ISSN 2278-3091
Volume 11, No.4, July – August 2022
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse071142022.pdf
https://doi.org/10.30534/ijatcse/2022/071142022

User Authentication Techniques of the Internet of Things

Fatimah Saif Alshahrani[1], Manal Abdullah[2]
[1]Department of Information System, King Khalid University, Saudi Arabia, falshahranii@kku.edu.sa
[2]Department of Information System, King Abdulaziz University, Saudi Arabia, maaabdullah@kau.edu.sa

Received Date : June 16, 2022 Accepted Date : July 22, 2022 Published Date : August 06, 2022

ABSTRACT

Internet of Things (IoT) is a growing technology that has got the attention of researchers from different fields. As more of IoT resources increasing, the number of users' sensitive data also increasing. Authentication process is one of the security factors which used to protect the users' sensitive data and identify whether the user is legitimate or not. IoT facing many authentication challenges due to its complicated environment it contains a massive number of connected devices, different layers, big data, cloud computing, and the open channels. The truly important challenge of the user authentication process for IoT resources is how to do it more securely and easily utilize for computer-illiterate users. In general, the password is the first defense line of user confidentiality, but the use of alphanumeric-based passwords is still widely, even with the existence of alternatives designed to overcome its weakness. Graphical-based Password is one of the practical alternatives which is developed to improve the security of the user authentication. This paper aims to explore the various authentication aspects that can be used in the IoT technology. Also, an overview of the graphical passwords which can be used as an alternative of the weak alphanumeric-based passwords in IoT technology.

Key words: Internet of Things, IoT security, IoT User Authentication, Passwords, Graphical-based Passwords.

1. INTRODUCTION

Internet of Things is an arising technology which has a big role in simplifying the people life and facilitate users' work, it's expected to be included into all aspects of humans lives for more comfort and an easy lifestyle [32]. IoT technology provides the ability to share data and information and respond to physical world actions by creating processes and making services, with or without human involvement [11, 13]. By 2023, the universal market of the IoT technology expected to reach $318bn [27]. IoT concept was born by Kevin Ashton, in the United States. IoT can be defined as “the resources that can be communicated to each other or to human with or without human intervention at any time and in any place using open channels (i.e., internet) and internet protocols”. There are different kinds of IoT applications, devices, and services, and here the user security issues is should be taking into consideration [13, 27].

The term security is related to "being free from threats and attacks", it was an unexpansive, simple, an easy task, and that was before the born of open channels (e.g., Internet), the idea of data traveling and sharing over open channels leads to the massive fear of the security attacks [32]. Security form an essential domain to be considered, resolves and fixed, these security fears form an exciting domain for research [12, 7]. However, the topic of security in IoT resources is very wide, it has to cover many security aspects [15, 34]. IoT technology facing a big number of security challenges due to the differences in functions of the devices and the resources in IoT technology, the differences in communication protocols in IoT and also the commercial aspect in most applications. The existing security techniques and strategies are not sufficient to ensure the basic security standards in the IoT resources due to the resources' nature (i.e., many things connected) of IoT technology [7, 23]. The number of IoT resources is expected to grow and that will be led to produce large amounts of sensitive data, so the security of this technology is a major important issue that must be fixed and resolve [32, 7]. The data and information confidentiality are the protection from disclosure by unauthorized users. Many techniques are built and designed to guarantee the confidentiality of data and information. These techniques are known as authentication techniques which is one of the basic techniques for secure users' data and information [35]. Authentication techniques can be defined as “the process of verifying the user identity to provide confidentiality to the users and their data/information from discovered by outside parties” [8]. However, IoT resources facing authentication security challenges because many users using the alphanumeric-based passwords where many of them are simple, easy, weak, and can be guessed [5]. Alphanumeric-based passwords authentication is still ubiquitous, even with the alternatives that have been developed to overcome its weakness. A graphical password is one of these alternatives, born to overcome the weaknesses of alphanumeric-based passwords [17, 22].

