Knowledge based Authentication Techniques and Challenges

Hosam Alhakami[1], Shouq Alhrbi[2]
School of Computer Science and Information Systems
Umm Al-Qura University
Saudi Arabia, Makkah

***Abstract*—Knowledge-based Authentication (KBA) is an authentication approach, which verifying the user identity when accessing services such as finical websites. KBA requests specific information to prove personal identity of the owner. This paper discusses the challenges that are faced by KBA techniques. Memorability is the main obstacle in KBA since the users trying to utilize simple passwords or unify the passwords in various services, a step that cause problems and issues with compliance with security policies. Furthermore, the technique of mixing username/password is considered as another important challenge of KBA due to the recall-based authentication. This discussion includes a comparative analysis of KBA's techniques based on trade-off criteria to support making of decision. This study's results can support organizations in the recommendations process of a suitable KBA technique for organizations.**

***Keywords*—Knowledge-based authentication; artifact-based authentication; biometric-based authentication; usability; vulnerabilities; memorability; performance; cost**

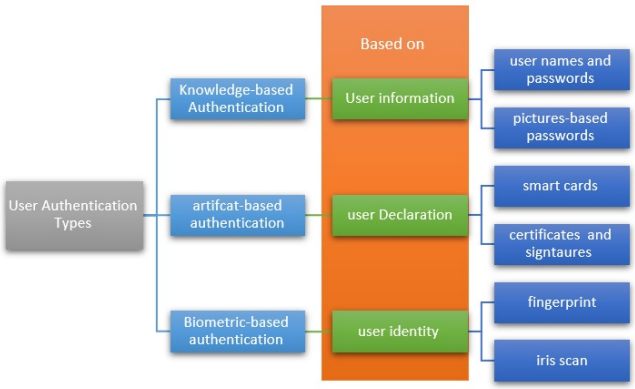

Fig. 1. Types of User Authentication.

I. Introduction

Authorization [1, 2] is the process of ensuring only authorized rights are exercised in the process of determining rights. Authentication is verifying the person's identity, such as (a user, or device) who intends to access data, resources, or applications. Confirming the identity of an entity proves a confidence relationship for interactions. Authentication [3] also allows accountability based on the possibility of mapping the access link and concurrent actions to identities. The techniques of authentication are classified into three essential categories which are token-based authentication, biometric based authentication [4] and knowledge-based authentication system [5]. Fig. 1 illustrates the types of user authentication types [6] but that differs in the focusing idea based on in each type.

Previous researches discuss the different identification and authentication techniques and their different key terms which include protect credentials, identity, password, biometrics, and others [6]. Any system requires to identify its users and authenticate them accordingly depending on the system's target and the target population. User authentication is of three types: knowledge-based, artifact-based, and biometric-based. Any system that relies on the secret user identity information such as text or image passwords that the user provided in the registrations process or when creating passwords is said to be dependent on knowledge-based authentication for its users authentication [7]. Any system that relies on authentication signature or smart issues is said to be dependent on artifact-based authentication for user authentication. Furthermore, any system that relies on the physical characteristics of the user such as fingerprints in the authentication process is considered to depend on biometric based authentication for authentication of its users.

This research targets studying KBA, and specifically emphasizing on security and usability challenges [8]. KBA is an authentication approach that searching the evidence to define of accessing a service. This study discusses different types of KBA and the requirements for each type of KBA. Authentication is necessary in this era of big data revolution on the internet that has affected the mode of human communication and the quality of services provided which all depends on sharing the information. KBA is a popular technique that is used by the largest population of IT systems users but it faces several challenges in this technique.

KBA is known for its simplicity, ease of revocation and legacy deployment that consists of textual and graphical password. Previous studies [9, 10] unearth several attacks that enabled attackers stealing user's identity and confidential information. KBA is defined by an authentication approach that looking for the evidence to define of accessing a service. Static KBA and Dynamic KBA are the main two types [11, 12] of KBA. Fig. 2 discusses these types [11] which figure includes the main feathurs and examples for each type. Static KBA refers to a pre-agreed set of shared secrets like passwords [13]. Dynamic KBA refers to questions generated from a wider based of personal information like registration or verification questions.

