Three-Factor Authentication Using Graphical Password

Kaushik Bhadane, Vipul Patel, Viraj Yadav, Nisarg Kutwal

Abstract—In recent times, digitization is spreading extensively in every part of modern society. One of the ways to keep this process secure is authentication. Authentication covers various areas of the digital world like online payments, communications and access rights management. Multi-Factor Authentication (MFA) is a combination of various authentication methods to create a secure authentication system. MFA adds an extra layer of security in the process of authentication. This paper surveys the already existing methods that authenticate a user with the system and identifies the gaps. The survey contains the challenges from the user's perspective. The proposed method suggests a graphical authentication method as a third factor; as graphical passwords are easy to remember over a long period of time.

Index Terms— Computer Security, Graphical Authentication, Implicit Framework, Login Security, Multi-Factor Authentication, Secure Login, Three-factor authentication.

1 Introduction

In today's world, everything is getting online creating a need for a secure authentication system to prevent unauthorized access to valuable users' data. But the majority of the users are using only username-passwords for login [1]. But the passwords are weak, reused, or commonly used. Most of the users are unaware of the potential attack vectors created by these passwords. To reinforce the rudimentary username-password, multi-factor authentication is used for adding extra layers of security. The most common example of MFA is 2FA. Generally, 2FA uses possession-based authentication methods like OTP, TOTP, push notification, etc. [2] Considering the significance of data in the current routine, more than 2 layers of security are required. Here comes 3FA in the picture providing one more layer of security.

In this survey, different research papers consisting of various authentication methods from a large pool were referred. After studying existing authentication methods and comparing them based on various parameters. From the analysis of survey results, distinct advantages and disadvantages became clear. The system proposed in this paper is a three-factor authentication system using username-password as the first factor, OTP as the second factor, and graphical password as the third factor. The graphical authentication method suggested by us is a memory-based authentication method as the graphical passwords are easy to use as well as easy to remember [3]. Graphical passwords are very hard to brute-force or guess, providing protection against various attack vectors.

2 Literature Survey

In 2013, [1] in a study of different multi-factor authentication techniques, as well as advantages and disadvantages of the MFA, are explained with various examples of techniques in three steps as

1. Something you know, e.g., Passwords, PIN, CVV no.
2. Something you have, e.g., OTP, smart cards, ATM, USB thumb drive.
3. Something you are, e.g., Biometrics, hand geometry, IRIS.

In 2019, [2] in a two-week survey to compare five common multi-factor authentication methods. The survey was based on usability and comparison between the five 2FA methods with 72 participants, collecting both quantitative and qualitative data on a dummy banking website. The methods used are Printed Codes, Push Notifications, SMS, TOTP, and U2F keys. The survey found that U2F keys are the easiest to use followed by TOTP and Push Notification. Considering the Time/Speed factor U2F keys are the fastest method of authentication followed by Push Notification. The survey also compared the usability of the setup phase for all of the five 2-factor authentication methods. While a few participants had difficulty in using U2F and TOTP as second factors.

In 2017, [3] the authentication system used consisted of four authentication stages. Three of which use the knowledge factor and the remaining one uses the possession factor. The authentication stages are the first stage as username & password the Second stage is an innovative authentication idea based on pattern remembering which is created in the registration process. Third stage as during login the user needs to put a preselected 5-digit pin. In the fourth stage as the system provides users with a seed value, they will need to input into their smartphone app to generate a passcode and enter it into the system. Two methods in the system are chosen randomly to increase security without sacrificing convenience. The system is resistant to almost all known types of attacks like Brute

