Three-Factor Authentication using Image-Grid Graphical Password

Kaushik Bhadane[1], Vipul Patel[2], Viraj Yadav[3], Nisarg Kutwal[4], Dr. Manish Giri[5]

Kaushik Bhadane
Computer Engineering
MIT Academy of Engineering
Pune, India
kaushikbhadaner@gmail.com

Vipul Patel
Computer Engineering
MIT Academy of Engineering
Pune, India
01vipulrpatel@gmail.com

Viraj Yadav
Computer Engineering
MIT Academy of Engineering
Pune, India
virajly007@gmail.com

Nisarg Kutwal
Electronics and Telecommunication Engineering
MIT Academy of Engineering
Pune, India
nature9173@gmail.com

Dr. Manish Giri
Computer Engineering
MIT Academy of Engineering
Pune, India
mbgiri@comp.maepune.ac.in

***Abstract*— In the high-tech digital world, authentication plays a vital role in making our online presence secure. Authentication is a must for various applications like digital asset management, social media, online communications, digital payments, different online businesses, etc. But in the modern world of technology, two-factor authentication is not sufficient as existing methods for the second factor can be bypassed/breakthrough easily. Here three-factor authentication comes into role. As graphical passwords are not only secure but also easy to remember and recall, using the graphical password method as a third factor in authentication strengthens security by far. This paper proposes a three-factor authentication method by using a graphical password as a third factor to secure our online presence.**

Keywords—Multi-Factor Authentication, Graphical Authentication, Graphical Password, Login Security, Implicit Framework, Three-Factor Authentication

I. Introduction

In today's modern era, most of the things are getting online such as banking, food ordering, social networking, etc. But securing the online presence is as important as becoming online. In general, most of the elder people use common passwords for their accounts that can be easily guessable and can easily be cracked. Some people use the same common password for multiple accounts which can be very dangerous. Having only a username and password for authentication is not sufficient to secure the online presence. Also in two-factor authentication, various generally used authentication methods like push notifications, OTP, and TOTP require a smartphone as a prerequisite.

Apart from that, it has also been observed that many people have default settings on their smartphones such that the incoming SMS and notifications are visible on the lock screen. As a result, anyone can see the important notifications containing OTPs and can bypass the second factor of authentication. If the smartphone gets stolen and the intruder/attacker has that smartphone or access to the smartphone; then the second factor will also become meaningless.

Hence, there is a need for an extra layer of security as a third factor because it should be universally adaptable and doesn't require any device as a prerequisite.

Here three-factor authentication with a graphical password as a third factor comes into role. Graphical passwords are not only easy to use but also they are easy to recall. They are hard to guess and brute force.

The three-factor authentication system proposed in this paper uses username & password as a first factor, OTP as a second factor and graphical password as a third factor. The proposed graphical password method does not require any special device as a prerequisite. It is total memory based so only registered users can authenticate it. It also protects against shoulder surfing as it is implicit.

The inability of two-factor authentication to prevent attackers from gaining access to a user's account resulted into development of a new efficient and secure third factor for authentication; which should be easy to learn as well as easy to remember and recall.

II. Literature Survey

A solution for complex text passwords is to use multifactor authentication techniques which don't need the user to remember complex passwords and makes the process easy, fast and secure. As researched by Reese, Smith and others [1] that the users had higher success rate for using the techniques which were easy for them like push notification, TOTP, etc. and didn't require them to remember text passwords.

Another way to add security to authentication system is by using physical devices like RFID scanners[9], Biometric scanners[2], U2F keys[1], etc. But using these types of authentication methods makes the process complex and adds hardware requirements discouraging users to use multifactor authentication further[1].

An implicit way to authenticate the user is to use graphical passwords in multifactor authentication systems. It makes the secret easier to remember and the entire process fast and more secure as graphical passwords are by default resistant to multiple attacks like shoulder surfing, guessing, dictionary attacks, etc. Effective graphical passwords can be created using multiple elements like grids, patterns, images, colors, etc[3,4,5,6,7]. Even parts of an image can be selected to verify the user[4].

