

Implementing Biometric or Graphical Password Authentication in a Universal Three-Factor Authentication System

Mohammad Naveed Hossain
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
naveedhossain99@gmail.com

Sheikh Fahim Uz Zaman
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sheikh.fahim.zaman@gmail.com

Tazria Zerin Khan
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
tazria.zerin.khan@g.bracu.ac.bd

Sumiaya Azad Katha
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sumiaya.azad.katha@g.bracu.ac.bd

Md. Tawhid Anwar
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
write2tawhid@gmail.com

Muhammad Iqbal Hossain
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
iqbal.hossain@bracu.ac.bd

Abstract—There are three critical aspects of cyber security: authentication, safety, and secrecy. Consumers have access to a wide range of alternatives for improving the safety of password-based login systems. With two-factor authentication, the majority of this was done. Two-factor authentication combines single-factor authentication processes. Two-factor authentication is becoming increasingly common and widely accepted in today's technological age due to the growing need for privacy and security. Customized security measures are more effective and bought if they are easy to use and implement. For increased website and mobile app security, this study examines the consequences of using a three-factor authentication scheme. This post will present an app we built that might provide a good three-factor authentication approach without losing the convenience.

Index Terms—OTP, Authentication, 2FA, 3FA, Hacked, Bio-Metric, alphanumeric password, data protection, network security, three-factor authentication.;

I. INTRODUCTION

The Information Technology sector is getting advanced day by day. People nowadays use the IT sector as part and parcel of their life. As every coin has two sides, people get what they need from this sector. Also, people are getting into trouble because of the vulnerability in the security of this sector. Single-factor authentication cannot keep up with security breaches. Hence, people started to get along with Two-factor authentication, which is not enough to ensure better security [1]. The two-factor authentication uses a physical token that is easily accessible to unauthorized people. An OTP (One Time Password) is sent to the user in Two-Factor Authentication. An unauthorized person can easily intercept it. Other than that, social engineering attacks, password-guessing attacks, sim cloning, and phishing attacks are expected for the Two-Factor Authentication [2]. So, to ensure the best security possible, Three-factor authentication and Three-Factor Authentication

are introduced, which contain an extra layer of protection with bio-metrics, which the user sometimes possesses. Bio-metric is not possible to use on every device. This paper introduced a pattern recognition system to make the system usable for all graphical passwords. So due to these multiple layers of security, it gets more complicated for the unauthorized person to get logged in with the correct credentials of the user. The main goal of Three-Factor Authentication is to increase the security of the whole system and make things complicated for the unauthorized person to figure out the correct credentials of the user [3].

II. EXISTING AUTHENTICATION METHOD

A. Related Works

As part of an attempt to boost network security, Li et al. proposed using biometrics as one of three authentication elements in a three-factor authentication system [4]. A three-factor authentication system that includes the usage of a password, a smart card, and biometrics is proposed here. As a result of this idea, the evolution of current technology and an in-depth investigation into the downsides of fewer security measures prompted the use of facial recognition as a component of this software. The argument over biometric authentication's speed and flow has substantially influenced this study compared to other authentication aspects. As a starting point, the proposed approach was capable of withstanding various attacks and preserving the hosts' multimedia and web resources. Users can benefit from multifactor authentication, but it can also be problematic when apps seek to supply credentials to autonomous software processes. An attack vector is opened up when credential permissions are provided to independent software processes. For a more secure system, background processes should not be issued credentials. According to this

research, they should not have been granted in the first place [5]. "Two-factor authentication is the cornerstone of even the most rudimentary cybersecurity program," says HCPPro in its two-factor authentication: cybersecurity for today's world. The primary emphasis of this paper's discussion and analysis was evaluating convenience and speed above security [6]. Making the procedure as seamless as possible while linking various processes with the fewest possible clicks is the relevance of this study for my ongoing research and development.