In Addition, the static KBA refers to the process that enable users to choose security questions and provide answers that are

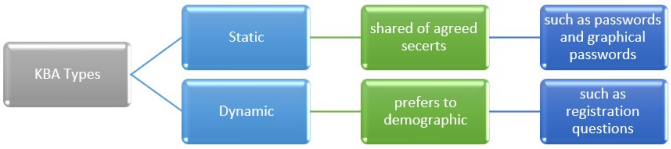

Fig. 2. The Types of Knowledge-Based Authentication.

stored by an organization to be accessed later. Moreover, the dynamic KBA refers to go a step that generate questions that applies only to the intended end user and do not require a previous relationship with the customer. The most used technique for authentication is username and password which is classified into one of the knowledge-based techniques [14]. The essential cause of utilizing password as a popular technique is that it does not require any special target hardware to observe in and out operations on protected areas in the systems [15]. According to the literature, KBA was identified as the approach used to combine some challenges (i.e. questions) to verify claimed users where the answers of these challenges came from their knowledge [16].

This study discuses the definition, importance, types, techniques, and challenges of KBA. Also, it explores KBA techniques which are usability, memorability, performance and cost and any combination of the stated KBA techniques. This paper includes a comprehensive review in term of comparative analysis which will be taken into consideration to provide tradeoffs criteria to help decision makers in their organization so that they can be able to select the most suitable KBA technique. This study mentions recent research trends in this domain.

This paper is organized as the following: Section 2, examining the related works of knowledge-based authentication and its security issues, Section 3, Discussion, Section 4, presents open research challenges of knowledge-based authentication. Finally, Section 5 discusses the conclusion and future works.

II. Related Works

The main goal [17] of a user authentication mechanism is offer security to information systems. Attackers are using several strategies to attack authentication systems that are in use in different systems. Therefore, schemes must be measured with respect to vulnerabilities and susceptibility to various attacks which can indicate absence of enough security for any system that uses that specific scheme. Use of passwords and user-identity in processing of login is one of the most popular scheme. Knowledge-based authentication (KBA) mechanisms utilize the memorized authentication secret that can be a text password (as numbers and characters), a personal identification number (PIN) or a graphical/image password such as CAPTCHA. The benefits of using traditional passwords is that there is no specialized personnel, hardware or software required, simple to use, and easy to remember. But that causes of many problems of using the password, that it is more likely to suspicious attacks and speculation of passwords.

A. Knowledge-based Authentication (KBA)

The evaluation of Knowledge-based authentication (KBA) is best when based on the following criteria that includes static and dynamic type (which illustrated in Fig. 2). A suitable security question should be acceptable to the largest segment population, possess answers that are easy to remember, have no redundant answers for the correct answer, and the answer of security question should not be simple to speculation to find out in searching. For any technique, it is based on KBA that requires to depend on four dimensions [18], which are known as KBA techniques (which illustrated in Fig. 3), memorability, usability, performance, and cost. Previous researches focus on the memorability and usability [16, 17] that differs the Fig. 3 includes other collective techniques performance and cost. There are many research and applications that recommend combinations of these techniques to reach the good level of KBA. Memorability refers to the saving passwords is the browser. Usability is meaning that the uses of passwords in several applications that is vulnerable to attack easily. Performance refers to the strength of password. Cost targets reducing fraud from fraudulent claims.

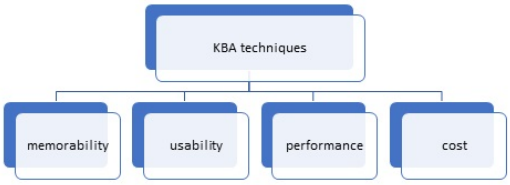

Fig. 3. The KBA Techniques.

Table I illustrates a comparative study between several motivation researches in authentication based on authentication type (which mentioned in Fig. 1), techniques, and the authentication mechanism. This comparison also mentions the advantages and disadvantages of these authentication mechanisms and techniques.

B. Knowledge-based Authentication Challenges

Knowledge-based authentication is the main target of study in this research. Fig. 4 mentions the challenges of KBA, it discusses main problems, security and usability as [8], but it includes the Characteristics of them that are divided into six Characteristics challenges. Table II discusses the comparison between the different types of KBA and their techniques. This research focus on Knowledge-based authentication with passwords credentials and properties. The Knowledge-based authentication has several techniques and challenges which are shown in the comparison Table II.