- *Kaushik Bhadane is currently pursuing Bachelor's degree program in Computer engineering in MIT Academy of Engineering, Alandi, Pune, India PH-+919049998692. E-mail: krbhadane@mitaoe.ac.in*
- *Vipul Patel is currently pursuing Bachelor's degree program in Computer engineering in MIT Academy of Engineering, Alandi, Pune, India PH-+919049998692. E-mail: vrpatel@mitaoe.ac.in*
- *Nisarg Kutwal is currently pursuing Bachelor's degree program in ENTC engineering in MIT Academy of Engineering, Alandi, Pune, India PH-+919049998692. E-mail: nskutwal@mitaoe.ac.in*
- *Viraj Yadav is currently pursuing Bachelor's degree program in Computer engineering in MIT Academy of Engineering, Alandi, Pune, India PH-+919049998692. E-mail: vlyadav@mitaoe.ac.in*

force attacks, Shoulder surfing because of graphical methods and 120 seconds timeout on each factor.

In 2011 [4] authors from Microsoft introduced authentication for legacy devices using trusted devices for solving challenges issued by servers and authenticating users without any extra processing on legacy devices. A similar method can be used to authenticate untrusted devices. Challenge may involve a numerical code that is to be entered in a trusted device then the solution is driven through the client application and is to be entered into the authentication portal and confirmed by server user then get authenticated for further activity.

In 2012, [5] a click-draw-based graphical password scheme was Proposed. Introducing a secret during the registration process and using it to authenticate users thus increasing password space and preventing regular text-based attack vectors. An image is provided by the user or selected by the server, hot-spot a clickable area is decided for the click draw base scheme. The secret consists of the selection of predefined sections of the grid in a specific sequence.

In 2013, [6] a study analysed 10 recognition-based and 12 recall-based graphical user authentication algorithms based on their usability, characteristics, drawbacks, and security attacks. Shoulder-surfing, Description, and Dictionary have been identified as the attacks that these authentication algorithms are most resistant to.

In 2013, [7] an implicit way to authenticate users using grids was introduced. Recall, recognition, pure recall, crude recall are different techniques suggested in the paper for implementing implicit authentication. An image is chosen from a pool of images based on the user's profile then a grid is introduced to create a secret relationship between image and grid. Then the same secret is used for authenticating users. Different types of secrets each use a unique approach for the relationship between image and grid and the approach to authentication.

In 2014 [8] authors conducted a usability study on authentication of tabletop devices with 16 participants with a mean age of 24. A total of 4 authentication types were considered on Microsoft Surface 2.0handsets Username and PIN Condition (UsPi), Username and Password Condition (UsPa), Tag, Tag and PIN Condition (TaPi). Tre results suggest the Tag (single factor) is the fastest method. TaPi was not the fastest for authentication, but users say TaPi authentication to be the most secure. A tangible user interface (TUI) was used for the study to provide a similar experience and prevent bias.

In 2015, [9] a Chebyshev chaotic map-based authentication protocol was proposed to address the security issues in RFID systems. The proposed architecture focuses on authentication and anonymity to enhance security and protect privacy. particularly Chebyshev polynomial semigroup with chaotic property is introduced to authenticate identity. For session freshness dual random numbers are generated, and one-way hash functions are adopted for data integrity. An efficient implementation of hash function as well as a power-saving module for maps, could be introduced with 16K to 23K gates.

In 2016, [10] authors proposed a graphical password-based 2-factor authentication system. The user needs to provide the username and graphical password at the time of login. For the first factor, the user has to enter a correct username and for a graphical password, there should be a correct selection of images in a sequence. The order of images within the set will differ at every time user logs in. For the second stage, the preselected image and the preselected three questions are used. In the second stage, areas/regions of images are selected as answers to the questions at the time of registration. At the time of login, the user will be asked to click on the area/region of the image as the answer. As password space is large it secures against brute force techniques. It is easy for user to create and memorize Passwords easily. Randomization at two steps provide better security against shoulder surfing threats.