B. Steps of Existing Authentication Method

Two-Factor authentication is the most common authentication system currently. Two-Factor Authentication is presently used by Google, Facebook, Apple, and many banking websites and applications. Two-Factor authentication starts with a basic logging system, the One-Factor Authentication, which is an only email address or username and password. after successfully entering the email address and password an OTP will be sent to the user's phone number. The phone number will be asked by the system from the user during the registration period. After receiving the OTP, the user has to enter the password into the system to log in successfully. The double-layered security is assumed as safe and adaptive.

C. Security and Privacy Issues with One-Factor Authentication

Single-factor or one-factor authentication is rare in social and banking software or websites. Once upon a time, it was much more popular and used in every place. Day by day, its helpfulness decreased cause it can be hacked in many ways. The most common forms are Phishing, Social Engineering, Malware, Shoulder Surfing, etc. In Phishing, a malicious link has been sent to the user. If the user visits the connection and provides the asked data in the relation, it will directly go to the hacker. By using that information, the user can hack the account quickly. In the case of Social Engineering, the hacker calls the user as a technical support agent and assists the user in service; during the service, the hacker takes all the necessary information requires to hack the user. Once upon a time, a UK-based company's CEO lost 201,000 euros to the hacker by this social engineering. Malware is the most common hacking method. Malicious files are continuously given to the user to the user's private data. Last but not least, shoulder surfing is also a reason for hacking; nearby people can see or guess the username and password later used to hack the system. In this way, single-factor authentication can be hacked [7].

D. Security and Privacy Issues with Two-Factor Authentication

Two-Factor authentication is the most popular security method in our daily life. But day by day, it is getting older and older. As it gets colder, the way to hack it is becoming much more accessible. It can be hacked by SMS-based man in the middle attacks, supply chain attacks, pass the cookie attacks, server-side forgeries, etc. In an SMS-based man in the middle attack, the hacker stays in the middle and convinces



Fig. 1. General Two-Factor Authentication. [10]

Method	Percentage
One-Factor	21%
Two-Factor	72%

TABLE I
PERCENTAGES OF PEOPLE USING 2FA AND 1FA.

[11]

the server to the user. Another hand, he convinces the user as the server using different unethical techniques. In this way, hackers can hack the two factors. Passing the cookie is done initially for user convenience so that users can stay signed into their applications [8]. A hacker can take over your account if they can extract that info. These are a few examples of two-factor authentication. It has many other nonpopular ways [9].

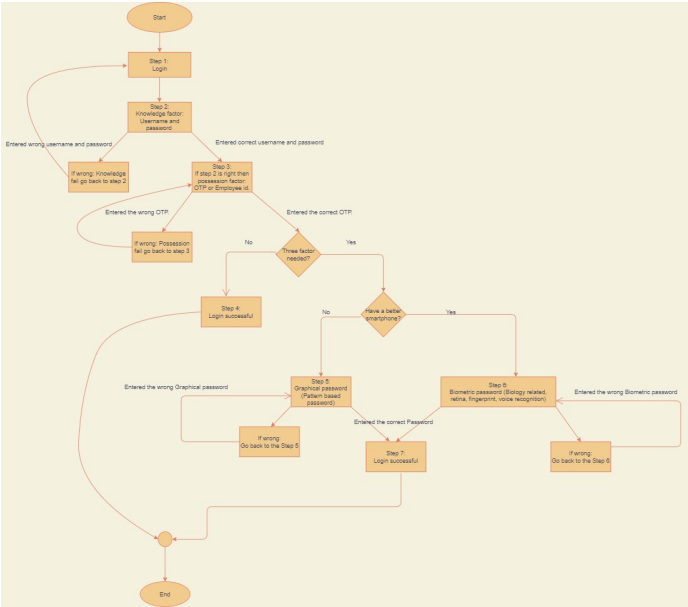


Fig. 2. Flowchart of the model

III. PROPOSED MODEL

A. Overall Approach of Proposed Model

Three-factor authentication works step by step. Mainly it is a 5-step process.