In graphical passwords the users utilize the pictures to creating their own passwords instead of the alphanumeric-based password depending on the reality that the users can easily remember the images more than the text. It has the ability to resist many alphanumeric passwords attacks like the spyware,

guessing, and brute force attacks, etc. [32]. In 1996, Blonder proposed the first scheme of graphical passwords [3]. This scheme using the pictures or patterns, that are easy to remember more than alphanumeric-based passwords. The graphical-based passwords authentication technique is one of the important techniques that can replace the alphanumeric-based passwords authentication technique [31]. This type of passwords is much more suitable for many IoT applications like the smart home/office, smart wearable device, smart city, smart healthcare, etc. [1].

Motivation

Internet of Things is a growing technology and as more of IoT resources increasing over the time, the number of users' sensitive data also increasing associated with it. IoT technology facing many authentication securities challenges due to its complicated environment it contains a massive number of connected devices, different layers, big data, cloud computing, fog computing, and the open channels, so breaking one device will break the others which leads to a huge damage of the users' data. The truly important challenge of the user authentication process for IoT resources is how to do it more securely and easily utilize for computer-illiterate users (ordinary users) which are represented the majority of the IoT users. In general, the password is the first defense line of user confidentiality, but the use of alphanumeric-based passwords is still widely, even with the existence of alternatives designed to overcome its issues and weakness. Graphical-based Password is one of the practical alternatives which is developed to improve the security of the user authentication process in the IoT resources. 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. Also, it can resist many alphanumeric-based password attacks like the brute force, guessing, and spyware attacks, etc. This paper aims to explore the graphical-based passwords as a solution that can be used as an alternative of the alphanumeric-based passwords to overcome of its weakness and its related problems, and how can exploit this solution to improve the user authentication process in the IoT resources. Moreover, the paper aims to find out what have been done in this security domain and can be done to improve this field, especially to enhance the IoT security. Further, what are the factors that should be taking in consideration when developing a graphical-based password scheme for the IoT technology.

The remainder of the paper is organized as follows: Section 2 introduces a literature review of the Internet of Things technology and its security. Section 3 describes the Internet of Things users' authentication process. Section 4 discuss the graphical-based passwords classifications. Section 5 highlights the graphical-based password pre-proposed schemes. Lastly, section 6 to conclude the paper.

2. INTERNET OF THINGS

IoT is not about a single technique, but it is about control and intelligence also. IoT consists of four major tasks: the sensing process, the telecommunication, the control process, and the actuators. Moreover, IoT has four main elements which are the physical devices, the inter-connectivity, the real-time application, the operating platform. The IoT technology has been built to implement many tasks such as collecting, transferring, exchanging, processing, storing, and executing the data. IoT technology works with the cloud computing environment, it's working to link between the real world and the Internet [1, 13]. So, users can access the application on demand wherever their real location. IoT applications can manage and control our real-world such as the users can remotely manage and control the temperature sensor, turn the AC on or off to change the temperature of the rooms. There are different applications of the IoT technology like smart cities, smart healthcare, etc. [18]. IoT moving toward control all human life aspects not only in the normal daily human life but also in the companies and businesses, factories, and all social aspects [18, 28].

2.1 INTERNET OF THINGS SECURITY

The security in IoT technology is considered as securing the entire environment architecture of IoT from threats. There are some major security requirements should be considered when developing IoT security solutions shown in Figure 1 [25]:

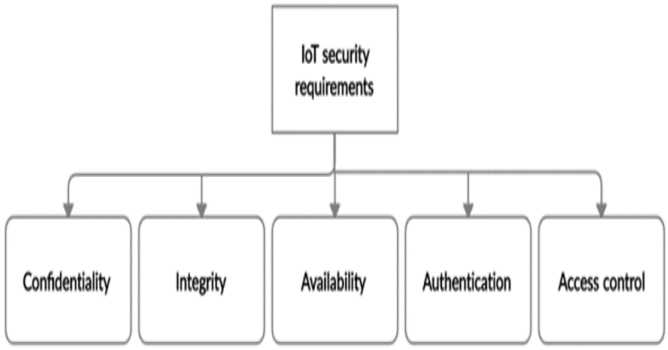

Figure 1: IoT Security Requirements

3. IoT USER AUTHENTICATION PROCESS

When talking about authentication, it means the method used to protecting user's data and information from discovered by an unauthorized party [32]. The authentication process using alphanumeric-based passwords still strongly entrenched and hard to changed or replaced. Although passwords continue to take control of the most user authentication techniques, they would be unsuitable for user authentication to the IoT due to the need for a high level of security mechanism [35].

3.1 User Authentication Aspects on the Internet of Things

The aspects of authentication can be classified into two main aspects single-factor and multi-factor. These factors can be classified as shown in Figure 2 [28, 29]. In the following subsections, we will briefly describe each factor.

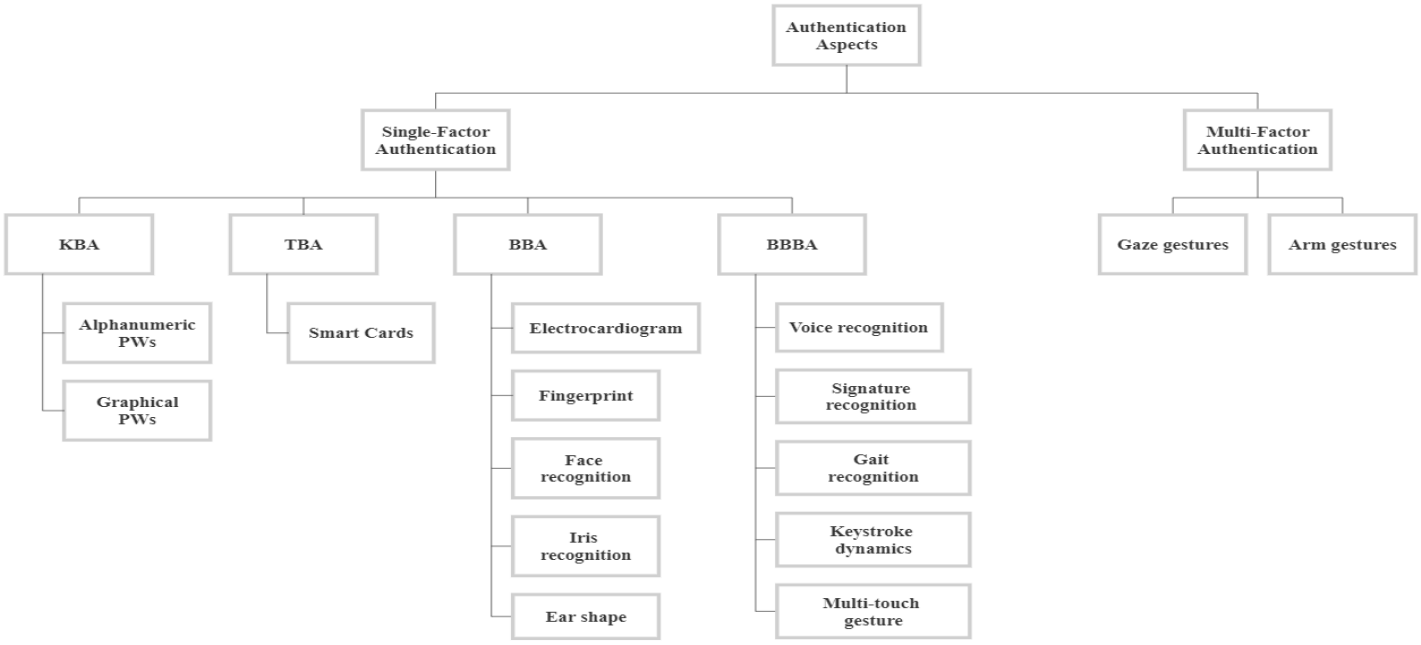

Figure 2: Authentication Aspects

3.1.1 Single-factor Authentication

The single-factor authentication can be classified into four main categories the knowledge-based authentication, the token-based authentication, the biometrics-based authentication, and the behavioral biometrics-based authentication, discussed as follows:

a) Knowledge-based Authentication (KBA)