In 2018, [11] the authors surveyed existing and emerging sensors (material providers) that allow user authentication through the system directly or through the cloud. The corresponding challenges from the user and the service provider's perspective are also reviewed. The MFA program based on Lagrange polynomials postponed within the Shamir's Secret Sharing (SSS) program has also been proposed to enable more flexible validation. This solution incorporates user verification conditions even if some features are different or missing. Our framework allows for the validity of non-existent content by verifying user without disclosing sensitive biometric data to the verification business. Finally, a vision for future trends in the MFA is discussed.

In 2019, [12] Authors proposed a novel pattern-based multifactor authentication scheme that involves the use of a combination of textual and graphical passwords. The proposed system has a larger password space and is secure against dictionary attacks. Moreover, a brute force attack would require an automatic generation of all possible mouse-click and text combinations to crack the actual password. This renders the brute force attack infeasible for the proposed system.

In 2020, [13] Defined a way to design an authentication scheme for SIP signalling protocol, due to the fact that IP Telephony based on SIP technology has been gaining attention for its progressive approach in providing VoIP service. At the same time, it has raised many new studies topics, particularly across the area of security. The new proposed 3-factor authentication scheme in this paper is scalable and every day for supplying safety services to its quiet-person. They have confirmed that the proposed scheme can assure against any potential known assaults in conjunction with the attacks identified in Mishra’s scheme. We have compared the performance with other related schemes and confirmed that the proposed scheme possesses greater safety features and is rapid for verbal exchange.

In 2020, [14] the report focusing on the intention and disseminate threats to National Security Systems, and issue cybersecurity specifications with mitigations, as well as to help Executive departments and agencies with security programs. It also includes a systematic review and comparison of Selecting Secure Multi-Factor Authentication Solutions

In 2013, [15] authors from La Trobe University introduced an implicit way to authenticate users using grids. Recall, recognition, pure recall, crude recall are different techniques suggested in the paper for implementing implicit authentication. An image is chosen from a pool of images based on the user's profile then a grid is introduced to create a secret relationship between image and grid. Then the same secret is used for authenticating users. Different types of secrets each using a unique approach for the relationship between image and grid and the approach to authentication.

In 2021, [16] a Modified ECC (Elliptic Curve Cryptographic) based secure data transfer and three-factor authentication system in the untrusted cloud environment to improve SL (security layer) in the CC (cloud computing) environment was proposed. The proposed system includes steps like compression, data authentication, and secure data transfer. For authentication, the SHA-512 and CCP are utilized. Then data is compressed utilizing CHA. The data are securely uploaded on the CS by MECC.

In 2021, [17] the proposed system, the user can log into the system without much of a stretch and proficiently. It reduces the security and convenience of the proposed system and creates a possibility of shoulder surfing and unplanned login. To use the proposed system, the user needs to initially enrol himself into this system by recording up the fundamental form for information.

In 2021, [18] a new authentication scheme for secure OTP generation using smartphones uses a lie sequence method in BrightPass mechanism with a nested hashing function for secure OTP generation on mobile phones was proposed. The server challenges the user with two variables then the server calculates its OTP using the same index variables and server-side SEED at the same time. The user enters the same variables in the system which generates a client-side PIN on the device itself.

In 2021 [19] a multifactor authentication scheme that combines all existing authentication schemes into a single 3D virtual environment was proposed. Alphanumeric passwords are the most commonly used authentication techniques in the world. Both recognition-based and recall-based authentication techniques have a few downsides & constraints when they are used independently or used as a sole authentication scheme at a time.

In 2021, [20] a Two-Factor Verification Scheme using a graphical password for a Web-Based authentication tool; besides it also avoids the use of a verifier table at the server for completing the user verification was proposed. E-design of an authentication scheme for e-services that should be resistant to various attack vectors like stolen verifier.

2.1 Highlights of the literature survey:

1. The graphical authentication method is fast, secure, user-friendly as well as efficient.
2. Graphical passwords are easy to remember.
3. Visual cryptography can be used to deliver passwords securely by dividing graphical passwords into multiple layers.
4. The implicit framework prevents shoulder surfing attempts and provides a secure way to authenticate users.