1. In step 1 user has to log in with a username and password. The user has to enter a valid username and a strong password.
2. In step 2, the verification will be started. The system will match the username and the password with the database. This step is known as the possession factor. If the username and the password match the database, the system will forward to step-3. If the user enters the wrong username or password, the system will loop to step-1 again and ask the user to correctly enter the username and password .
3. In step 3, the second step verification will be started, known as the possession factor. In this step, OTP or a similar kind of employee id will be used to verify. In an OTP system, the user will receive a 4-to-6-digit pin in their personal phone number. If they fail to enter the pin number correctly, it will be looped to step 3 again will ask for the new OTP.
4. Then, the user will get the open platform if the user selects the three-factor authentication. If If the user is not interested in three-factor authentication, then the sequence will be ended, and the user can login at step 4 from the second time when will they use.
5. If the user selects three-factor authentication, two options will be available. If the users have a well-featured smartphone, they can choose the Bio-metric password; otherwise, they can use the Graphical password. If the user selects the Graphical password, steps 1,2, and 3 will work in the same pattern step 5 will be the new step. If the user enters the Graphical password correctly, it will go to step 7. The user can log in successfully; otherwise, it will go step 5 again and ask the user to reenter the Graphical password again. If the user selects a bio-metric password, steps 1,2 and 3 will work in the same pattern step 6 will be newly added. If the user gives a correct bio-metric password, it will move on to step 7, and the login will be successful; otherwise, it will go back to step 6 and ask the user to enter the password again. By following the above five steps, users can have a secure login with three-factor authentication.

B. Proposed Model Implementation

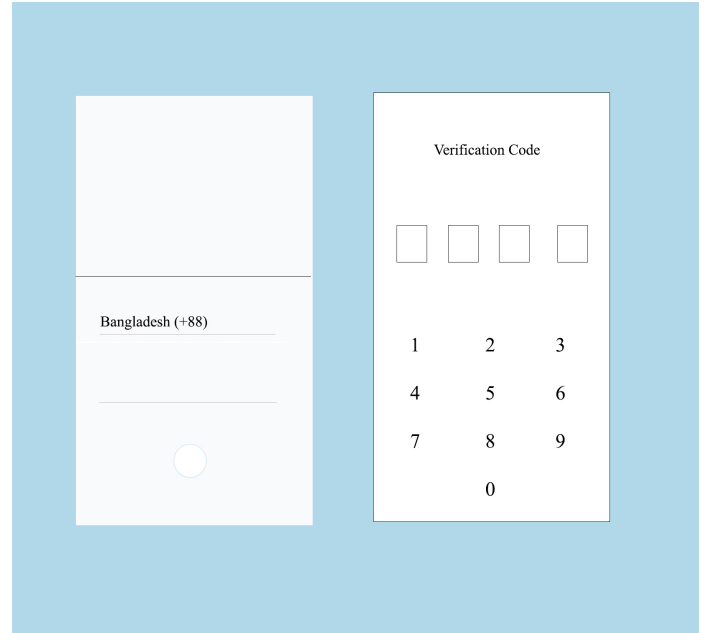


The image shows a login module interface with a blue background. It contains two input fields: 'Username :' with the value 'teamprethesistwo@gmail.com' and 'Password :' with the value '*****'. Below these fields is a 'Submit' button.

Fig. 3. Login Module

1) *Login Page:* In the first stage, there will be a regular login page. On that page, there will be a username and password. If a user enters the correct username, name, and password, the

first stage of our authentication will be successful. If the user enters the wrong username or password, it will stay on the same page and ask for a correction. After correction, it will move to the next stage, the OTP sender stage. [2]



The image shows an OTP sender interface with a light blue background. It contains a 'Verification Code' input field with four empty boxes for digits. Below this is a numeric keypad with digits 1 through 9 and 0.

Fig. 4. Sending OTP

2) *OTP sender:* The second stage of authentication is the OTP sender. If our first step of authentication is successful, it will move on to the OTP stage, and a four-digit pin will be sent to the user's phone number. Then the user has to enter the nail in the correct place; then, it will move to the third step of authentication if the user selects the third factor. Otherwise, it will stop here, and the user can successfully log in via two-factor authentication.

