Multi-Factor Authentication to Systems Login

Bandar Omar ALSaleem
Department of Computer Engineering
College of Computer
Qassim University (QU)
Buraidah, Saudi Arabia
bandarsf@gmail.com

Abdullah I. Alshoshan
Department of Computer Engineering
College of Computer
Qassim University (QU)
Buraidah, Saudi Arabia
drshoshan@gmail.com

2021 National Computing Colleges Conference (NCCC) | 978-1-7281-6719-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/NCCC49330.2021.9428806

***Abstract*—Multi-Factor Authentication is an electronic authentication method in which a computer user is granted access to an application or a website only after successfully presenting two or more factors, or pieces of evidence. It is the first step to protect systems against intruders since the traditional log-in methods (username and password) are not completely protected from hackers, since they can guess them easily using tools. Current Systems use additional methods to increase security, such as using two-factor authentication based on a one-time password via mobile or email, or authentication based on biometrics (fingerprint, eye iris or retina, and face recognition) or via token devices. However, these methods require additional hardware equipment with high cost at the level of small and medium companies. This paper proposes a multi-factor authentication system that combines ease of use and low-cost factors. The system does not need any special settings or infrastructure. It relies on graphical passwords, so the user, in registration phase, chooses three images and memorizes them. In the login phase, the user needs only to choose the correct images that he considered during the registration process in a specific order. The proposed system overcomes many different security threats, such as key-loggers, screen capture attack or shoulder surfing. The proposed method was applied to 170 participants, 75% of them are males and 25% are females, classified according to their age, education level, web experience. One-third of them did not have sufficient knowledge about various security threats.**

Keywords—graphical password, multi-factor authentication (MFA), key logger, a third-party authenticator (TPA), screen capture, shoulder surfing, ID.

I. Introduction

Authentication is considered a very important verification method when someone is trying logging into computer resources, such as networks, applications, or devices. Several popular web services such as google and amazon employ multi-factor authentication as an optional feature that is deactivated by default. In IT industry, developers also face serious challenges for securing their systems, wherein unauthorized persons may easily damage many hours of software development, and since fall into consequences of breaking down the system. Consequently, authentication is the process or the action that decides whether a person or an application is allowed to access the system or not.

Modern advances in security versus intruding motivate us to seek for an efficient solution that does not relay on old methods and study traditional methods deeply to enhance them and create new system that avoid all drawbacks of traditional methods. Therefore, several security techniques are proposed, such as Anti-Key-Loggers, Anti-Capture Screening, and Anti-Shoulder-Suffering [1] . Subsequently, even if the hacker is able to expose the username and password by any way, it will be very difficult for him, if not impossible, to break in the system because he would need to know and break all authentication factors.

Psychological research and modern practices support that humans can retrieve pictures faster and easier than words. When you read, for example, a car or a book, you automatically draw a picture of it in your mind, while if you mention words such as ‘amount’, ‘level’, ‘ease’, you may not draw anything and will only remember them as words.

II. Authentication Systems

A. Authentications Types

The main problem with knowledge-based mode is it’s vulnerable to guessing, dictionary attack, key-logger, shoulder surfing, social engineering, and screening capturing. In addition, the cost is considered in case of SMS based factor and difficulty of implementation. Moreover, the user must have a phone number and a subscription of SMS service provider [2]. Another cost is considered when using some devices such as fingerprinting, where the user may be classified suspicious if he buy new device or if he travel outside his country [3]. In addition, biometric mode cannot be applied on all situations due to many reasons; like high cost, need of special devices, or when the person has physical changes.

Therefore, using multifactor authentication might be the best practice. Many researchers use a threshold cryptography multifactor that depends on one time passwords (OTP) with username and password and a pin code generated by the system or token device [4]. A multi-factor authentication system is depicted in Fig. 1.

