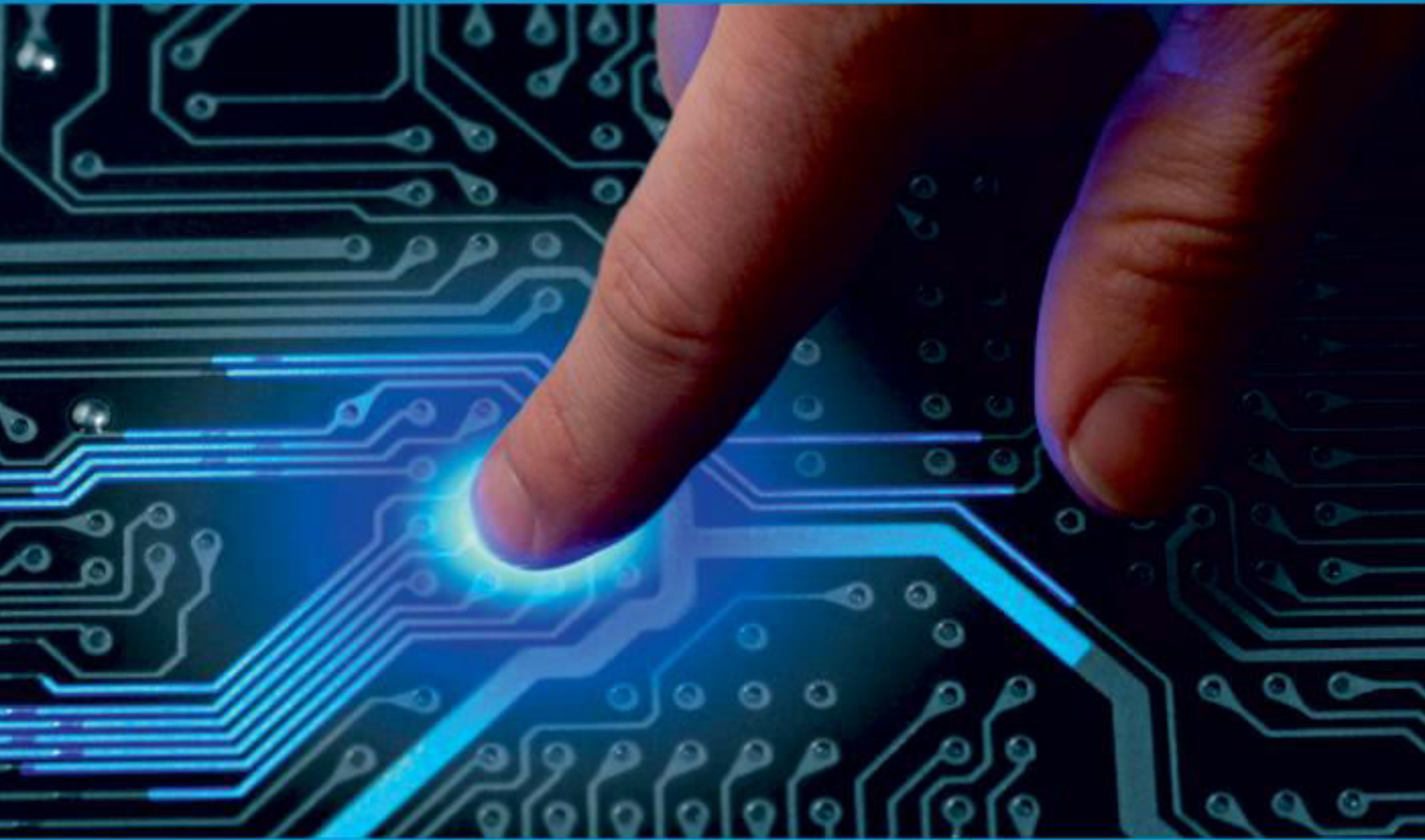
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

Survey on User Multi- Authentication System

Prof. Ms. ASHWINI C, NIKHITHA D

Department of MCA, UBDTCE Davangere, Karnataka, India

Department of MCA, UBDTCE Davangere, Karnataka, India

ABSTRACT: Nowadays, the internet plays a major role in everyone's life where security and privacy are the biggest challenges. The Hackers can easily access the user data if it is not secured or authenticated. There are different methods to provide security to the user. Authentication is one of the important factors to provide security to the system. Security is provided by one-factor authentication (1FA), Two-factor authentication (2FA) which is considered to be an inefficient way. The proposed paper discusses a multi-authentication system, an efficient way to ensure security that consists of three different levels to log in so that only authorized persons have the right to handle that system and related data securely. It also describes the algorithms and techniques used on three different levels (3FA). This paper is mainly to address and survey the significance of practicing the multi-authentication system to add security for applications and websites.