3) *Bio-Metric:* If the users have a better-quality smart-phone, then they can choose bio-metric as their third-factor authentication. Mainly when the user registers his/her account, they will provide their fingerprint. Those fingers print will be updated on the database. Later, it will be used in further authentication. In the place of fingerprints, many other ways can be implemented as well, like voice recognition, iris scan, and face recognition. But they are few loops whole in those processes. In voice recognition, a false user can record the genuine user's voice and easily break the third factor [12]. In the case of iris scan, it requires a lot of cost user won't show much interest in this feature. In the case of face recognition, sometimes the sensor fails to identify the real user when the wear spectacles or wear makeup [13]. From the above situations, we made a conclusion that fingerprint scan will be the most preferable among the rest of the procedures. There will be two fingers fingerprints. For example, the right-hand thump and the left-hand thump. If the user sets the right hand's thump as the bio-metric option, the left-hand thump's fingerprint will be automatically set as an emergency backup. If a user gets kidnapped and the kidnapper wants to steal the

user's personal data, the user will put the left-hand thumb's fingerprint in the sensor, which will instantly block any type of transaction for a certain amount of time and immediately sends the current location of the user to the bank or user's close one and if they find anything suspicious they will contact the police [14].

4) *Graphical Password*: Mainly graphical password is an optional authentication process in our system. The user does not have the option of a fingerprint scanner on the phone or on a laptop. A graphical password is a randomly generated graphic pattern. In our example, we are showing this using a fruit pattern given in Figure 5.

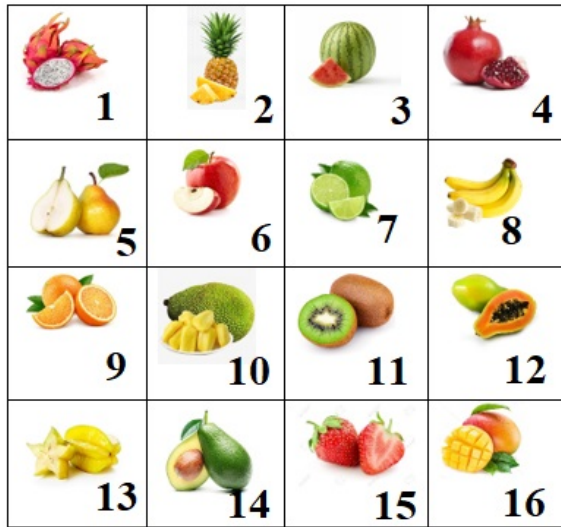


Fig. 5. Initial pattern of Graphical Password

If a user selects the sequence Dragon Fruit → Apple → Kiwi → Jack Fruit. According to Figure 5, the box number is 1→6→11→10. So the user has to swipe through 1→6→11→10. Like figure 6. From the next time when will the user reaches to graphical password, the pattern Dragon Fruit → Apple → Kiwi → Jack Fruit will remain as the privacy pattern, but the order will be changed. Which is shown in Figure 7. From figure 7, we can see when the user reaches to graphical password, the next time the user might see the random pattern few examples can be Random Pattern 1, Random Pattern 2, Random Pattern 3, and so on. There will be no fixed pattern every time. Users have to find the fruits that they have chosen and swipe accordingly. To successfully login in, the users have to put Dragon Fruit → Apple → Kiwi → Jack Fruit in the correct order. The correct form is shown in figure 8 [15] [16].