This factor is related to something that the user knows it, for example the PIN, or username/password, or an answer to a question or any type of needed information [5, 10]. It is the most popular mechanism for user authentication and has gained a big number of users through its very long history. KBA uses the user's information as a mystery key between the users and systems as information related to the identity for authentication. This knowledge may be a text (e.g. alphanumeric-based passwords) or graphics (e.g. click points on images). Even so, the KBA have a challenge with the user's secret knowledge such as, weak, leakage and theft [28, 38, 39]. KBA aspect has different examples such as the Alphanumeric-based passwords and the Graphical-based passwords [36, 26].

b) Token-based Authentication (TBA)

This factor is related to something that the user owns for example, the student ID card, or smart cards or, etc. It is a process to prove the user authentication through providing the needed token [5, 10]. The token can be defined as "a tangible entity include information about the authenticity of the user". TBA is one of the authentication mechanisms where the user authentication is verified by the required token [28, 38, 39]. TBA aspect has different schemes, such as the smart card which is one of the token-based authentication methods. It uses a smart card (e.g., National ID cards, Students ID cards, etc.) to authenticate the user, it is the simplest scheme for IoT technology authentication compared to other authentication schemes [26].

c) Biometrics-based Authentication (BBA)

This factor is related to biological features the user's own; it is a process to prove the user's authentication by using their own unique biological features [5]. The unique biological features of the user that were already recorded in the system are matched with the current login information with the already recorded information to verify the user and allow him to login. BBA depends on human biometrics such as face recognition iris or retina matching to prove user authenticity [10]. On the other hand, to get the human biometric features from users there are some required devices that use different kinds of sensors [28]. For many users, these devices may be expensive because it is only available in sophisticated devices, because of that many users are unwilling to using the BBA mechanism. It is possible to use the ready-made cameras in the devices to get the human biometric features for user authentication, but the accuracy of these kinds of cameras is comparatively less than those using the sensors [38, 39]. BBA aspect has different examples such as Electrocardiogram, Fingerprint, Face recognition, Iris recognition, Ear shape [26].

d) Behavioral Biometrics-based Authentication (BBBA)

This factor is related to the unique human behavioral biometrics' features (e.g. walking or speaking). In these years, BBBA mechanism has taken increased attention, it uses the unique human behavioral biometrics features for user authentication such as the finger motion which shows a unique behavior that can be used for authentication it give a unique pattern that can be used to differentiate between users.

Generally, the BBBA method is more acceptable to users and face less resistance to using it than the BBA method due to the low use of private and sensitive information in BBBA compared to the BBA method. On the other hand, the sensors in the devices (e.g. motion sensors) suffer from less accuracy, and this leads to a rejection from the users due to the unreliability of those sensors [10, 28, 39, 5, 38]. BBBA has different examples like the Voice recognition, Gait recognition, Keystroke dynamics, Signature recognition, Touch dynamics, Multi-touch gesture [26].

3.1.2 Multi-factors Authentication

This factor is related to the combines of two or more authentication methods to improve authentication security such as, using multi biometrics features, or combine the KBA method with the TBA method or with any other method to increase security. For instance, the authentication system may ask for more than one biometrics features (e.g., face ID, fingerprint) to proof the user authentication. In this case, the attacker needs to spend more time and effort to break the different authentication mechanisms. On the other hand, the users have to create more than one authentication method to login and this less suitable than the single authentication method. For example, it will be unpractical to scan the iris ID, then scan the fingerprint and then enter a password all that to proof identity every time to log in. However, the future of user authentication methods is moving towards the multi-factors authentication to improve the security of user authentication process [10, 28, 39, 5, 38]. Authentication process in multi-factor mechanism has different examples such as, the Gaze gestures and Arm gestures [26].