KEYWORDS: Authentication; 1FA; 2FA; 3FA; Security; Password attacks;

I. INTRODUCTION

The main factor to secure the computing system is User Authentication. It is the process where a user is recognized, and only that person can have the right to use the data securely. Authentication is usually provided by username and password, where the password is a secret word to access the resources, and the username is to identify the user. It ensures privacy and keeps sensitive data secured. The process of authentication varies from simple password-based to enhanced authentication systems. Cryptography is one of the ways to secure the data. The transmission of text or images, or any data needs high security, it is achieved by data encryption and decryption. Encryption is the process to convert normal data (plaintext) to unreadable format (ciphertext). Whereas, Decryption converts unreadable data to its original format.

This paper prefers especially more secured system which includes three levels of security such as textual passwords, one-time passwords, and graphical passwords.

Nowadays, every device needs a password to control access to the data. And also it describes different password attacks so that everyone can understand and be aware of them and use secured authentication methods.

A weak textual password can be easily hacked by attackers and if we use a strong password it is hard to remember. So, there are three levels to secure the data, the first level needs the user name and password if it is correct then it confirms the user in the second level by sending an OTP to the registered number or email and the third level is graphical where the user can select images to authenticate the data. This leads to the development of strong authentication techniques.

II. PASSWORD ATTACKS

Brute Force Attacks

Brute force attack is one of the oldest types of password attacks. Usually, it is applied to break the encrypted passwords where passwords are in the encrypted form. All possible combinations of the password are applied to break the password. In the early days, hashing schemes were used to steal passwords. There will be a password file in an operating system that stores the user name and password. The original password is not in a file but it is in hash format and if it is stolen then the password can be caught. The process of brute force attack is very time-consuming as it takes time to search a hash for all possibilities is time taking. This attack is effective for smaller passwords.

Credential Stuffing Attacks

Credential stuffing is the most commonly used cyber-attack where they steal usernames and passwords from one site to access user accounts at a different organization. Most people have multiple accounts and they use the same username and password for each. It is one of the common causes of data breaches as most people reuse the same password for multiple accounts. Credential stuffing can be prevented if the right cyber security measures are implemented. It is prevented by password-less authentication (where they verify users with biometrics instead of password) and Multi-factor authentication (which uses more than one factor for verifying users such as biometrics, one-time password, etc).

Phishing Attacks

The Phishing attack is web-based attack where the attacker deviates from the user to a fake website to get the passwords of the user. Such as fake resetting your password and some links that install harmful code on your device. Usually, it is carried out through email. The main aim of this attack is to steal sensitive data like login information and credit card details. To avoid phishing attacks check the sender of the email and double-check with the source of the mail.

Key Loggers

Key loggers are the type of harmful software designed to monitor every keystroke and report back to the hacker. It is similar to login spoofing attacks and is also called Key Sniffers. The attacker installs key logger software himself or trickily makes the user click to install that malicious file into the user's system. They make the log file of the keys pressed by the user and then send that log file to the attacker. Then finally the attacker gets the password and can access the user system.

III. AUTHENTICATION TECHNIQUES

In general, authentication methods are broadly classified into three types. They are as follows

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

1. Token based authentication

Token-based means something you have. This technique use tokens such as smart cards and bank cards which are used by everyone. A person when loses a key would not be able to open the lock. Similarly, the user when loses token would not be able to log in. Nowadays, people do not rely on the additional layer for security instead they turned to the token-based authentication. Token-based method is quite unprotected from fraud, theft or loss of tokens.

2. Biometric based authentication

Biometric means what you are. It considers the user's physical characteristics to provide security by identifying the user. The most commonly used biometric systems are face detection, fingerprint, and retina scan. Biometric characteristics cannot be similar to one another so it is the only secure way to know about the user. Furthermore, these characteristics cannot be stolen as it happens with tokens and cards, and also no need to remember passwords. Biometrics is more secure if it is paired with a password.

3. **Knowledge based authentication**

Knowledge-based means what you know. It is a technique in which the user is asked to answer a secret question for which the answer is only known to the user. It is a widely used technique for authentication that includes both text-based and picture-based passwords. To log in the user needs to answer the security question based on the user's personal information. In general, it is hard to remember the different security questions. This technique can be used in multifactor authentication to improve the security of the user.

IV. PROPOSED AUTHENTICATION SYSTEM

The paper proposes a multi-authentication system which is a combination of three different authentication techniques. The first level consists of a textual password, the second level is to send OTP to registered numbers and email, and the third level employs a graphical password which will provide a more secure authentication system.