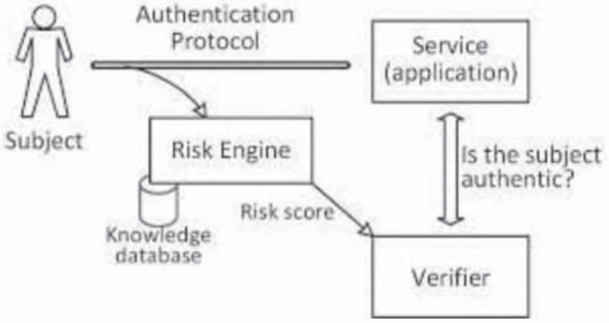


Fig. 1. A multi-factor authentication system

Since the proposed system is focusing on knowledge-based mode, and not using external devices or special configuration, the proposed system combines knowledge-based (username and password) with other factors (like graphical password, PC ID, user information). This allows user to use at least two factors, and the third factor is made optional to be identified and let him access the system. Table I shows the authentications types and modes. Graphical password authentication is a way that uses images as password leting the user draw something during the registration phase, then identify him later by asking him to do it again.

TABLE I. AUTHENTICATIONS TYPES.

Knowledge-based mode	Biometric mode	Mix mode
1. Username and password 2. Pin Code 3. Lock Pattern 4. Graphical password 5. Identification Based on SMS [2] 6. Device Fingerprint [3]	1. Finger Print 2. Face 3. Iris 4. Voice 5. Palm	1. Two factors 2. Multi-factor

The system can be classified as a recognition-based system or a recall-based system. Some examples of the proposed method, under these categories, will be presented below.

B. *Recognition-based systems*

The idea of the recognition-based system is to display images to the user so he chooses the correct image (predefined) by clicking or touching it in particular order. Examples of this category are: Awase-E system [5], Passfaces system [6], Securing Passfaces for description [7], graphical authentication scheme [8], and Implicit Password Authentication System (IPAS) [9], and GPS-based graphical password system [10].

Drawbacks of these systems:

- Social engineering.
- If the system has a vulnerability and hacked the intruder can reach the verbal Password and access to the system.
- Not protected from screen recording.
- Normal pictures easier to remember than shapes.
- Default to remember.

C. *Recall-based systems*

The other category is recall-based systems. The idea of this category is that the user needs to reproduce something during the registration phase that he created or selected. Examples of this category are: Draw-A-Secret (DAS), Pass Doodle [8], Syukri [11], Blonder [12], Cued Click Points [13]. An example of a recall-based system is depicted in Fig. 2.

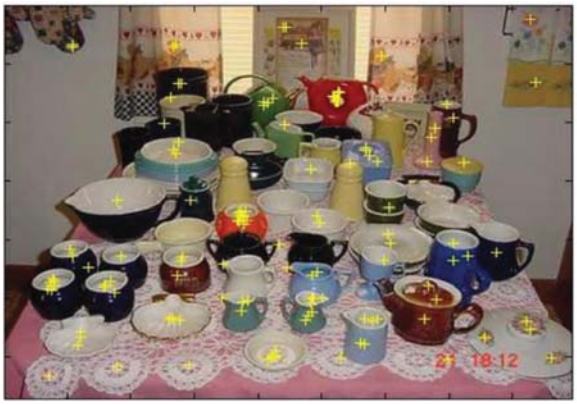


Fig. 2. A recall-based system.

Drawbacks of these systems:

- Not protected against shudder surfing.
- Not protected against screen recording.
- If users forget the points position, it cannot be retrieved and password lost.
- Default to remember.
- If the user forgot the password, he cannot retrieve it.

Another section, some researchers classify it as a third section, is the serial recall, in which points on the image will be clicked by the user in a serial order [14].

III. METHODOLOGY

The proposed method is to find a way that verifies the user in a simple, easy to prepare and publish manner. There are many ideas using image-based verification. It is one of the ideas put forward. Images are the simplest and more appropriate solutions that provide strong protection, in addition to the easy of setup on most programs and systems.

A. *Programing Language*

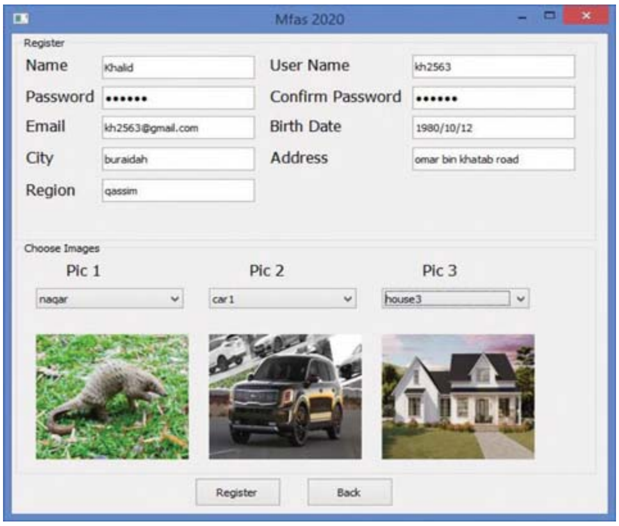
As a starting point, several log-in topologies will be discussed then will narrow down to one final log-in topology, then analyze the whole system after reviewing several programming languages. Python is our vehicle for programing language and SQLite is the database system.

