

# Graphical-based password for user authentication in internet of things

Fatimah Saif Alshahrani<sup>1</sup>, Manal Abdulaziz Abdullah<sup>2</sup>

<sup>1</sup>Department of Information Systems, Computer Science Faculty, King Khalid University, Abha, Saudi Arabia

<sup>2</sup>Department of Information System, King Abdulaziz University, Jeddah, Saudi Arabia

---

## Article Info

### Article history:

Received Mar 9, 2022

Revised Jul 24, 2022

Accepted Aug 30, 2022

---

### Keywords:

Alphanumeric-based password

Graphical-based password

Internet of things

Internet of things security

Internet of things user

authentication

---

## ABSTRACT

Internet of things (IoT) has become a significant and evolving technology that cannot be avoidable in most of the sectors. However, the internet of things security became a concern due to the huge amount of the sensitive data that transferring through IoT resources. Secure the users' authentication process of the IoT is the first line of defense to protect the users' data from violation. Typically, the alphanumeric-based password is the popular method to authenticate the users of the IoT. But it is a vulnerable mechanism that can be violated easily. For that, this research aims to develop a graphical-based password scheme to support the traditional text password in the IoT technology. The proposed scheme is a hybrid (Two-factor) approach, based on two types of Knowledge-based Authentication method (alphanumeric-based password and graphical-based password) naming as IoT-GP. IoT-GP aims to improve the users' authentication security considering the usability enhancement. The results obtain from the conducted field study indicated that IoT-GP significantly improved the security and the usability. The results of the password entropy and password space indicated that IoT-GP obtained a high rate comparing to another schemes, which reflected on the IoT-GP ability to resist the guessing and brute force attacks.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

## Corresponding Author:

Fatimah Saif Alshahrani

Department of Information Systems, Computer Science Faculty, King Khalid University

Abha, Saudi Arabia

Email: falshahrani@kku.edu.sa

---

## 1. INTRODUCTION

Internet of things (IoT) is an arising technology which has a big role in simplifying the people life and facilitate users' work [1]-[3]. It's expected to be included into all aspects of humans lives for more comfort and an easy lifestyle [3], [4]. IoT is considered as a growing technology and as more of IoT resources increasing over the time, the number of users' sensitive data also increasing associated with it [5]. IoT technology facing many authentication security challenges due to its complicated environment [6], [7]. It contains a massive number of connected devices, different layers, big data, cloud computing, fog computing, and the open channels [7]. So, breaking one device will break the others which leads to a huge damage of the users' data [8]. The truly important challenge of the user authentication process for IoT resources is how to do it more securely and easily utilize for the different IoT users [8]-[10]. In general, the password is the first defense line of user authenticity, but the use of alphanumeric-based passwords is still widely used, even with the existence of alternatives designed to overcome its issues and weakness [11]-[14]. Graphical-based Password is one of the practical solutions developed to improve the security of the user authentication process in the IoT resources [14]-[16]. Graphical-based password using images as a password instead of the

text depending on the reality that people can easily remember images more than text [17]-[19]. Also, it can enhance the security to resist many alphanumeric-based password attacks like the brute force and guessing attacks [20]. This paper discusses a novel internet of things graphical-based password (IoT-GP) scheme. IoT-GP is based on two types of knowledge-based authentication methods (KBA). It is a hybrid of an alphanumeric-based password (username and password) and a graphical-based password (images). The combination of the two mechanism aims to support each other to improve the security of the users' authentication by using a usable authentication procedure [21]. This mixture of the alphanumeric-based password and graphical-based password aims to protect against three main attacks. Those attacks are the shoulder-surfing, guessing, and brute force attacks. The guessing and brute force attacks are threatening the traditional alphanumeric-based passwords, while shoulder-surfing attack is considered the main weakness point for the graphical-based password approach in general [22]. For that, IoT-GP combines the two mechanisms to overcome the weakness in each. The paper presents the IoT-GP model, in general the concept of model refers to the virtual representation of a real system to understand the purpose of the system [23]. It helps the developers to test the system, improve its quality, and support the development of the system activities and processes [24]. The paper also discusses the followed methodology and the obtained results.

The remainder of this paper is organized as follows: Section 2 presents the proposed IoT-GP general model, and the registration and Login interfaces. Section 3 provided the research method. Section 4 presents the obtained results and discussion. Lastly section 5 presents the conclusion and the future work.