The two main challenges to KBA is Usability and Security. Each type of KBA has several challenges as the following: usability challenges includes usability in several applications, management problems, and the domino effect. The security challenge includes security issues, searchable personal data, and privacy. Mostly, attacks are the most feared challenge in all the mentioned challenges of KBA. The challenges are discussed in the following:

1) Security challenge

The main challenge of the KBA is how to be safe from attacks and hacks. The required challenge is how to

TABLE I. THE KNOWLEDGE-BASED AUTHENTICATION TECHNIQUES FOR SECURITY ASPECTS

No.	Authentication mechanism	Authentication Type	Technique	Pros	Cons
[19]	password	Knowledge	It includes sign in and sign up for users. It uses mathematical analysis and combination between years and visits number of passwords	prevent multiple brute-force attack	Has a long time
[20]	Finger print	Biometric	It is based on a comparison between four authentication schemes: facial recognition, finger print, pin code, and NFC ring	Higher accuracy And finger scan is easy to use and trus	Can not guarantee the trust in this technique for using in the public setting; Hardness to use facial recognition
[21]	password	Knowledge	efficient password protocols	Ensure the security of data that can be safer from attacks	Hardness security and usability
[22]	Graphical password	Knowledge	A proposed technique is entitled WYSWYE (where you see is what you enter) strategy.	Decrease guessing attacks	Improving accuracy with user's images
[23]	Voice Recognition	Biometric	Using text-to-speech technique and speech-to-text technique	Easy to use and minimize cost and memory	Improve efficiency
[24]	Multi-Factor based authentication(voice, text, iris, DNA, ...)	Biometric	It is based on Multi-Factor Authentication	Improve security level and prevent attacks	Hardness to apply it
[25]	Graphical passwords	Knowledge	The technqiue is based on Pictorial password systems	High secure and usability	Difficulty to upload personal images
[26]	graphical random authentication technique (gRAT)	Knowledge	The technique is based on the classification of the existing graphical password methods into recognition-based, cued-recall-based, pure-recall-based, and hybrid techniques.	More secure and powerful in usability	Complex implementation
[27]	Textual password	Knowledge	Studying twelve passwords schemes	Improving decision making and usability when combining the most used password the is text with fingerprint	That is very powerful for smartphone only
[28]	Dual-Factor Authentication Protocol	Knowledge	It does not employ a password verifies. s dynamically changed each time the user logs in	Increasing security with multi-factors from inside and outside attacks	Time- and energy-consuming

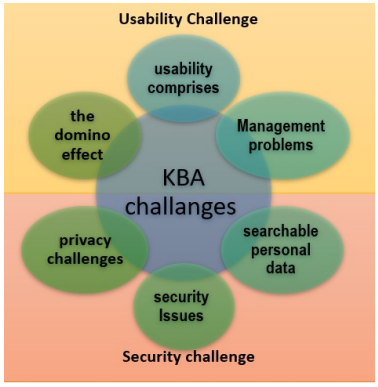

Fig. 4. KBA Challenges.

Fig. 5. Example of username and password profile.

save personal information, as the username and password example are shown in Fig. 5, in various domains.

Previous researches discuss the state-of-the-art of knowledge-based user authentication mechanisms that are classified two dimensions: security and usability. Security authentication mechanisms discuss and compare the strength of each mechanism depends on various policies. The major discussion of this analysis and identify areas for further research and enhanced methodology with the target to drive this research towards the design of sustainable, secure and usable authentication approaches. This challenge divides into three parts: security issues of attack types, searching about the people's information or identity, and privacy challenges of the user accounts. Security challenge is divided into three types as the

following:

a. Searchable personal

The use of passwords that are the same in different social networks simplifies things for users but that is considered a challenge because of the repetition and circulation of the password. That may be caused by easy attacks or guessing the passwords.

b. Security Issues

There are several types of attacks and hacks with fake account or stealing data. Hackers can steal personal data and accounts and sell these data to benefit from the information. The main challenge of security is guessing the account's passwords. There multiple online and offline password guessing techniques that are in use. The famous method to prevent guessing while online is inclusion of CAPTCHA in systems. Offline method does not need computational power, but it is based on several times of guessing passwords and writing them in a repetitive way.

c. Privacy challenges

Privacy is implemented using privacy laws that protects client privacy and aim at controlling access to client's data. So, there is always a need to make verification questions that are not private to users and not discriminate for specific users to avoid attacks.