3.2 Passwords-based Authentication

In this era, password mechanisms are the universal used mechanism in knowledge-based authentication. They are the first line of defense of most of the technologies. Password-based authentication security in IoT technology concerns the security of the whole information and data of the user. The problem of the traditional passwords in the IoT environment is the insecurity and the weaknesses to face many attacks. IoT environment is complicated it contains many devices and different layers [17]. The passwords are the most access process method used for user identification used in IoT technology even with the big weakness of using such authentication methods. Using weak passwords and using the same password to secure different accounts, systems, or devices this can destroy the digital life of the user if the password leakages, and this phenomenon is called the "domino effect". It is very clear that the passwords are not going away anytime soon and still dominating the authentication landscape [24]. For this reason, it is necessary to find alternative solutions to reduce the dangers of using weak passwords [30].

3.2.1 Alphanumerical -based Password Authentication

The passwords are the major and the first step that must be taken to reach the confidentiality of user's data and information. Alphanumeric passwords facing different serious problems and attacks such as, the dictionary attacks, the brute force attacks etc. [20]. However, to meet security requirements, the users should assign different passwords to different accounts or systems they use, they should not write down their passwords, and they should not keep the passwords the same for a long time. Now, we can realize the reason that makes the people choosing a short password, to easily remember the password, which makes it very simple for attackers to find it [4, 16, 6, 33, 14].

3.2.2 Graphical-based Passwords Authentication

A graphical-based password is considered a good replacement of the alphanumeric-based password, as images are easy to remember and reuse when needed more than the text, which can be a good alternative to the users to use instead of using the alphanumeric passwords [20]. Also, it has the ability to withstand many alphanumeric-based password attacks such as guessing, brute force and spyware attacks. The first scheme of graphics password was proposed by Blonder [3], in which the users have to click on the predefined positions of a predefined image in with the same sequence [31]. The graphical-based passwords allow the users to reuse their passwords better comparing to recall the alphanumeric-based passwords. Graphical-based passwords can provide more security against Dictionary, Guessing, Spy-Ware, and Brute Force Attacks, but maybe having a less security to Shoulder-Surfing attacks comparing with the alphanumeric-based passwords. But the graphical-based password process is comparatively costly to be implemented and that may reduce the widespread of it [18].

4. THE CLASSIFICATIONS OF THE GRAPHICAL-BASED PASSWORDS TECHNIQUES

Graphical-based password has several techniques that can be used to generate a new scheme of graphical passwords to enhance the user authentication process shown in Table 1 [9, 18, 20, 38].

Table 1: Classifications of the Graphical-based Passwords Techniques.

Technique	Explanation
Recognition Technique	The images are displayed in a list and the user has to select the password from the listed information, then the user has to select the same images that were selected at the signup phase e.g., passface.
Cued Recall Technique	The user has to reuse (recall) the same selected items that he has chosen at the stage of sign up e.g., passpoint.
Pure Recall Technique	the user has to redraw the same item that he has drawn at the phase of sign up. The authentication is handled by comparing between pattern at the login phase with the pattern at the registration phase. e.g. PassShapes.
Hybrid Technique	This technique combines more than one of the previous techniques to provide more security to the users' secret data e.g., uses text passwords and images password.