## 2. IOT-GP METHODOLOGY AND PROPOSED SCHEME

Internet of things graphical-based password IoT-GP model consists of three phases as shown in Figure 1. The first phase is the initialization phase where the user has to register as a new user or login if already has account. The second phase is the image pre-processing phase where the selected password image has to going through some processes before stored in the database. In both registration and login procedures this phase required the user to call the images based on the selected images' file, taking into consideration the image will be shuffled every time the user call the images from the images' file. As shown in Figure 2 there are three files each contains nine images the first file named as "Flower" includes nine different images of flowers, the second named as "Tree" includes nine different images of trees, the third named as "Sea" includes nine different images of seas Figure 2(a) and Figure 2(b). Additionally, in this phase the selected password image is passing through some other processes like segmentation, blurring/deblurring, hashing processes.

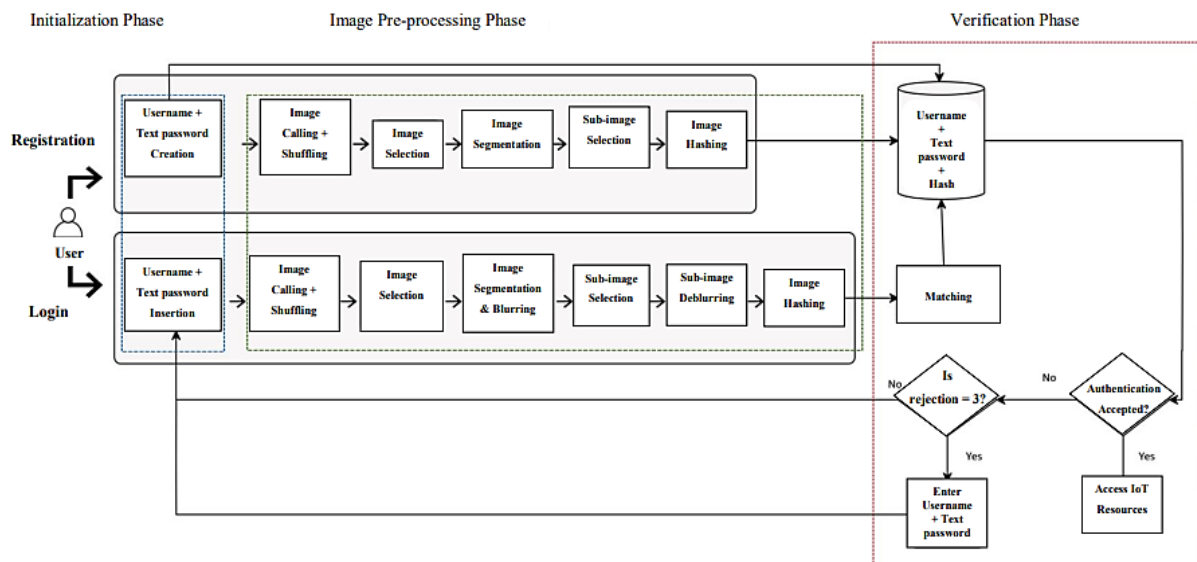


Figure 1. IoT-GP general model

In the IoT-GP, the username and the alphanumeric-based password can be created without any composition requirements. That means the user can use any of the American Standard Code for Information Interchange (ASCII) printable characters (e.g., uppercase, lowercase, numbers, or special character) to

generate the username and the text password. The graphical-based password relies on two level of “Grid Selection Approach”. In the first level, one image out of three groups of 3X3 image grid should be selected (i.e., total 27 image, 9 images for each group). Then one sub-image out of 3X3 sub-image grid should be selected in the second level.

The third phase in IoT-GP is the verification phase. After registration, user’s username and password are stored in database where the data entered by the user is checked to be matched with data already stored in the database when user login. The database also includes the hash chain of the sub-image selected by the user. The verification phase also check the allowed three trials of the user to login. After three rejected trials the user has to re-enter the username and the text password that were established at signup procedure. However, Figure 2 shows the registration and login screens of IoT-GP. Figures 3 and 4 in the appendix shows the detailed models of the registration and login procedures of the IoT-GP.