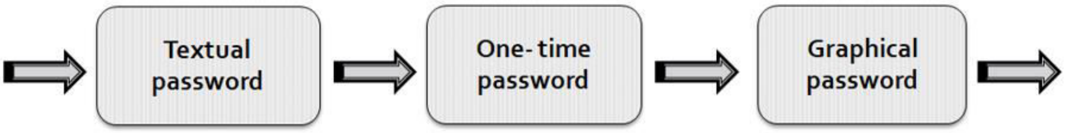
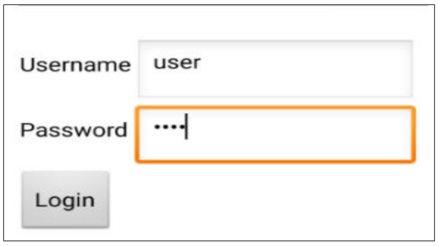


Fig 1 : 3-level password authentication

1. Textual password

A password could be a secret key that offers access to computer resources such as messages, files, etc. Passwords are more than just a key. They maintain privacy by keeping sensitive information secured. A textual password is a string of characters that include numbers or special characters. But these passwords are not fully secured and more exposed to password attacks. To overcome this problem graphical or image password schemes are developed as an alternative to the text-based scheme. When the user sets a password for security that should be easily remembered by the humans and that should be hard to guess by others. Passwords should be changed frequently to avoid password attacks.



Username user

Password ••••|

Fig 2 : level-1 login through textual password

2. One-time password

A one-time password is a dynamic password that changes whenever the user logs in. It is a set of characters that authenticates a user only for one session. Once the password or OTP is used to log in, it is not used for further authentication. This is more secure than a text-based password when the user creates a password that can be weak and unsecured. OTP is the secret code to access the system which changes every 30 or 60 seconds for security.

| DOI: 10.15680/IJIRCCE.2022.1005340 |

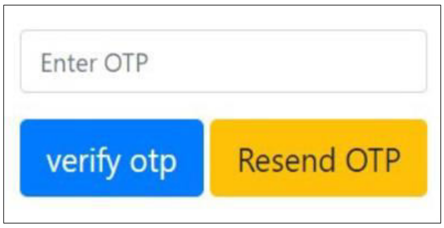


Fig 3 : level-2 login through one-time password

3. Graphical password

The graphical password authentication provides high security. These methods are broadly classified into three types – Recall based, Recognition based, and Cued click points.

- Recall-based

  In this method, the user recollects something that he selected at the registration stage. During login time, the user has to select with tolerance in the correct sequence otherwise he would not be able to log in.
- Recognition-based

  When the user registers, have to select the image from a large set of images. While login the user has to recognize the pre-selected image from various images.
- Cued Recall-based

  Cued click points is a technique where users click one point on each image instead of clicking on five points on one image. It alerts the users if they make mistake while selecting their last click point.

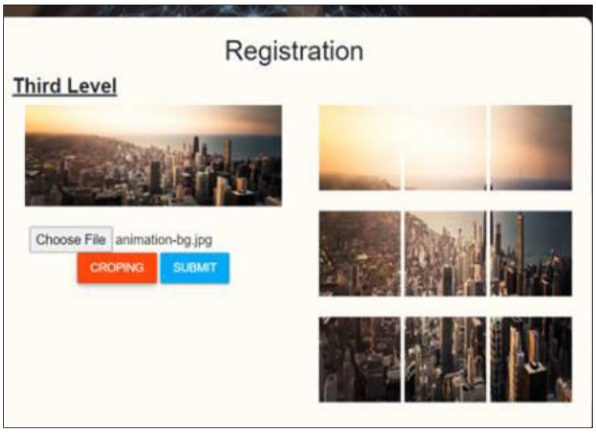


Fig 4 : level-3 login through graphical password

V. METHODOLOGY

In the registration phase, the user has to provide user details such as username and password which is strong and difficult to guess. The users have to register with a phone number so that OTP would be sent to their number while logging in. The advantage of this method is that there is no need to remember the password and no threat of password attacks. And at last, the user must select one of the images from a set of images to register and should remember so it is used while logging in. After all, the steps are completed user completes his registration.

This user-friendly multi-authentication system involves three security levels. Here, the preceding level must be passed to move to the next level of authentication. As shown in fig 2, the user should enter a username and password to log in which is the first level of authentication. The system validates the password and if passed, the user can proceed to the second level of authentication for one-time password verification. Here user gets a random code to a registered mobile number, the user has to enter that 6-digit code to log in. Once the second level gets verified then only it proceeds to third level authentication. Where the user has to select a pre-selected image at the time of registration from a set of images. This is the last level of authentication. The last level is also validated, the user can get access to the system otherwise access can be denied.