3 Gap Identification

1. It is hard to remember long and complex passwords, therefore users use simple passwords and reuse them.
2. The second factor like OTP can be easily bypassed if the intruder has access to the user's trusted device.
3. Several authentication methods are secure but they are not user-friendly; whereas some authentication methods are fast and user-friendly but they are not secure.
4. Some methods are secure as well as fast; but they require external hardware for implementation like U2F keys, biometric scanners, etc. which reduces the system efficiency. U2F keys are not compatible with all browsers and older versions.
5. Authentication methods like OTP and push notifications require mandatory access to a trusted device.

4 Proposed System

A functional web application implementing a three-factor authentication system. Where the first factor will be username-password, the second factor will be OTP and the third will be graphical password.

5 Methodology

5.1 Username-Password:

Username-Password is the most commonly used method of authentication using a passphrase consisting of alphanumeric characters and symbols. The user creates and remembers a username and a passphrase and uses it to authenticate.

At the time of sign-up, the user has to create a username and password by filling up the required information and saving it in the database. At the time of login, the user has to enter the predefined username and password. If the login details are valid then the user will be directed to the next authentication page else if the login credentials are invalid user has to retry to login.

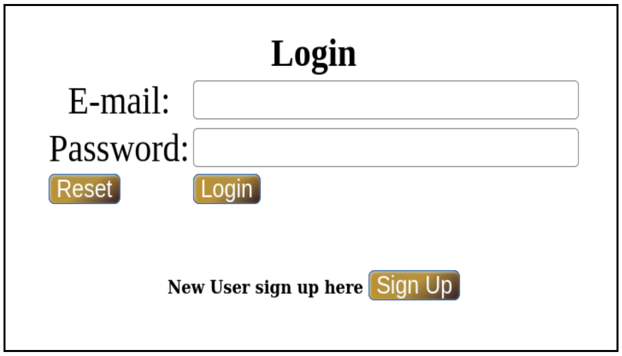
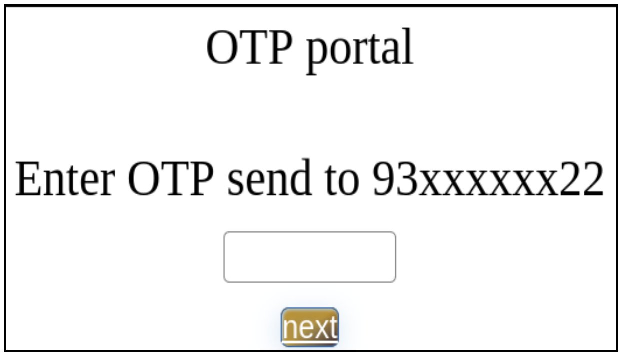


Fig. 1. First factor (username-password)

5.2 OTP:

OTP is a possession-based authentication method. The user is authenticated using a randomly generated code delivered via SMS or Email through a trusted device.



OTP portal

Enter OTP send to 93xxxxxx22

Fig. 2. Second factor (OTP)

The user has to select a phone number or email id to get an OTP via email/SMS which the User has given at the time of registration. If the OTP is correct then the user will be directed to the next authentication page otherwise, the OTP is invalid; the user has to retry or be asked to resend the OTP.

5.3 Graphical Method:

The graphical authentication method is a knowledge-based authentication method in which the user creates a secret with the authenticating system and remembers it, while the authentication system creates a challenge to confirm the identity of the user.