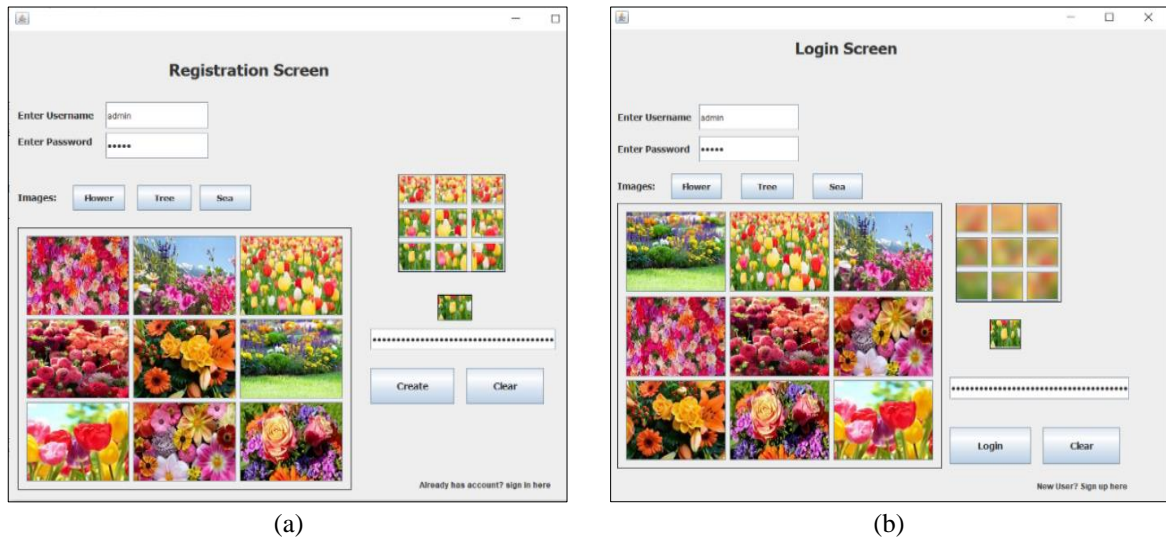


Figure 2. IoT-GP layout screens (a) shows the registration screen and (b) shows the login screen