5. RELATED WORKS OF GRAPHICAL-BASED PASSWORD SCHEMES

Many researches were conducted to improve and evolve the graphical-based password schemes, each of one of these researches has a determined goal to achieve such as, improve the security, or enhance the usability, or withstand a specific attack like, shoulder surfing attack, some of these researches were listed in the Table 2 [2, 19, 32, 31, 37, 9, 21]:

Table 2: Pre-proposed Graphical-based Password Scheme:

Scheme	Advantages	Disadvantages	Summary
Hybrid Images [2]	- More secure against shoulder surfing attack due to unclear images.	- Hard to remember. - Not appropriate for visual weakness people.	This scheme was proposed by Basak et al, here the users have to create a username at the signup phase, then choosing a six black/white pictures, and then they have to create a story (contains at least 80 characters) by thinking about the pictures they selected, to help them to recall the chosen pictures later.
g-RAT [19]	- User friendly, usability.	- Not secure against shoulder surfing attack, because the image is so simple and clear.	This scheme was proposed by Ali Khan et al, it's called gRAT, it uses the draw pattern mechanism and a randomization algorithm to randomize the images at user authentication. The randomized images help against the shoulder-surfing attack.
TCpC [32]	- More secure against shoulder surfing attack, due to its complexity.	- Hard to be understood by computer-illiterate people. - Double effort to login. - Hard to remember.	This scheme was proposed by Matta et al, which is called Two Clicks per Character (TCPC). The idea is the user has to select two characters to create only one character of the password. The user has to work on a row or a column that including the needed character. Then the user has to choose two characters depending on the selected row or column.
SG-PASS [31]	- The user has more flexibility to create his own passwords.	- Hard be to be understood by computer-illiterate people. - Double effort to login. - Hard to remember.	This scheme was proposed by Suryakanta et al, this scheme is a challenging process it uses a big number of icons or images shown in a window on the screen. In this scheme the users have to enter the items by drawing a shape using the keyboard and create a password, this drawn shape will appear on the screen as a user's password.
RouteMap [37]	- Easy to remember.	- Not secure against shoulder surfing attack.	This scheme was proposed by Meng et al, it's called RouteMap which is a graphical password depends on the maps. Here, the user has to create a new path on the map as a password. For example, the user may choose his house as the first point to draw the route, then complete drawing the route and choose the supermarket as the second point and keep moving to the hospital as the last point of the drawn route, etc. The goal of the scheme is to improve the remembering the password.
Coin Passcode [9]	- More secure against shoulder-surfing attack, because of the big set of items contained in the coins.	- Hard to be understood by computer-illiterate. - Hard to remember, due to the big set of factors contained in the coins.	This scheme was proposed by Fong et al, it's called as Coin Passcode it is a hybrid scheme, which uses the concept of multielement it contains a factor of colors, a factor of numbers, and a factor of icons to create unique coin passcodes. There is an entire set of 30 items (icons, numbers, colors) used as the factors to form the coin. The factors in the Coin Password are randomized each time the users attempt to login.
FlexPass [21]	- Flexible, allows choose the authentication way (textual or graphical).	- Not secure against shoulder surfing attack.	This scheme was proposed by Marios et al, here there are two choices for the user by using two types of keys the text or the graphics keys. Entering the textual key has the same rule as the traditional passwords. On another hand, by using a 7x7 grid the user can select the graphical key to log in, image positions are randomly positioned for each login attempt.

6. CONCLUSION

Internet of Things security is one of the arising topics which needs more attention and exploration. At the beginning, the paper mentions a background about the Internet of Things and highlighted the IoT security. A comprehensive study of the user authentication in the IoT was presented. The traditional user authentication process by using the alphanumeric-based passwords is not secured sufficiently to authenticate the users in IoT due to the nature of the IoT environment. IoT has a very complicated environment because it connects different kinds of devices with each other, it is composed of various layers each layer has its own workflow, and it is transporting and analyzing a huge amount of the sensitive data. Graphical-based passwords are one of the alternatives of the alphanumeric-based passwords, which is the most used user authentication mechanism in the IoT. A graphical-based password has the ability to resist various of the alphanumeric-based password attacks. However, after an exhaustive search, developing a hybrid authentication mechanism is a promising technique for more protection against unauthorized access, the challenge here is how to make it simple and secure at the same time. The hybrid alphanumeric-based password and graphical-based password looks more secure and the simplest mechanism, it also more appropriates for the IoT technology and the computer-illiterate (ordinary users) users who are represent the majority users of IoT resources. However, there are four factors should be taking into consideration when developing a graphical-based password suitable for the IoT resources. First factor is the usability, the designed graphical-based password should be simple and easy to used and appropriate for the computer-illiterate users. Second factor is the security, it should be secure enough to protect users' sensitive data in the various IoT resources. Third factor is minimizing the time taking to login, the users should not take a long time to access the needed IoT resources. Last factor is the memorability, it should be uncomplicated in which the users can remember the password easily. However, more studies should be conducted on the graphical-based passwords to enhance the security of the user authentication process in IoT, explore more solutions to beat the weak and dominance of the alphanumeric-based passwords in the user authentication process in IoT, and to improve the graphical-based passwords performance aginst the shoulder-surfing attack.

