim Istyaq, Khalid Saifullah. A new hybrid graphical user authentication technique based on drag and drop method. International Journal of Innovative Research in Computer and Communication Engineering. 2016;4.
44. Adam J. Aviv, Markus Duermuth. A survey of collection methods and cross-data set comparison of android unlock patterns. arXiv; 2018.
45. Paweł Weichbroth, Łukasz Łysik. Mobile security: Threats and best practices. Mobile Information Systems; 2020.
46. Rutvij H. Jhaveri, Narendra M. Patel, Yubin Zhong, Arun Kumar Sangaiah. Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT. Presented at the Security and Trusted Computing for Industrial Internet of Things; 2018.
47. Bonneau J. The science of guessing: analyzing an anonymized corpus of 70 million passwords," presented at the IEEE Symposium on Security and Privacy, San Francisco, CA, USA; 2012.
48. Hala Assal Al, ChiassonSonia Chiasson, "An exploration of graphical password authentication for children," International Journal of Child-Computer Interaction; 2016.
49. Tay Yi Yang PS. Muruga Chinniah, Cik Feresa Mohd Foozy, "Graphical Password Authentication For Child Personal Storage Application," Journal of Physics: Conference Series. 2020;1739.
50. Nandhini K, Sankar R. 3D password for more secure authentication in android phones. International Journal of Research in Engineering, Science and Management. 2019;2:202-205.
51. Weizhi Meng, Fei Fei, Lijun Jiang, Zhe Liu, Chunhua Su, Jinguang Han. CPMap: Design of click-points map-based graphical password authentication. International Conference on ICT Systems Security and Privacy Protection. 2018;529:18-32.
52. Safiyanu Ahmad, Souley Boukari, Samson Henry Dogo, Aishat Mohammed. An improved map based graphical android authentication system. Science World Journal. 2018;13.
53. Tamajit Bhattacharya PS, Sheetal Joshi, Shilpi Sharma, Authentication Aura to Secure Graphical Password: The Case of Android Unlock Pattern," International Journal of Computer Science and Mobile Computing; 2019.
54. Saiful Azad, Musfiq Rahman, Noman Ranak MSA, Kamal Ruhee BMF, et al. VAP code: A secure graphical password for smart devices. Computers & Electrical Engineering. 2017;59:99-109.
55. Bing Yao, Hui Sun, Xiaohui Zhang, Hongyu Wang, Jingwen Li, Guanghui Yan.

Graph theory towards designing graphical passwords for mobile devices. Presented at the 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China; 2017.

56. KapilJuneja. An XML transformed method to improve effectiveness of graphical password authentication," Journal of King Saud University-Computer and Information Sciences. 2020;32.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/69289