III. Methodology

The authentication system has three phases: registration, login and verification. In the Registration phase, the user has to create an account, enter contact details and create a pattern. In the second phase, the user has to use credentials to log in and in the third phase, the user has to verify the OTP and graphical challenge.

A. *Username-Password:*

The first factor of the three-factor authentication system is username-password. It is the most commonly used method for login. In the registration phase, the user has to create a strong password with a minimum length of 8 having a combination of alphanumeric characters.

In the login phase, the user need to log in using the credentials created in the previous phase. If the credentials are valid then the user will be reddirected towards the next phase. Else the user can use the forgot password option. The user will get only three incorrect attempts before getting a cooldown.

B. *OTP*

OTP falls into the 'something you have' category of authentication methods. After the successful completion of the first factor, the user is authenticated using a randomly generated password sent to the user by email or SMS.

At the time of registration, the user has to provide at least an email address. The user can also add multiple phone numbers and email addresses to get OTP delivered. While logging in, the user will get to choose the delivery method for the OTP. The server will then generate a random 6-digit password and send it to the chosen email-id or phone number. After successful verification of the OTP, the user will be redirected to the graphical password challenge.

C. *Graphical authentication method*

The new graphical authentication method is a knowledge-based authentication method. In this method the user has to create a secret and remember it, which gets verified by solving a challenge at the time of login.

While registering in the first phase, the user creates a pattern of minimum length of 4 in a 4x4 grid. At the time of logging in the user will get a challenge. The challenge will have a 4x4 grid of images with 6 randomly selected images. The user has to select the images which are lying on the pattern created by the user. After verifying the selections, the user will get logged in or access denied. The user will have maximum three choices to complete the challenge before getting locked out.