B. *The Proposed System*

Initially, in the proposed system, the user is asked to create username, password, and fill-in all private information, such as name, age, address, and city, etc. During the registration process of the first time, user needs to select three images among several categories in sequence order like (1-red car, 2-white home, 3-black cat). As a second factor of security, it will appear each time the user logs into the system. Then, it appears after entering the user name and password. Categories are represented in the database in a form of images. Each category consists of at least 20 images. This idea may face some difficulties, likeg key-logger's programs, screen recording programs, and shoulder suffering to steal user's personal data. However, in our proposed system, these problems will be overcome as the system is designed in a way that key-logger's software's cannot catch the entered keys. Password, passcode, image number, and category number are stored in the database hashed. When the user try to login to the system, he will be asked for username and password, then when he presses login button, the system generates passcode for every image and graphical screen appears. Also, the proposed system provides a third factor as a feature using the PC ID. This factor makes the user unable to login from another PC if the admin did not add this PC to the user whitelist. After the registration process, the user needs to contact the admin for activating his whitelist.

C. *How proposed system works?*

When the user registers for the first time, he fills the fields of registration form and selects 3 pictures. After that, the system hashing the password field, get the selected photos IDs, merging them and hashing them with SHA256 and stores this data into the user's table. The next stage is to login with the username and password, as usual, and then a screen appears to the user with 9 randomly selected images including 3 correct ones. Some images may not appear. If the correct images did not appear, the user needs to click on skip until the correct ones appear. Then, below each image, a randomly generated code indicates the displayed images, and the user is asked to enter these codes in the box below the image, in the same order that was made during the registration process. The verification equation then verifies the entered code and compares it with the user's table data. If the codes match, then the user is allowed to enter. This process is depicted in Fig. 3.



Mfas 2020

Register

Name: Khalid
User Name: kh2563
Password: ••••••
Confirm Password: ••••••
Email: kh2563@gmail.com
Birth Date: 1980/10/12
City: buraidah
Address: omar bin khatab road
Region: qassim

Choose Images

Pic 1: nagar
Pic 2: car1
Pic 3: house3

Fig. 3. MFAS Registration Screen.

IV. Results and Discussion

In this section, the results obtained from surveys are discussed and analyzed. When reviewing the survey answers, many respondents are unaware of the importance of verification or using strong passwords. Almost 42% of users use non-strong passwords, as well as there are those who do not use two-factor verification in their accounts.

Moreover, many users do not know the correct decision when they face a security problem. This confirms the importance of holding training sessions and workshops for increasing the user awareness of information security and learning the minimum level of information security principles, which some people consider it unimportant.

The number of participants in this survey is 170 participants. 75% of them are males and 25% are females, divided by age group, education level, web experience. About 25% of the participants do not have sufficient knowledge on how to deal with various security threats, as well as the importance of activating the two-factor authentication in various programs.

More than 60% of the users liked the image authentication method used in the survey, however, 26% of them mentioned that it might be difficult for a user's to memorize images. In addition, 33% of the users do not prefer using this method. For authentication methods currently used in apps and websites, about 42% of them, think that it is enough, 28% think that it is medium, 15% think that it is not enough, and 15% said they do not know. Verification methods that users use to log in to systems and applications are shown in Fig. 4.