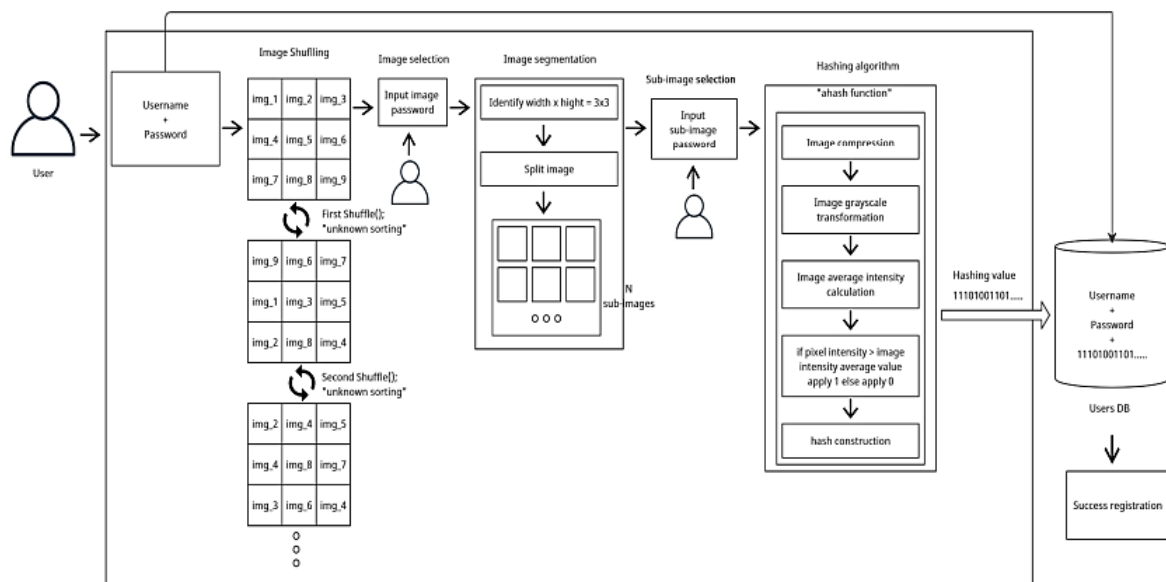


Figure 3. Detailed model of the registration procedure

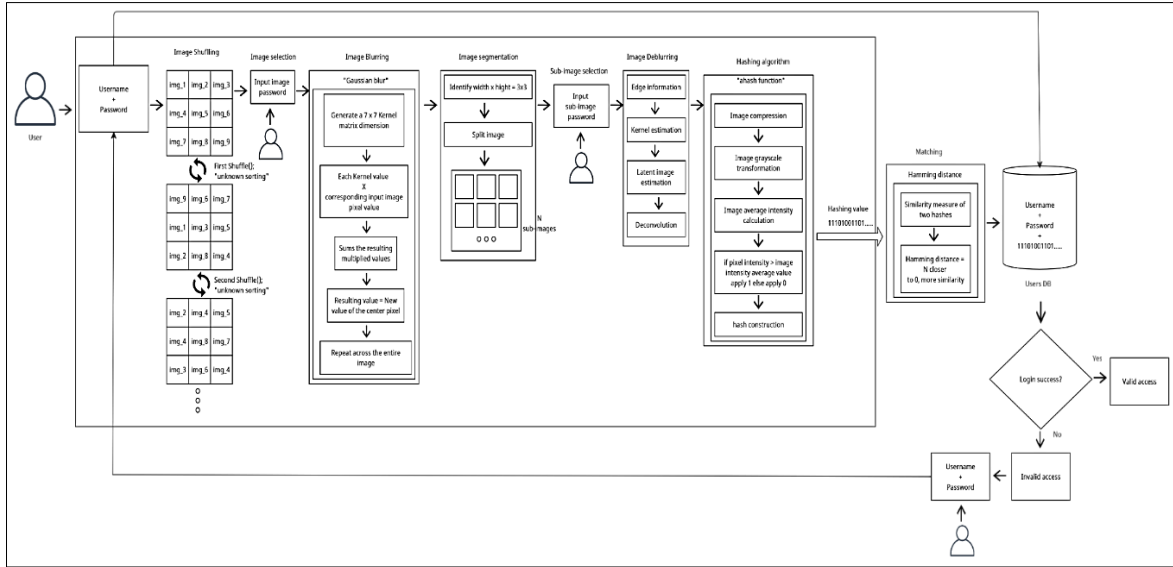


Figure 4. Detailed model of the login procedure

### 3. RESEARCH METHOD

This section discusses the methodology that is followed to evaluate the IoT-GP. A mixed of two methods are used to evaluate the system: a) the qualitative method and b) the quantitative method. For that, five evaluation mechanisms are used to evaluate the IoT-GP scheme the interview, questionnaire, shoulder-surfing attack experiment for the participants, password entropy to measure the strength of the IoT-GP, and the password space to calculate the password options availability.

## 4. RESULT AND DISCUSSION

### 4.1. Interview

The interview was a semi-structured interview including a close-ended (Yes, No questions), and open-ended question (Comments). The interview conducted with seven expert and Ph.D. holders' participants from Information System and Computer Science Departments of King Abdulaziz University. The responses of the question are shown in Figure 5 and Table 1.