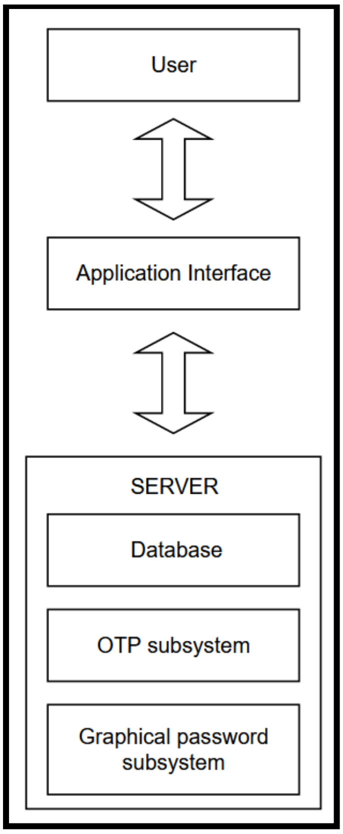


Fig 1. Block diagram

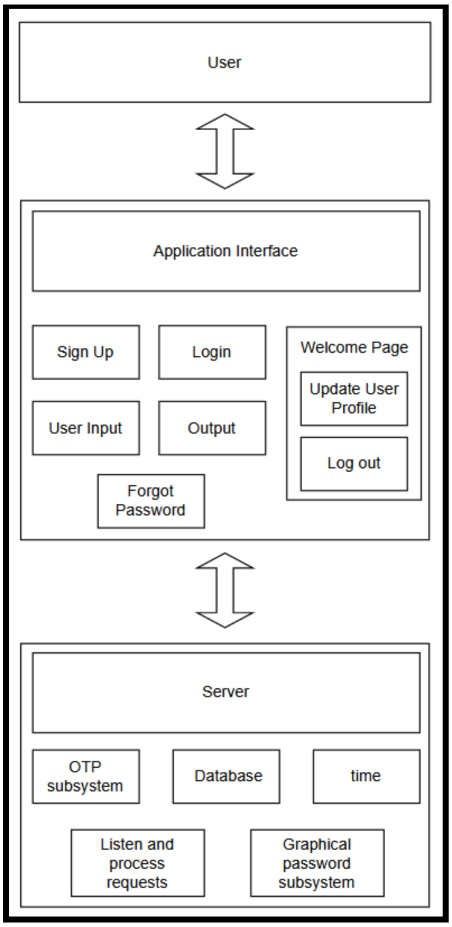


Fig 2. Architecture diagram

IV. Implementation

The proposed system was implemented using Django in the backend with sqlite3 as a database. Pythonanywhere to host web applications with let's encrypt SSL certificates for https. It's currently on trial basis on Pythonanywhere available with limited resource server in free tire. The system is accessible from any type of web browser either android or laptops.

Additional features to harden the security of application:

1) Limiting number of attempts:

For the first and second factor which is password and OTP, the number of attempts is three if the user cannot get the correct password in three attempts he gets locked out for a certain duration.

2) Informing user of attempted logins:

If multiple unsuccessful attempts are made to log into the system, the user will be informed of the incident and further actions can be taken.

3) Limiting time for user sessions:

Specifying the time for which user session validity. After the user will be forced to authenticate again. It prevents threats from cookie attacks and unauthorized use of sessions.

V. Evaluation

No single authentication method is completely secure or can stop every attack. Even though graphical password provides better security compared to text-based passwords, there are still potential threats. Below, the probability and potential time required to crack each password is calculated:

A. First factor implementation:

For a text password, length is the most important factor along with special characters used in passwords. For example, a 10-character long password with two special characters takes about 23 years and 11 months while a 10-character password with only alphabets takes 13 hours and 48 minutes**.

B. Second factor implementation:

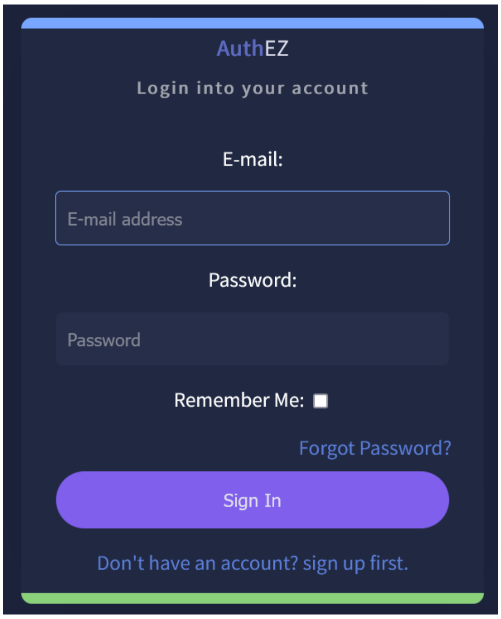
The system is using a 6-digit OTP, with 3 attempts, the probability of guessing the OTP is: 3/10^6 i.e., 0.000003%. Also, every OTP is valid for only 60 seconds which makes it impossible to perform guessing attack on the system.

C. Third factor implementation:

For the graphical password a 4x4 grid with pattern length of 4 is used. For every challenge there are 6 options and 2 are correct therefore the probability of guessing correct password is 1/15 i.e., 6.667%***. For this method too there are only three attempts available again making it impossible to guess.

This data proves that even if the first and second factors of authentication are compromised, there is 93.333% chance to prevent unauthorized access to the system.