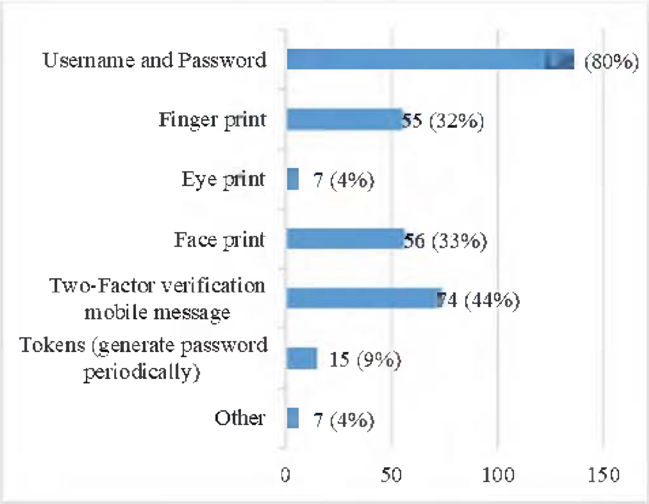


Fig. 4. Verification Methods used by respondents.

The proposal system was tested against 7 of most common key-loggers on Microsoft windows platform. All of these key-loggers failed to detect the password or the image pass code, as shown in Table II. In Table III, the survey results are depicted, however, in Table IV, the advantages and disadvantages of the proposed method is listed. Respondents' opinion for authentication methods on apps and websites is depicted in Fig. 5.

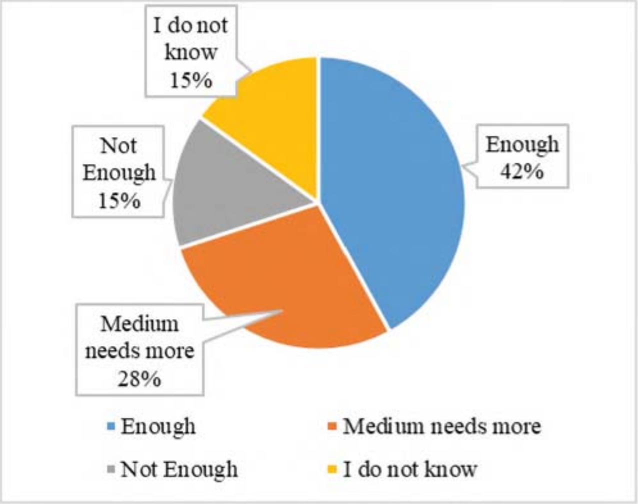


Fig. 5. Verification Methods used by respondents.

TABLE II. Test proposed system against key-loggers.

No.	Key logger name	Version	Detect password or Image Secret code (Keyboard)	Detect password or Image Secret code (Screen recorder)
1.	Refog	9.2	Can't detect	Can't detect
2.	Best Free	7.0	Detected on first version and after updating some points in the program now can't detect	
3.	I want soft	5.3		
4.	Revealer	2.26		
5.	Actual	5.5	Can't detect	
6.	Virtuoza	2.0	Can't detect	
7.	Quick	6.0	Can't detect	
8.				

TABLE III. USER'S INTERVIEW RESULT.

Proposed system	STRONGLY AGREE (%)	AGREE (%)	DISAGREE (%)	STRONGLY DISAGREE (%)
Images Easy to remember	**84**	**10**	**6**	**0**
Is the proposed system better?	**81**	**8**	**11**	**0**

TABLE IV. MAFS ADVANTAGES AND DISADVANTAGES

Advantages:	Disadvantages:
1. **Database Server Not needed:** it is up to programmer if he wants to use or not. 2. **Can work only on file system:** It can be used as a file-based database. 3. **Not required additional devices:** because no fingerprint. 4. **Anti-key-logger:** key-loggers cannot detect what is typed in keyboard. 5. **Anti-screen recorder:** key-loggers cannot detect which picture has been chosen. 6. **Anti-shoulder surfer:** if someone sit behind the user, he cannot catch the password 7. **protected against hardware key-logger, key-sweeper:** − Proposed system uses PC ID. − Image pass code changed every login.	1. **For small and medium business:** big company may need to spend more money for using other secured solution authentication. 2. **Users not familiar with this method:** need an explanation and some practice. 3. **Registration takes longer than normal login:** sometime authentication may take more time. 4. **Can apply on desktop apps and web apps only:** on mobile apps need some changes. 5. **Key-logger, key-sweeper:** user may need secured keyboard and check for physical USB port.