REFERENCES

1 B.B.Gupta, M. Quamara. (2018). "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols". Concurrency and Computation Practice and Experience.

2 Basak Bilgi, B. Tugrul. (2018). "A Shoulder-Surfing Resistant Graphical Authentication Method". International Conference on Artificial Intelligence and Data Processing (IDAP).

3 Blonder, Greg E. (1996). "Graphical password". In: Google Patents.

4 Chaudhry, J. Farmand, S. Islam, Syed Islam, M. Rafiqul, P. Valli. (2018). "Discovering Trends for the Development of Novel Authentication Applications for Dementia Patients", Cham.

5 Chen Wang, Y. Wang, Y. Chen, H. Liu, J. Liu. (2020). "User Authentication on Mobile Devices: Approaches Threats and Trends". Journal Pre-proof.

6 Christoforos Ntantogian, S. Malliaros, C. Xenakis. (2019). "Evaluation of password hashing schemes in open source web platforms". Computers & Security.

7 J. Cynthia, H. Sultana, M. Saroja, J. Senthil. (2019). "Security Protocols for IoT". In N. Jeyanthi, A. Abraham, H. McHeick (Eds.), Ubiquitous Computing and Computing Security of IoT (pp. 1-28). Cham: Springer International Publishing.

8 D. Dasgupta, A. Roy, A. Nag. (2017). "Authentication Basics". In Advances in User Authentication (pp. 1-36). Cham: Springer International Publishing.

9 T. Fong, A. Abdullah, H. Boveiri. (2019). "A Next Generation Hybrid Scheme Mobile Graphical Authenticator". In M. Elhoseny & A. K. Singh (Eds.), Smart Network Inspired Paradigm and Approaches in IoT Applications (pp. 221-237). Singapore: Springer Singapore.

10 Frank Stajano, M. Lomas. (2018). "User Authentication for the Internet of Things". Springer Nature Switzerland AG.

11 Geeta Sharma, S. Kalra. (2018). "A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services". Iranian Journal of Science and Technology, Transactions of Electrical Engineering.

12 Geeta Sharma, S. Kalra. (2019). "Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications". Journal of Ambient Intelligence and Humanized Computing.

13 Gupta, Aditya. (2019). "Internet of Things: A Primer". In The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things (pp. 1-16). Berkeley, CA: Apress.

14 J. Haber, B. Hibbert. (2018). "Password Hacking". In Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations (pp. 39-48). Berkeley, CA: Apress.

15 Hamed Pajouh, A. Dehghantanha, R. Parizi, M. Aledhari, H. Karimipour. (2019). "A survey on internet of things security: Requirements, challenges, and solutions". Internet of Things.

16 A. Hassan, R. Hijazi. (2017). "Essential Privacy Tips". In Digital Privacy and Security Using Windows: A Practical Guide (pp. 33-102). Berkeley, CA: Apress.

17 J. Song, D. Wang., Z. Yun, X. Han . (2019). "Alphapwd: A Password Generation Strategy Based on Mnemonic Shape". in IEEE Access.