2) Usability challenge

Usability is considered a critical challenge of managing user's accounts due to the ease of use of the same password in several domains and applications. But it is a threat that threatens the safety and confidentiality of data. It includes management problems of various systems, the problem effect on domains, and usability challenges which can be interpreted in the repeatedly used passwords.

a. Management problems

Management has several problems such as the organization authentication of several users who want to access the system due to the similarity of passwords and registration questions. There are several conditions for suitable questions as the following. They do not include default values, texts, and the organizations have quick recovery techniques for any sudden attacks.

b. Usability compromises

The ability of usability challenges provides to the user some capability. Graphical/audio challenges can be employed. Using the same password in several platforms becomes risk of user accounts. Users are threatened by attackers via guessing accounts users and passwords without the user's knowledge. These guessing of passwords have several policies to minimize the challenge of passwords memorability.

c. The domino effects

The accumulative impact introduces a group of similar events. The idiom is best known as a mechanical impact and is utilized as an analogy to a falling row of dominoes.

C. Knowledge-based Authentication Security Measurements

From previous researches, we found that it is very important to find a way to evaluate authentications for various platform's policies [9,10, 29]. The evaluation criteria are built based on a combination of three parts: password intensity, guessability percentage rate, and entropy measurement.

a. Password intensity: It refers to the strength of using characters, numbers, and the length of the password. The password should not be related to the name or email. A password's intensity can be in one of these types (weak, medium, strong, and very strong).

b. Guessability percentage rate refers to the numbers of speculations from attackers or hackers to guess the user's password. This rate depends on the password's parameters of guassability that is used for improving the password intensity and saving data.

c. Entropy measurement: It is defined by one of the security measurements for each policy. Entropy refers to the random number of ways that users can choose the passwords from given keys that are related to the hardness rate of guessing the textual passwords.

Table II discusses a comparative study of knowledge-based authentication challenges. It reviews the strengths and weaknesses of each technique and suitability in different applications.

TABLE II. A COMPARATIVE STUDY OF KBA CHALLENGES

Application scheme	Password Length (minimum # of characters)	Guessability	Authentication advantages
Google	8	Yes, that is easy to guess google passwords	Weak and short. Powerful and password Strong.
Yahoo	9	Yes, that is simple to suggest yahoo passwords	Can't enough authentication security.
Facebook	6	No, that is not simple enough that has complex rules for prevent many attacks types	It includes three categories: Weak, average or password Strong
Twitter	6	No, that is not easy to attack due to the complexity of passwords authentications It requires very short and clear.	That is classified into four classes Weak, Good, Strong, Very Strong
Instagram	6	No, that does not put complex rules for authentication security and save user's accounts	It has not enough security roles for passwords and length
Amazon	6	No, that is not suitable secure for this system and its users	It has not enough security roles for passwords and length
Booking	8	No, that is not enough secure the used passwords	It has not enough security roles for passwords and length
Linked in	6	No, that does not take care of the importance of authentication passwords	It is a medium password challenge and small length
Ebay	6	No, that has not authentication rules enough for secure system	It has not enough security roles for passwords and length
Dropbox	6	Yes	That is classified into four classes Weak, medium, Good, Great

III. DISCUSSION

The evaluation of Knowledge-based authentication (KBA) technique is satisfied when criteria for static and dynamic KBA are achieved. This criteria consists of:

A. Static: Any system requires strong password (fixed length such as from 6 to 8 characters). It has suitable number of

characters and the password must include special characters and alphabetic letters. It also needs to minimize the complexity to make the passwords and authentication profiles and questions are easy to remember.

B. Dynamic: Any system requires to be dynamic to create suitable security question that are related to the large segments of the population. The answers to the question should be such that, they make it easy for users to remember them easily. But each question requires to have unique answer. This means that there should be no redundant answers for correct answer. The answer of security question should not be simple to speculation to find out in searching.

Since the main goal of user authentication mechanism is to improve the security of the information systems, several strategies are applied by the attackers to compromise the authentication to the system. Passwords have many challenges which include their high susceptibility to exposure to attacks, password guessing, and key-loggers. KBA includes techniques: memorability, usability, performance, and cost, and combinations of any of these techniques. Most of the challenges of implementing KBA techniques are in online services. Also, analysing and testing the strength are essential in comparing different KBA techniques. The comparison will focus on usability, memorability, security, and performance. The research will study cases of combining different KBA techniques, and the resulting framework, its strengths, weaknesses, and applications. Previous researches conclude that the importance of security challenge is bigger than usability. Several applications require to improve their security systems and authentication rules to protect users and to prevent attacks. This improvement might be necessary depending on the KBA security measures.