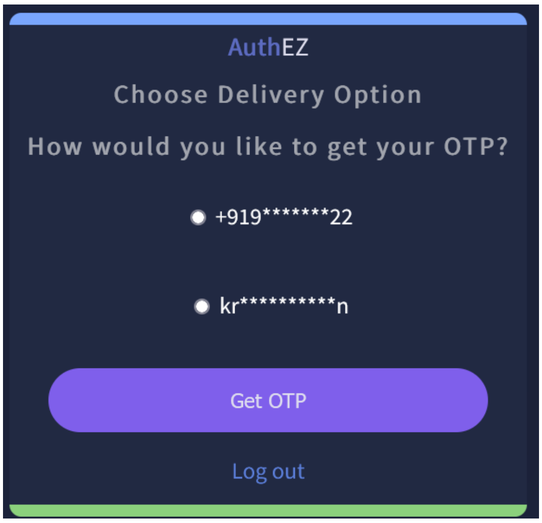
VI. Result and Discussion



AuthEZ

Login into your account

Fig. 3. First Factor (Username-Password)

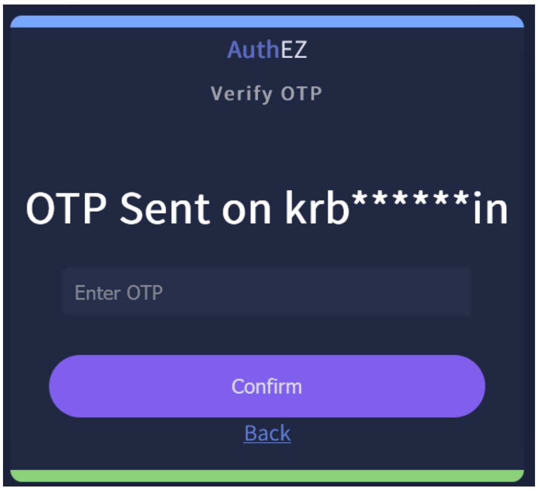


AuthEZ

Choose Delivery Option

How would you like to get your OTP?

Fig. 4. Second Factor (Get OTP)



AuthEZ

Verify OTP

OTP Sent on krb******in

** data for this is calculated on https://random-ize.com/how-long-to-hack-pass/ this.
*** data depends on construction of challenges.

Fig. 5. Second Factor (Verify OTP)

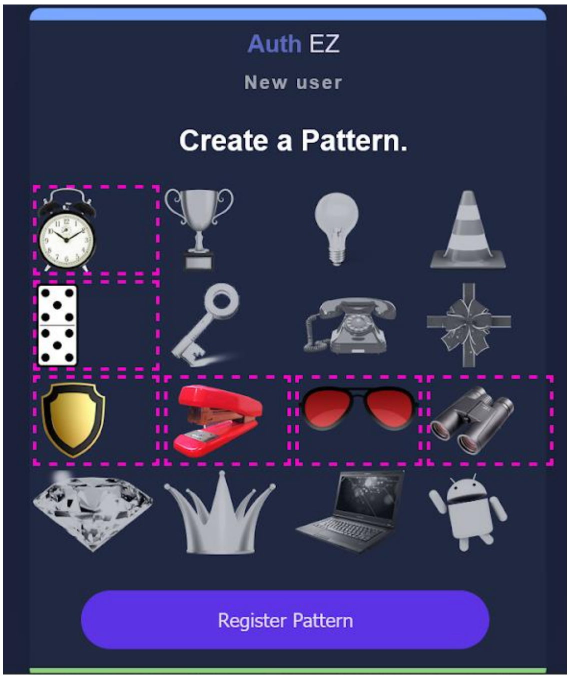


Fig. 6. Third Factor (Registering the pattern)