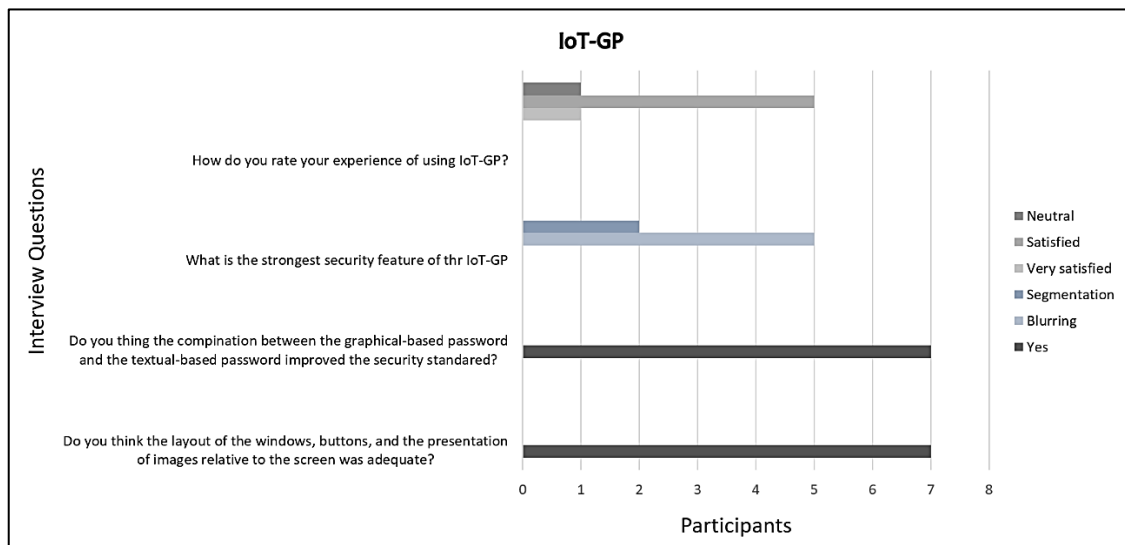


Figure 5. Interview questions and interviewee answers

Table 1. The open-ended interview question and some of the interviewee answers

Question	Answer
Do you have any comments/ advices?	- "I recommend providing instructions to enhance the usability and clarify the procedures". - "I found IoT-GP more secure and usable than the many other approaches like the Captcha technique". - "I suppose this hybrid scheme can reduce the time taken at authentication".

**4.2. Questionnaire**

The questionnaire included closed questions, scaled from strongly agree to strongly disagree according to the five-point Likert scale. 42 participants were participating in the study questionnaire. The demographic data of the study sample came as shown in Table 2.

Table 2. The demographic data of the study sample

Items	Frequency	Percent	
Age	20 to 30 years old	15	35.7%
	31 to 40 years old	14	33.3%
	41 to 50 years old	9	21.4%
	Over 50 years	4	9.5%
Education level	Diploma/Bachelor	13	31.0%
	Masters/PhD	17	40.5%
	Undefined	12	28.6%
Computer experience	Beginner	12	28.6%
	Middle	15	35.7%
	Expert	15	35.7%
Total	42	100%	

**4.2.1. Security criteria**

According to Table 3, there is a high degree of agreement about the security standards of the IoT-GP scheme from the participants' point of view, with an arithmetic mean of (4.30 ± 0.07). It is an arithmetic mean that strongly indicates the degree of approval. This axis was addressed through three statements all came with an arithmetic mean indicates a degree of strong agreement. The arithmetic averages ranged between (4.21 to 4.38 out of 5) according to the five-point Likert scale.

Table 3. The mean, SD, and percentages for participants' opinion on measures the security criteria

Items	Strongly agree	agree	Not Sure	disagree	Strongly disagree	Mean	SD	Degree
1. It is difficult to for the attacker to guess the user's password when using Graphical-based Password.	N 13 % 31.0%	26 61.9%	2 4.8%	1 2.4%	0 0.0%	4.21	0.64	strongly agree
2. It is difficult for an observer to understand what a user selects as his password during an authentication round when he/she uses the Graphical-based password.	N 15 % 35.7%	25 59.5%	2 4.8%	0 0.0%	0 0.0%	4.31	0.56	strongly agree
3. The Graphical-based Password scheme is reliable and secure enough.	N 18 % 42.9%	22 52.4%	2 4.8%	0 0.0%	0 0.0%	4.38	0.58	strongly agree
Mean						4.30	0.07	strongly agree

**4.2.2. Usability criteria**

According to Table 4, there is a high degree of agreement about the usability criteria of the IoT-GP from the participants' point of view with a mean of (4.21 ± 0.11). Which is an arithmetic mean that indicates the strong degree of approval. This axis came through eight statements. The averages of three statements indicate a strong degree of agreement, while five statements indicate a degree of agreement only. Where the arithmetic averages ranged between (4.11 to 4.43 out of 5) according to the five-point Likert scale.

**4.3. Shoulder-surfing attack experiment (Scenario)**

This experiment was conducted specially to test the effect of the IoT-GP graphical-based password scheme on the shoulder-surfing attack. However, 16 participants were invited to test the IoT-GP scheme.

They were assigned in two different groups, the 'Users group' contains 8 participants, and the 'Attacker group' contains the other 8 participants. The scenario of the experiment was as:

- a) Separately, half of the participants (Users group) were performing the authentication process.
- b) Separately, the other half of the participants (Attacker group) had to standing in behind and tries to be catching the entered password.
- c) On the same way the experiment was repeated once again to validate the trial of the attack.
- d) The obtained result from the shoulder-surfing experiment clarifies that none of the 'Attack group' participants' were able to detect the users' authentication information in both rounds due to the following reasons.
  - The combination of the alphanumeric-based password & the graphical-based password.
  - The three security features (image shuffling, image blurring, and image segmentation).
  - The color of the pass-images.
  - The two-levels of images selection.
  - Tiny size of the sub-images after segmentation.