IV. Open Research Trends

This research can support researchers and students to make several motivations in this area to improve the performance of their security systems. First, they can work on solving the knowledge-based authentication challenges. In the Memorability challenge, the research can improve the memorability to make easy and simple to use passwords but while still adhering to the restrict rules. Use of the same password in several platforms should never be allowed. In the usability challenge, open research provides important information on how to make passwords and authentication for users based on KBA security measurements [30]. For the security issues challenges, open research goes forward to give information on how to prevent attacks and hacks. Second, dynamic KBA is very difficult to implement and is considered harder than Static KBA. Finally, there is no standard reusable model available for dynamic KBA that fits the need of all the organizations.

V. Conclusion and Future Works

This paper introduces the authentication survey and makes comparison of the different types of authentication mechanisms. It discusses the importance of knowledge-based authentication (KBA) from a security perspective. It also examines the challenges of knowledge-based authentication challenges and open more research areas. This survey concludes that there is a good criterion for knowledge-based authentication based on a textual methodology based on the types of KBA whether static or dynamic. Textual KBA is the most usable method although several platforms and studies suggest using an image or graphical authentication mechanisms. Textual KBA faces many challenges to be secure and safe from attackers and hackers. KBA includes four techniques as the following: memorability, usability, performance, and cost, and combinations of any of those techniques. The major challenges when it comes to implementing KBA techniques lies in online services. Also, the strength and analysis will be essential in comparing the different KBA techniques.

Acknowledgment

The research for this paper was financially supported by Umm Al-Qura University. We gratefully acknowledge the support and generosity of the University, without which the this study could not have been completed.

References

[1] Manjunath D, Nagesh A S,Sathyajeeth M P, Naveen Kumar J R, and Syed Akram, A Survey on Knowledge-Based Authentication, Volume 2, Issue 4, 2015.

[2] Mohammad A Alia, Adnan Hnaif, Ayman M. Abdalla, and Mohammad Abu Maria, An improved authentication scheme based on graphical passwords, ICIC Express Letters, Volume 12 (8), pp.775-783, 2018

[3] Alican Beydemir; İbrahim Soğukpinar, Lightweight zero knowledge authentication for Internet of things,International Conference on Computer Science and Engineering (UBMK), 2017.

[4] Hasini Gunasinghe and Elisa Bertino, PrivBioMTAuth: Privacy Preserving Biometrics-Based and User Centric Protocol for User Authentication From Mobile Phones, IEEE Transactions on Information Forensics and Security (Volume: 13) , Issue: 4, 2018.

[5] M. Yildririm, and I.Mackie, Encouraging users to improve password security and memorability,International Journal of Information Security,Volume 18, Issue 6, pp 741–759, 2019.

[6] Nurul Afnan Mahadi, Mohamad Afendee Mohamed, Amirul Ihsan Mohamad, Mokhairi Makhtar, Mohd Fadzil Abdul Kadir and Mustafa Mamat, A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication,Recent Advances in Cryptography and Network Security, 2018.

[7] Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H. and Bhogle, P. (2015). " Comparison of Graphical Password Authentication Techniques". International Journal of Computer Applications (0975 – 8887) April 2015. Vol. 116, No. 1.

[8] Katsini, C., Belk, M., Fidas, C., Avouris, N. and Samaras, G., "Security and Usability in Knowledge-based User Authentication: A Review"., 2016.

[9] Jyoti Deogirikar and Amarsinh Vidhate, Security Attacks inIoT: A Survey, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.

[10] Ramsha Fatima, Nadia Siddiqui, M. Sarosh Umar, and M. H. Khan, A Novel Text-Based User Authentication Scheme Using Pseudo-dynamic Password, Information and Communication Technology for Competitive Strategies pp 177-186, 2018.

[11] Yusuf Albayram, Mohammad Maifi Hasan Khan, Athanasios Bamis, Sotirios Kentros, Nhan Nguyen, and Ruhua Jiang, Designing challenge questions for location-based authentication systems: a real-life study, Human-centric Computing and Information Sciences, 2015.

[12] George Hadjidemetriou, Mario Belk, Christo Fidas, and Andreas Pitsillides,Picture Passwords in Mixed Reality: Implementation and Evaluation, CHI EA '19,CHI Conference on Human Factors in Computing Systems, pp. 1–6, 2019.