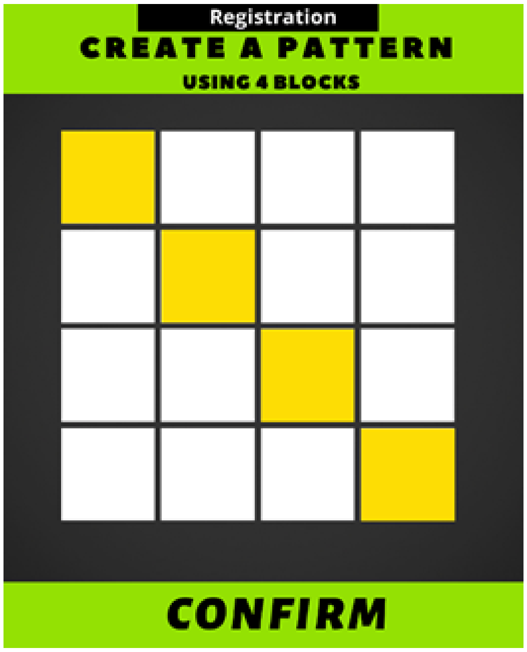


Fig 3. Third factor (graphical password registration)

While registering the user has to select a pattern in a 4x4 grid. At the time of login, the user will be given a 4x4 image grid with random images and 4 random images from the grid to verify the pattern. The user will check the checkbox if the corresponding image is on the pattern, else the checkbox will be left unchecked. The server will then verify the choices made by the user to authenticate.

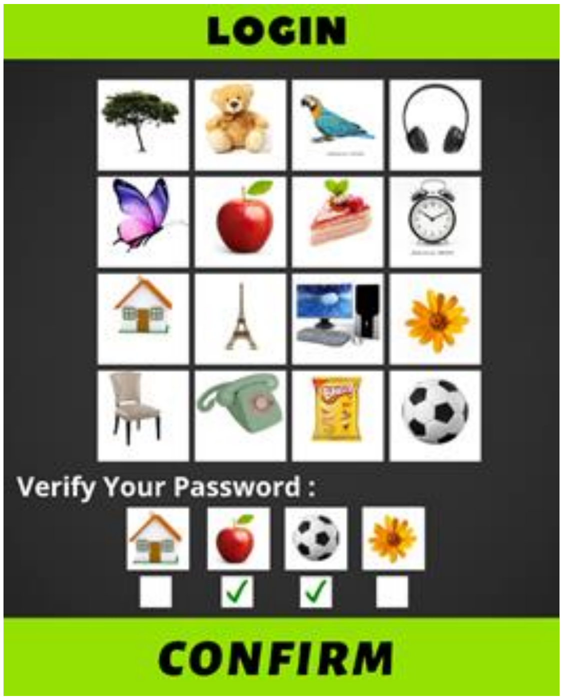


Fig 4. Third factor (graphical password login)

6 Conclusion and Future Work

After referring to many authentication methods, it was clear that single-factor authentication like password or pin is no longer considered as a best security practice. This research paper survey identifies the advantages and drawbacks of the existing authentication methods. In the prominently increasing digital world, at least two-factor authentication is vitally required to create a secure digital environment. The second factor mainly focuses on possession-based authentication. But the second factor can be bypassed, by gaining access to the trusted device. Here, the third factor helps to overcome this issue by adding a completely memory-based authentication layer.

The extra layer of the proposed memory-based implicit graphical authentication method is more secure than the traditional 2FA. Graphical passwords are efficient, secure and implicit. By default, they counter some of the possible attack vectors.

In the future, depending on the requirements and circumstances, different combinations of authentication methods can be created to develop multiple authentication systems focusing on speed, security, or usability.