Table 4. The mean, SD, and percentages for participants' opinion on measures the usability criteria

Items		Strongly agree	agree	Not Sure	disagree	Strongly disagree	Mean	SD	Degree
1. I think that I would like to use this system frequently.	N	12	26	3	1	0	4.17	0.65	agree
	%	28.6%	61.9%	7.1%	2.4%	0.0%			
2. I found the system easy and without any inconsistency.	N	13	25	2	0	2	4.12	0.88	agree
	%	31.0%	59.5%	4.8%	0.0%	4.8%			
3. I thought the system was easy to use and well-integrated.	N	12	24	5	1	0	4.12	0.70	agree
	%	28.6%	57.1%	11.9%	2.4%	0.0%			
4. I would imagine that most people would learn to use this system very quickly.	N	11	26	3	2	0	4.11	0.72	agree
	%	26.2%	61.9%	7.1%	4.8%	0.0%			
5. I felt very confident using the system.	N	15	25	2	0	0	4.31	0.56	strongly agree
	%	35.7%	59.5%	4.8%	0.0%	0.0%			
6. I didn't need to learn a lot of things before I could get going with this system and I would not need the support of a technical person.	N	13	25	3	1	0	4.19	0.66	agree
	%	31.0%	59.5%	7.1%	2.4%	0.0%			
7. I found the Graphical-based Password was easy to remember.	N	14	25	2	1	0	4.24	0.65	strongly agree
	%	33.3%	59.5%	4.8%	2.4%	0.0%			
8. The time taken for a user to finish the registration/authentication procedure is adequate.	N	19	22	1	0	0	4.43	0.54	strongly agree
	%	45.2%	52.4%	2.4%	0.0%	0.0%			
Mean							4.21	0.11	strongly agree

#### 4.4. Password entropy

Typically, password entropy does not measure the generated password security. But it's conceptually related to the difficulty of the password random guessing [16], [25]. And it's usually calculated as:

$$Entropy = N \log_2 L \quad (1)$$

where  $N$  represents the number of the digits in the password,  $L$  represents the number of possible digits that can be used to create the password [16], [25].

In our case, the above formula is a logarithm formula used to calculate the text password entropy with the base 2, all ASCII printable characters except space (whitespace) can be used to initiate the text password, which means  $L = 94$  based on the ASCII, also the symbol  $N = 12$  represent the number of the digits in the IoT-GP text password.

$$Entropy = N \log_2 (|L||O||C|) \quad (2)$$

where  $N$  represents the number of images selected,  $L$  represents the images' locations that can be clicked,  $O$  represents the whole number of objects (images) that can be selected, and  $C$  represents the colors.

In case of IoT-GP, the above formula is an logarithm formula used to calculate the graphical-based password entropy with the base 2,  $N = 2$  which are the user's selected images (i.e., the main image at the 1selection level and the sub-image at the 2selection level),  $L = 18$  which are the whole possible images' locations that can be clicked, in the IoT-GP there are two level of 3x3 images grid (i.e., 9 images' locations in

each grid),  $O = 36$  which are the total images that can be used in the IoT-GP (i.e., 27 main images at the 1 level and 9 sub-image at the 2level), and  $C = 3$  which are the colors of the images (i.e., the main images are classified into three files based on the type and the color of the image; *Red*=Flower images, *Green*=Tree image, and *Blue*=Sea images). Summary of the above results shown in Table 5.

Table 5. IoT-GP alphanumeric-based password and graphical-based password entropy results

Password type	Result
Alphanumeric-based password	Entropy = $12 * \log_2(94) = 12 * 6.554 = 78.65$
Graphical-based password	Entropy = $2 * \log_2(3*36*18) = 2 * \log_2(1944) = 2 * 10.924 = 21.85 \approx 22$ = 100.65

#### 4.5. Password space

Password space term refers to the available options in the scheme that allow the users' to choosing their own password. In general, there is no possibility to determine a one specific formula to obtain the password space, but there is an ability to calculate the password space for each scheme based on the generated algorithm [16], [25]. However, the IoT-GP password space discussed in Table 6.