[13] Nawaf Aljohani, Joseph Shelton, Kaushik Roy, and Albert Esterline, Robust password system based on dynamic factors,6th International Conference on Information Communication and Management (ICICM), 2016.

[14] Alsuhibany, S. (2016). "Evaluating the Usability of Optimizing Text-based CAPTCHA Generation". International Journal of Advanced Computer Science and Applications (IJACSA) 2016, Vol. 7, No. 8.

[15] Alexander Popov, Neural Network Models for Word Sense Disambiguation: An Overview,BULGARIAN ACADEMY OF SCIENCES,CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume 18, No 1 Sofia , 2018.

[16] Abrar Ullah, Hannan Xiao, and Trevor Barker, A study into the usability and security implications of text and image-based challenge questions in the context of online examination, Education and Information Technologies January 2019, Volume 24, Issue 1, pp 13–39.

[17] Harakannanavar, Sunil Swamilingappa; Renukamurthy, Prashanth Chikkanayakanahalli; and Raja, Kori Basava, ,Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends,International Journal of Advanced Networking and Applications Vol. 10, Iss. 4.

[18] Muhammad Sharif, Mudassar Raza, Jamal Hussain Shah, Mussarat Yasmin, and Steven Lawrence Fernandes, An overview of biometrics methods,,Handbook of Multimedia Information Security: Techniques and Applications pp 15-35, 2019.

[19] Amirul I Mohamad, Mohamad A Mohamed, Mokhairi Makhtar, Mustafa Mamat, Norziana Jamil,and Marina Md Din, A Framework for Experience Based User Authentication Technique for Minimizing Risk of Brute-Force Attacks, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-5S4, February 2019.

[20] Matthias Baldauf, Sebastian Steiner,Mohamed Khamis, and Sarah-Kristin Thiel, Investigating the User Experience of Smartphone Authentication Schemes -The Role of the Mobile Context,Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019.

[21] Kaur, Amanpreet A; Mustafa, Khurram K., A Critical appraisal on Password based Authentication, International Journal of Computer Network and Information Security; Vol. 11, Iss. 1, 2019.

[22] Yogesh V. Mahajan, Ganesh R. Tile, and Paresh S. Patil, Cued Click Point Graphical Authentication,National Level Conference On "Advanced Computing and Data Processing"(ACDP 2K19).

[23] Kapile Namrata Rajesh, Bhanushali Nayan Valji, Pawase Kalpesh Dattatray, Pawar Shubham Gangaram, and Prachi S. Tambe, Voice Assistant for visually impaired person,National Level Conference On "Advanced Computing and Data Processing"(ACDP 2K19),Vidyawarta Research Journal, 2019.

[24] Oladimeji Biodun S, Prof. Gloria Chukwudebe ,Dr. A.O Agbakwuru, and Osodeke Charles Efe, Comparative Study of Multi-Factor Authentication Systems, intternational Journal of AdvancedResearch in Science, Engineering and Technology Vol. 6, Issue 4, April 2019.

[25] Mr.Devidas S. Thosar, Mr.Narayan B. Vikhe, Ms.Rajashree R. Shinde, Ms.Prachi S.Tambe, and Ms.Priyanka S. Hase, ClickPoints:An Advanced Graphical Authentication Using Image Descrimination & Fusion,National Level Conference On "Advanced Computing and Data Processing"(ACDP 2K19), 2019.

[26] Mudassar Ali Khan, et al., g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices, IEEE Transactions on Consumer Electronics , Volume: 65 , Issue: 2 , May 2019.

[27] Verena Zimmermann, and Nina Gerber, The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes,International Journal of Human-Computer Studies Volume 133, January 2020, Pages 26-44.

[28] Abdelrahman Abuarqoub, D-FAP: Dual-Factor Authentication Protocol for Mobile Cloud Connected Devices, journal of sensor and actuator networks, volume (9), issue (1), 2019.

[29] Abrar Ullah, Hannan Xiao, and Trevor Barker,A Dynamic Profile Questions Approach to Mitigate Impersonation in Online Examinations,Journal of Grid Computing, Volume 17, Issue 2, pp 209–223, 2019.

[30] Amanpreet Kaur and K. Mustafa, Qualitative assessment of authentication measures,3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016.