Just need to keep the fruits order the same as the initial one no need to think about the box order. The user can set the backup pattern as well. If the users face any emergency, they can draw this pattern, and an emergency notification will

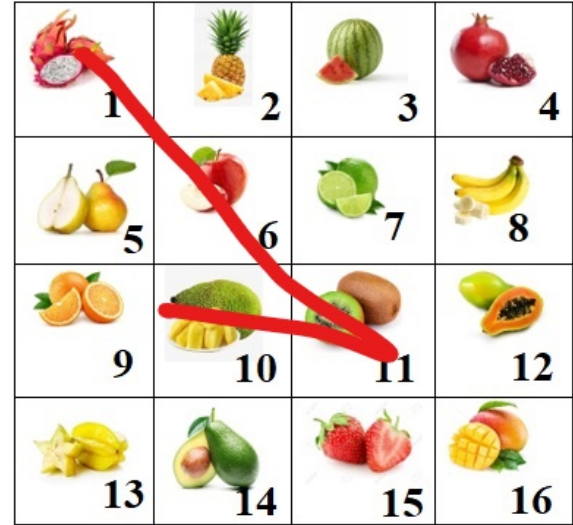


Fig. 6. Unlocking pattern

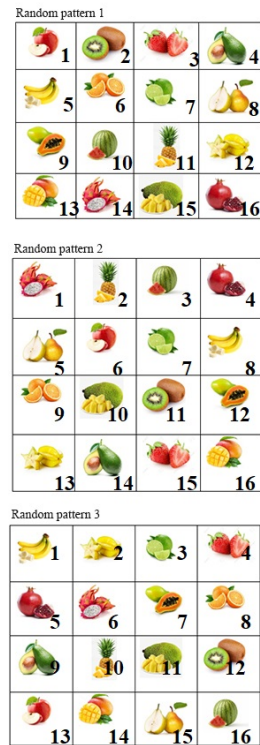


Fig. 7. Random Pattern

be sent to the user's relative or user bank, depending on the system settings.

IV. RESULT ANALYSIS

For single-factor authentication, the password can be hacked in a limited amount of time. The complexity of the single

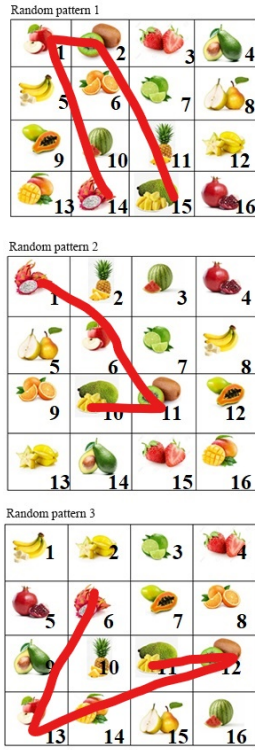


Fig. 8. Correct Order for Graphical Password Example

factor is around $T = 2 \times \log_2[A^N / (10^9 \times 3600)]$ where A is the list of the total number of valid characters, and N is the size of the password. For two-factor authentication the complexity is $T = 2 \times \log_2[A^N / (10^9 \times 3600)]$ and $O(A \text{ XNOR } B)$ for the XNOR gate and $O(A.B)$ for the AND gate. Total complexity, $T = 2 \times \log_2[A^N / (10^9 \times 3600)] + O(A \text{ XNOR } B) + (A.B)$ even after having complex method to be hacked, two factor authentication is getting hacked it is taking a extra time but it is possible. In other existing three-factor authentication cases, they use the secret question, pattern lock system, pin system, etc. Secret question and pin system have complexity similar to a password, the 3X3 pattern lock system has a complexity of $9P3 = 504$, and the 4x4 pattern system has a complexity of 43680, which is possible to be hacked within an hour. In our proposed model it will ensure $T = 2 \times \log_2[A^N / (10^9 \times 3600)] + O(A \text{ XNOR } B) + (A.B)$ along with $O(i, j) = 0.5 * \tan^{-1} * (V_y(i, j) / V_x(i, j))$ for Bio-metric password, where V_y is Horizontal complexity of the bio-metric matrix and V_x is Vertical complexity of the bio-metric matrix and i,j is number of rows and columns. For the graphical password the complexity is $T = 2 \times \log_2[A^N / (10^9 \times 3600)] + O(A \text{ XNOR } B) + (A.B) + 16P4 * 16^2$ as we are considering 4x4 pattern. Both graphical password and bio-metric factors mathematically ensure more security to the data other than the existing method.