The multi-authentication secures the system from attackers and the level of security also increases. If it was one-level authentication only the password could not protect the system that effectively. So, a multi-authentication system is commonly used by the users to protect their sensitive information.

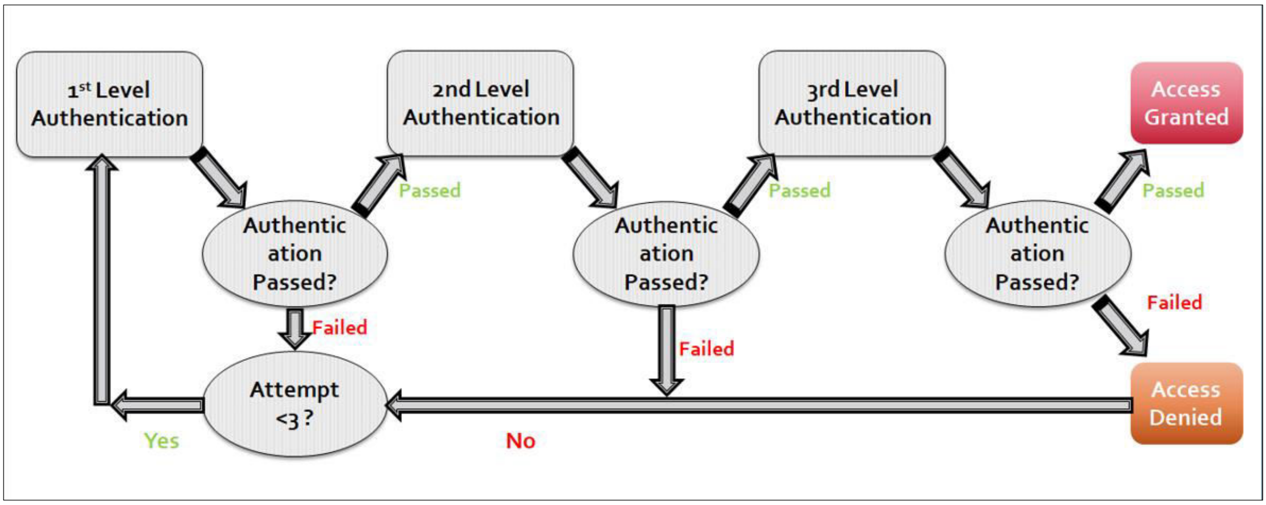


Fig 5 : Flow diagram of three-level authentication system

VI. CONCLUSION

Authentication enables their networks to be secured by permitting only authenticated users to access their protected resources. Till now, no authentication mechanism is efficient and effective to provide proper security. The paper explains the multi-authentication technique which employs three levels such as textual password, one-time password, and graphical password. The combination of these three methods enhances the security of computer resources. Also, this paper can be helpful to design more secure password schemes.

VII. ACKNOWLEDGMENTS

Sincere thanks to Ms. Ashwini C, Faculty of the Department of MCA for providing support and motivating to carry out the project as listed under the paragraph “METHODOLOGY”.

REFERENCES

1. Lalu Varghese, Nadiya Mathew, Sumy Saju, Vishnu K Prasad (2014): 3-Level Password Authentication System. International Journal of Recent Development in Engineering and Technology Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)
2. M.Manjunath, K. Ishthaq Ahamed and Suchithra (2013): Security Implementation of 3-Level Security System Using Image Based Authentication. Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com Volume 2, Issue 2, March – April 2013

3. Nagesh.D Kamble and.Dharani J (2014): Implementation of Security System Using 3-Level Authentication. International Journal of Engineering Development and Research (www.ijedr.org) © 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939
4. International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October2012 1 ISSN 2229-5518. IJSER © 2012 http://www .ijser.org
5. Y. X. A. C. J. Z. R. D. Xinyi Huang, "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems," IEEE, vol. 22, no. 8, pp. 1390-1397, 2010.
6. Passlogix graphical password system, www.passlogix.com [Last Visited on 01/11/21].
7. Alomar, N.; Alsaleh, M.; Alarifi, A. Social authentication applications, attacks, defense strategies and future research directions: A systematic review.
8. Anand Sharma and Vibha Ojha, 2010. Password based authentication: Philosophical Survey. IEEE.
9. Walanjkar, D. D., & Nandedkar, V. (2014). User authentication using graphical password scheme: a more secure approach using Mobile Interface. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), Vols, 2(12).
10. Towhidi, F., Manaf, A. A., Daud, S. M., & Lashkari, A. H. (2011). The knowledge based authentication attacks. In Proceedings of the International Conference on Security and Management (SAM) (p. 1).

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details