REFERENCES

[1] B. Madhuravani, Dr. P. Bhaskara Reddy, P. Lalitha Samantha Reddy, “A Comprehensive Study On Different Authentication Factors”, in International Journal of Engineering Research & Technology (IJERT) Vol. 2, 2013

[2] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons, “A Usability Study Of Five Two-factor Authentication Methods”, In USENIX Symposium on Usable Privacy and Security (SOUPS) 2019: 357-370, 2019

[3] Monther Aldwairi, Saoud Aldhanhani, “Multi-factor Authentication System”, In International Conference on Research and Innovation in computer Engineering and Computer Sciences (RICCES'2017), 2017

[4] Ziqing Mao, Dinei Florˆencio Cormac Herley, “Painless Migration From Passwords To Two-factor Authentication” IEEE SPS, 2011

[5] Meng, Weizhi, “Designing Click-draw Based Graphical Password Scheme For Better Authentication”, in IEEE 7th International Conference on Networking, Architecture, and Storage, 2012

[6] Ejike Ekeke Kingsley Ugochukwu, Yusmadi Yah Jusoh, “A Review On The Graphical User Authentication Algorithm: Recognition-based And Recall-based”, International Journal of Information Processing and Management, 238-252, 2013.

[7] Almuairfi, Sadiq & Veeraraghavan, Prakash & Chilamkurti, Naveen, “A Novel Image-based Implicit Password Authentication System (Ipas) For Mobile And Non-mobile Devices”, Mathematical and Computer Modelling, 108–116, 2013

[8] Anders Bruun, Kenneth Jensen, Dianna Kristensen, “Usability Of Single-factor And Multi-factor Authentication Methods On Tabletops: A Comparative Study”, 5th IFIP WG 13.2 International Conference, 2014

[9] Zhihua Zhang, Huanwen Wang, Yanghua Gao, “C2mp: Chebyshev Chaotic Map-based Authentication Protocol For Rfid Applications”, Pers Ubiquit Comput, 1053–1061, 2015

[10] Mrs. Aakansha S. Gokhale, Vijaya S. Waghmare, “The Shoulder Surfing Resistant Graphical Password Authentication Technique”, in Procedia Computer Science, 490-498, 2016

[11] Ometov Aleksandr, Bezzateev Sergey, Makitalo Niko, Andreez Sergey, Mikkonen Tommi, Koucheryavy Yevgeni, “Multi-Factor Authentication: A Survey”, 2018

[12] Miss Pankhuri & Sinha Akash & Shrivastava Gulshan & Kumar Prabhat, “A Pattern-Based Multi-Factor Authentication System", Scalable Computing, 101-112, 2019

[13] Saeed Ullah Jan, Fawad Qayum, Ajab Khan, “SIP Issues and Challenges -A Scalable Three-Factor Authentication Scheme”, in Mehran University Research Journal of Engineering and Technology, 287-309, 2020

[14] National Security Agency | USA, “Selecting Secure Multi-factor Authentication Solutions”, 2020

[15] Ponnampalam Pirapuraj, Nafrees A C M, Kariapper Ahmadh, Razeeth Suhail, “Effectiveness of Atm and Bank Security: Three-Factor Authentications With Systematic Review”, in Journal of Physics Conference Series, 2020

[16] Dilip Venkata Kumar Vengala, D. Kavitha, A. P. Siva Kumar, “Three-factor Authentication System With Modified Ecc Based Secured Data Transfer: An Untrusted Cloud Environment”, Complex & Intelligent Systems, 2021.

[17] Bhumika Patel, Amaan Sarwar, Prof. Sachin Chavan, “Graphical Password Authentication Using Colour Login Technique”, in International Research Journal of Engineering and Technology (IRJET), 3650-3653, 2021

[18] Ms.Saylee Deshpande, Vimla Jethani, “Multifactor Authentication On Mobile Phones Using Existing Brightpass”, in Turkish Journal of Computer and Mathematics Education Vol.12 No.12, 948-953, 2021

[19] Rahul Thakran “3d Password- A Desirable Unification Of Pre-existing Authentication Techniques” International Journal of Research Publication and Reviews Vol(2) Issue(6), Page 185-195, 2021

[20] Khaja Mizbahuddin Quadry, A Govardhan, Mohammed Misbahuddin, “Design, Analysis, And Implementation Of A Two-factor Authentication Scheme Using Graphical Password”, Computer Network and Information Security, 39-51, 2021