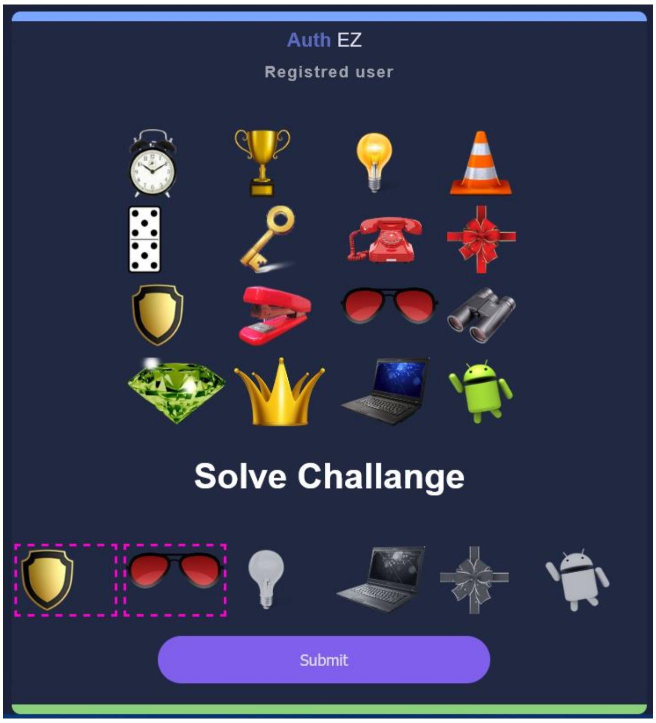


Fig. 7. Third Factor (Solving the challenge)

The present graphical schemes are lagging one aspect between security, quickness or easiness. Some graphical schemes are quick but not secure, some schemes are secure but not quick or easy to use. It is hard to find a graphical scheme which is quick, secure as well as easy to use.

The implemented image grid password scheme has following perks over other graphical schemes :-

1) It is based on implicit framework and resistant against shoulder surfing attacks.

2) It is quick, reliable and has high success rate against guessing attacks.

3) It has simple learning curve even for non-technical users.

Table 1 [8], below shows the security features and resistance of graphical authentication methods against various attack vectors.

	Attacks						Security features	
Graphical Password Schemes	Brute Force	Spyware	Guessing	Shoulder Surfing	Dictionary Attack	Social	Large Password Pool	Limited Login Try
Déjà Vu	N	Y	N	N	Y	N		
Triangle	N	X	N	Y	Y	Y	/	
Moveable Frame	N	Y	X	Y	N	X	/	
Intersection	N	X	N	Y	Y	X	/	
Picture Password	N	N	X	N	X	X		
Man et al.	X	X	X	Y	X	X	/	
Takada and Koike	X	X	X	N	X	X	/	
Story	N	X	N	N	X	X		
Passfaces	X	X	N	N	X	X		
Weinshall	X	Y	X	N	Y	Y		
ColorLogin	X	Y	X	Y	X	X		
GUABRR	Y	Y	Y	Y	Y	X		
Jetafida	X	X	N	N	X	X		/
ImagePass	X	Y	Y	x	X	X		
Wang et al.	X	Y	X	x	X	X	/	
TwoStep	Y	X	X	X	X	X		
Dynamic Block-style	Y	X	X	Y	X	X	/	/
Image Grid Password	N	N	N	N	N	X	/	/

Table 1. Possible attacks on graphical passwords and features of graphical authentication methods.

Y: Resistant, N: Non-Resistant, X: Not Researched, /:Yes

VII. Conclusion

Hence, graphical password as a third factor increases security of the system without adding extra burden on user of remembering complex passwords or procedures. In addition, the implemented graphical scheme is resistant towards shoulder surfing attacks and is based on implicit framework.

This implementation of three factor authentication has simple learning curve for non-technical users. Also, compared to other available graphical password schemes , it is quick and reliable.

The implemented graphical scheme has 93% success rate against guessing attacks.

In future, a graphical scheme can be created based on current system by having a larger grid to reduce the probability of guessing attacks. The success rate can be increased up to 98% .

Acknowledgement

We would like to express our sincere gratitude to Dean of Computer Engineering Department, MIT Academy of Engineering for providing us the infrastructure and support to complete this work.

References

[1] 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

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

[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] 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.

[5] 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

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

[7] 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

[8] Robert G. Rittenhouse, Junaid Ahsenali Chaudry, Malrey Lee, "Security in Graphical Authentication", in International Journal of Security and Its Applications Vol. 7, No. 3, May, 2013