Table 6. IoT-GP alphanumeric-based password and graphical-based password space results

Password type	Result
Alphanumeric-based password (with 12 characters length contains capital alphabets, small alphabets, numbers, and special characters)	Password space = $94^{12}$
Graphical-based password (with 3 files, 36 images, 2 selected images, and 18 locations to be clicked)	Password space = $(3*36*18)^2 = (94)^{12} + (1944)^2$

According to the previous results IoT-GP achieved a significant positive impact through improving the users' authentication security of the IoT technology. The interview results indicated to the effect of the hybrid mechanism to increase the security of the authentication process. Furthermore, the questionnaire results show a significant satisfaction of the participants about the IoT-GP security and usability factors. The obtained results from the password entropy and password space prove the ability of the IoT-GP to resist the guessing and brute force attack.

### 5. CONCLUSION

This research presented a new graphical-based password scheme designed to be appropriate for the IoT users' authentication. IoT-GP is the internet of things graphical-based password scheme designed to improve the IoT users' authentication security taking into consideration simplify the authentication process to enhance the usability of the novel scheme to considerate the IoT users' skill-ability differences. The IoT-GP promising success to prevent against shoulder-surfing, guessing, and brute force attacks threatening. In the future researchers will continue working on the IoT-GP by conducting an extra security and usability features. Such as, adding extra security factor to upgrade the IoT-GP from two-factor authentication to three-factor authentication to increase the security criteria but considering the usability criteria. Also, increasing the number of the pass-images that the user can choose. Also, providing the ability to change the alphanumeric-based password, or the graphical-based password, or even both based on user's needs.

### REFERENCES




- [1] R. Jeyaraj and A. Paul, "Internet of things: A primer," *Human Behavior and Emerging Technologies*. Wiley Online Library, vol. 1, no. 1, p. 37-47, 2019, doi: 10.1002/hbe2.133.
- [2] M. Q. Brij and B.Gupta, "An overview of internet of things (IoT): Architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience*. Wiley Online Library, vol. 32, no. 21, p. e4946, 2020. doi: 10.1002/cpe.4946.
- [3] S. Kalra and G. Sharma, "Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications," *J Ambient Intell Human Comput*. Springer, Cham, vol. 11, no. 4, p. 1771-1794, 2019, doi: 10.1007/s12652-019-01225-1.
- [4] A. Dehghantanha, H. HaddadPajouh, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions, internet of things," *Internet of Things*. Elsevier B.V, vol. 14, no. 2542-6605, p. 100129, 2019, doi: 10.1016/j.iot.2019.100129.
- [5] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Security and Communication Networks*. vol. 2019, p. 20, 2019, doi: 10.1155/2019/5452870.
- [6] F. Stajano and M. Lomas, " User authentication for the internet of things," *Cambridge International Workshop on Security Protocols*. Springer, Cham, vol. 11286, no. 978-3-030-03251-7, p. 209-213, 2018. doi: 10.1007/978-3-030-03251-7-25.
- [7] M. Nikravan and A. Reza, "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the internet of things," *Wireless Pers Commun*. Springer, Cham, vol. 111, no. 1, p. 463-494, 2020, doi: 10.1007/s11277-019-06869-y.
- [8] B. Pant and P. Matta, "TCpC: a graphical password scheme ensuring authentication for IoT resources," *International Journal of Information Technology*. Springer, Cham, vol. 12, no. 3, p. 699-709, 2020, doi: 10.1007/s41870-018-0142-z.