CONCLUSION

In this paper, a multi-factor authentication system that combines the ease of use and the low-cost factors is proposed. The system did not need any special settings or infrastructure. It was designed depending on graphical passwords. In registration phase, the user might choose and memorize three or more images. In the login phase, the user needed only to choose the correct images that he has chosen during the registration process in a specific order. The proposed system might overcome many different security threats, such as key-loggers, screen capture attack or shoulder surfing. The proposed method was applied to 170 participants, 75% of them are males and 25% are females, classified by age group, education level, web experience, where one-third of them do not have sufficient knowledge about various security threats. It also protects the user when installing malicious programs that contain Trojan or Malware, as these malicious programs record everything that user types on the keyboard as well as recording the user's screen. Malicious program may also modify the system files, and hence, for this reason, the proposed system was created to protect the user's data in a way that no program can catch the user passwords or even the authentication methods he uses.

REFERENCES

[1] A. N. O. Hammed M, "PREVENTING SHOULDER SURFING ATTACK IN GRAPHICAL PASSWORD AUTHENTICATION SCHEME," *Ann. Comput. Sci. Ser. Tome 18, Fasc. 1*, vol. XVIII, 2020.

[2] S. Yang and J. Meng, "Research on Multi-factor Bidirectional Dynamic Identification Based on SMS," *Proc. 2018 IEEE 3rd Adv. Inf. Technol. Electron. Autom. Control Conf. IAEAC 2018*, no. Iaeac, pp. 1578–1582, 2018, doi: 10.1109/IAEAC.2018.8577505.

[3] L. Dostalek, "Multi-Factor Authentication Modeling," *2019 9th Int. Conf. Adv. Comput. Inf. Technol. ACIT 2019 - Proc.*, pp. 443–446, 2019, doi: 10.1109/ACITT.2019.8780068.

[4] V. Venukumar and V. Pathari, "Multi-factor authentication using threshold cryptography," *2016 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2016*, pp. 1694–1698, 2016, doi: 10.1109/ICACCI.2016.7732291.

[5] E. E. Ugochukwu and Y. Y. Jusoh, "A review on the graphical user authentication algorithm: Recognition-based and recall-based," *Int. J. Inf. Process. Manag.*, vol. 4, no. 3, pp. 238–252, 2013, doi: 10.4156/ijipm.vol4.issue3.23.

[6] O. Osunade, I. A. Oloyede, and T. O. Azeez, "Graphical User Authentication System Resistant to Shoulder Surfing Attack," *Adv. Res.*, vol. 19, no. 4, pp. 1–8, 2019, doi: 10.9734/air/2019/v19i430126.

[7] H. Umar Suru and P. Murano, "Security and User Interface Usability of Graphical Authentication Systems – A Review," *Int. J. Comput. Trends Technol.*, vol. 67, no. 2, pp. 17–36, 2019, doi: 10.14445/22312803/ijctt-v67i2p104.

[8] M. A. S. Gokhale and V. S. Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," *Procedia Comput. Sci.*, vol. 79, pp. 490–498, 2016, doi: 10.1016/j.procs.2016.03.063.

[9] S. Almuairfi, P. Veeraraghavan, and N. Chilamkurti, "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices," *Math. Comput. Model.*, vol. 58, no. 1–2, pp. 108–116, 2013, doi: 10.1016/j.mcm.2012.07.005.

[10] G. C. Yang, "Development status and prospects of graphical password authentication system in Korea," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 11, pp. 5755–5772, 2019, doi: 10.3837/tiis.2019.11.026.

[11] Y. Meng, "Designing click-draw based graphical password scheme for better authentication," *Proc. - 2012 IEEE 7th Int. Conf. Networking, Archit. Storage, NAS 2012*, no. June 2012, pp. 39–48, 2012, doi: 10.1109/NAS.2012.9.

[12] R. Thawani, P. Rao, A. Jadhav, and S. Rajgire, "Graphical Password for Desktop," *Ijarcce*, vol. 5, no. 12, pp. 231–233, 2016, doi: 10.17148/ijarcce.2016.51250.

[13] R. Shantha, S. Kumari, and S. Viji, "Cued Click Points Password Authentication using Picture Grids," *IJCSN Int. J. Comput. Sci. Netw.*, vol. 4, no. 6, pp. 2277–5420, 2015, [Online]. Available: www.IJCSN.org.

[14] S. A. K. K Himaja Sri, M Vishnu Vardhan, K Nikitha, K M Kiran, "Graphical Password Authentication - Survey," *J. Xi'an Univ. Archit. Technol.*, vol. XII, no. IV, p. 3701, 2020.