18 K. Mekki, E. Bajic, F. Chaxel, F. Meyer. (2019). "Concept and Hardware Considerations for Product-Service System Achievement in Internet of Things". International Conference on Wireless

Technologies, Embedded and Intelligent Systems (WITS).

19 A. Khan, A. Chefranov. (2018). "A New Secure and Usable Captcha-Based Graphical Password Scheme", Cham.

20 Mackie, M. Yıldırım. (2018). "A Novel Hybrid Password Authentication Scheme Based on Text and Image", Cham.

21 Marios Belk , C. Fidas, A. Pitsillides (2019). "FlexPass: Symbiosis of Seamless User Authentication Schemes in IoT". ASSOC COMPUTING MACHINERY.

22 W. Meng, L. Zhu, W. Li, J. Han, Y. Li. (2019). "Enhancing the security of FinTech applications with map-based graphical password authentication". Future Generation Computer Systems.

23 Mengxia Shuai, N. Yu, H. Wang, L. Xiong. (2019). "Anonymous authentication scheme for smart home environment with provable security". The International Source of Innovation for the Information Security and IT Audit Professional.

24 C. Missaoui, S. Bachouch, I. Abdelkader, S. Trabelsi. (2018). "Who Is Reusing Stolen Passwords? An Empirical Study on Stolen Passwords and Countermeasures", Cham.

25 Mohamed Amanullah, R. Ahamed, F. Nasaruddin, A. Gani, E. Ahmed, A. Nainarf, N. Akim, M. Imran. (2020). "Deep learning and big data technologies for IoT security". The International Journal for the Computer and Telecommunications Industry.

26 Mohamed Ferrag, L. Maglaras, A. Derhab. (2019). "Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends". Security and Communication Networks.

27 Mohamed, K. Salah. (2019). "The Era of Internet of Things: Towards a Smart World". In The Era of Internet of Things: Towards a Smart World (pp. 1-19). Cham: Springer International Publishing.

28 Mohammad Nikravan, A. Reza. (2019). "A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things". Wireless Personal Communications.

29 Mudassar Khan, I. Ud Din, S. Member, S. Jadoon, M. Khan , S. Member, M. Guizani, K. Awan. (2019). "g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices". IEEE TRANSACTIONS ON CONSUMER ELECTRONICS.

30 Naomi Woods, M. Siponen. (2019). "Improving password memorability, while not inconveniencing the user". International Journal of Human-Computer Studies.

31 S. Panda, S. Mondal. (2017). "SG-PASS: A Safe Graphical Password Scheme to Resist Shoulder Surfing and Spyware Attack", Cham.

32 Priya Matta, B. Pant. (2018). "TCpC: a graphical password scheme ensuring authentication for IoT resources". International Journal of Information Technology.

33 G. Sadasivam, C. Hota, C. Anand. (2018). "Honeynet Data Analysis and Distributed SSH Brute-Force Attacks". In S. Chakraverty, A. Goel, & S. Misra (Eds.), Towards Extensible and Adaptable Methods in Computing (pp. 107-118). Singapore: Springer Singapore.

34 Seyed Aghili, M. Ashouri-T, H. Mala (2017). "DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT". The Journal of Supercomputing.

35 F. Stajano, M. Lomas. (2018). "User Authentication for the Internet of Things", Cham.

36 Verena Zimmermann, N. Gerber. (2020). "The password is dead, long live the password–Alaboratory study on user perceptions of authentication schemes". International Journal of Human-Computer Studies.

37 Weizhi Meng, L. Zhu, W. Li, J. Han, Y. Lie. (2019). "Enhancing the security of FinTech applications with map-based graphical password authentication". Future Generation Computer Systems.

38 Gi-Chul Yang. (2019). "Development Status and Prospects of Graphical Password Authentication System in Korea". KSII Transactions on Internet & Information Systems.

39 Yangguang Tian, Y. Li, B. Sengupta, N. Li, C. Su. (2020). "Leakage-resilient biometric-based remote user authentication with fuzzy extractors". Theoretical Computer Science.