- [9] A. Roy, D. Dasgupta and A. Nag, "Authentication basics," *Advances in User Authentication. Infosys Science Foundation Series. Springer, Cham*, no. 978-3-319-58808-7, p. 1-36, 2017, doi: 10.1007/978-3-319-58808-71.
- [10] Y. Li, Y. Tian, B. Sengupta, N. Li, and C. Su, "Leakage-resilient biometric-based remote user authentication with fuzzy extractors," *Theoretical Computer Science. Elsevier B.V.*, vol. 814, no. 2020, p. 223-233, 2020, doi: 10.1016/j.tcs.2020.02.
- [11] V. Zimmermann and N. Gerber, "The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes," *International Journal of Human-Computer Studies. Elsevier B.V.*, vol. 133, no. 2020, p. 26-44, 2020, doi: 10.1016/j.ijhcs.2019.08.006.
- [12] J. Song, D. Wang, Z. Yun, and X. Han, "Alphapwd: a password generation strategy based on mnemonic shape," *IEEE Access*, vol. 7, p. 119052-119059, 2019, doi: 10.1109/ACCESS.2019.2937030.
- [13] S. Z. Nizamani, S. R. Hassan, and R. A. Shaikh, "TQ-Model: a new evaluation model for knowledge-based authentication schemes," *Arabian Journal for Science and Engineering. Springer, cham*, vol. 45, no. 4, p. 2763-2778, 2019, doi: 10.1007/s13369-019-04137-6.
- [14] C. Ntantogian, S. Malliaros, and C. Xenakis, "Evaluation of password hashing schemes in open source web platforms," *Computers & Security. Elsevier Ltd*, vol. 84, no. 2019, p. 206-224, 2019, doi: 10.1016/j.cose.2019.03.011.
- [15] G.-C. Yang, "Development status and prospects of graphical password authentication system in Korea," *KSII Transactions on Internet and Information Systems (TIIIS). koreascience.or.kr*, vol. 13, no. 11, p. 5755-5772, 2019, doi: 10.3837/tiis.2019.11.026.
- [16] O. Osunade, I. A. Oloyede, and T. O. Azeez, "Graphical user authentication system resistant to shoulder surfing attack," *Adv. Res.*, vol. 19, no. 4, p. 1-8, 2019, doi: 10.9734/air/2019/v19i430126.
- [17] M. A. Khan, I. U. Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "G-RAT| a novel graphical randomized authentication technique for consumer smart devices," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 2, p. 215-223, 2019, doi: 10.1109/TCE.2019.2895715.
- [18] M. Versaci and F. C. Morabito, "Image edge detection: A new approach based on fuzzy entropy and fuzzy divergence," *International Journal of Fuzzy Systems. Springer, cham*, vol. 23, no. 918-936, p. 1-19, 2021, doi: 10.1007/s40815-020-01030-5.
- [19] N. Woods and M. Siponen, "Improving password memorability, while not inconveniencing the user," *International Journal of Human-Computer Studies. Elsevier Ltd*, vol. 128, p. 61-71, 2019, doi: 10.1016/j.ijhcs.2019.02.003.
- [20] G. K. Sadasivam, C. Hota, and B. Anand, "HoneyNet data analysis and distributed SSH brute-force attacks," *Towards Extensible and Adaptable Methods in Computing. Springer*, no. 978-981-13-2348-5, p. 107-118, 2018, doi: 10.1007/978-981-13-2348-5-9.
- [21] M. Belk, C. Fidas, and A. Pitsillides, "Flexpass: symbiosis of seamless user authentication schemes in IoT," *In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. dl.acm.org*, Paper No.: LBW2318, p. 1-6, 2019, doi: 10.1145/3290607.3312951.
- [22] M. A. Hossain, P. Khan, C. C. Lu, and R. J. Clements, "IET Institution of Engineering and Technology 2020", vol. 14, no. 12, pp. 2937-2947, 2020, doi: 10.1049/iet-ipt.2019.0150.
- [23] T. J. Fong, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "The coin passcode: a shoulder-surfing proof graphical password authentication model for mobile devices," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 1, p. 302-308, 2019, doi: 10.14569/IJACSA.2019.0100140.
- [24] F. M. Alfarid, A. A. Keshlaf, and O. M. Bouzid, "IoT GazePass: A new password scheme for IoT applications," *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, p. 299-304, 2021, doi: 10.1109/MI-STA52233.2021.9464390.
- [25] F. Ghiyampour, "Secure graphical password based on cued click points using fuzzy logic," *Security and Privacy. Wiley Online Library*, vol. 4, no. 2, p. e140, 2021, doi: 10.1002/spy2.140.

## BIOGRAPHIES OF AUTHORS



**Fatimah Saif Alshahrani**    received her bachelor's degree (B.Sc.) in 2015 in Information System from King Khalid University KKU, Saudi Arabia. She received the master's degree (M.Sc.) in 2022 in Information System from King Abdulaziz University KAU, Saudi Arabia, she is a lecturer in faculty of computer science King Khalid University KKU, Saudi Arabia SA. She can be contacted at email: falshahrani@kku.edu.sa.



**Prof. Manal Abdulaziz Abdullah**    received her PhD in computers and systems engineering, Faculty of Engineering, Ain-shams University, Egypt, 2002. She has experienced in industrial computer networks and embedded systems. Her research interests include Artificial Intelligence, performance evaluation, WSN, IoT, network management, Big Data analysis, and streaming data analysis. Dr. Abdullah published more than 200 research papers in various international journals and conferences. Currently she is a professor in faculty of Computing and Information Technology FCIT, King Abdulaziz University KAU, Saudi Arabia SA. She can be contacted at email: maaabdullah@kau.edu.sa.