As our proposed model has some advantages, on the other hand, it has some disadvantages also. Using bio-metric passwords is almost impossible to use on personal computers

and button phones and is rarely used cheaper on laptops. Mainly our system is much more efficient in smartphones and expensive new model laptops.

V. CONCLUSION AND FUTURE WORK

The advancement invalidation technique has to look into the authentication inequalities in the coming times, not for the present time. At this moment, one needs to invest more to get a superior security standard. Preserving the standard of security will be difficult day by day. It is getting tough to protect the security protocol. Sometimes password databases can be easily dictionary-attacked because some challenges can be estimated and quickly predicted, like reformation in computation. On the other hand, some challenges are hard to predict, such as the exposure of new "day-zero" vulnerabilities in the software being used. Subsequently, security preconditions are not modified yet increment with time. As a result, three-factor authentication can be an excellent solution to the security problem. Integrated three-factor authentication gives the best expediency for better security. Moreover, it provides multiple options according to users' abilities and preferences. So, 3FA can be applicable in many applications. For example, online banking systems, online shopping systems, online money transactions, and many other applications. 3FA has two options for users in their third authentication step. If a user has a good quality smartphone and cost is not an issue for him, the user can easily use a bio-metric password as the third authentication for security purposes. It can be biology-related, retina, fingerprint, or voice recognition. But if any user has cost issues or if he does not have a good smartphone but the user wants more security, it can also be solved by 3FA. Instead of bio-metric, they can choose a graphical password as the third authentication. It will be a pattern-based password. So, the cost problem can be easily solved by giving 2 options to the customers two options in three-factor authentication. It is user-friendly, and user can easily choose their type of authentication. Through this process, our database will be much more secure [17].

As we previously discussed, our system is much more efficient in smartphones and expensive new model laptops. Our target should be to make it more efficient for all types of devices and all category people. We wanted to implement this model practically with companies like IBM and SOPHOS. As 2FA has various kinds of security breaches discussed above so 3FA has strong security that can fix this security breach. Also, we want to make an app to offer to the companies for their testing purpose. Moreover, we will start a beta testing phase for the app to understand how the people are using it or getting used to the new 3FA. Furthermore, there could arise some problems related to the graphical password section. There is a lot to improve about the space and time complexity of the whole model when it is implemented practically [18].

VI. ACKNOWLEDGEMENT

This research is supported by Brac University, Dhaka, Bangladesh.

REFERENCES

- [1] Abraham Bookstein, Vladimir A Kulyukin, and Timo Raita. Generalized hamming distance. *Information Retrieval*, 5(4):353–375, 2002
- [2] T. T. Contributor. three-factor authentication (3fa). retrieved from tech. 11 2014.
- [3] G Barrow. What’s wrong with two-factor authentication? retrieved from security.11 2020
- [4] Aspen Olmsted. Three factor authentication.
- [5] Rossow C. Dmitrienko A., Liebchen C. On the (in)security of mobile two-factor authentication. 2014
- [6] NevonProjects. Smart android graphical password strategy. 2018
- [7] su-Yang Wu. A provably secure three-factor authentication protocol for wireless sensor networks. pages 15–17, 2021.
- [8] Mohammad S Jalali, Bethany Russell, Sabina Razak, and William J Gordon. Ears to cyber incidents in health care. *Journal of the American Medical Informatics Association*, 26(1):81–90, 2019.
- [9] Geeks for Geeks. How to add fingerprint authentication in your android app. 2021.
- [10] ADEO. Why you should activate two-factor authentication. 2020
- [11] Dan Kobialka. Duo security 2fa research findings.
- [12] Jean-Paul Delahaye. The mathematics of (hacking) passwords. In *The science and art of password setting and cracking continues to evolve, as does the war between password users and abusers*, 2019
- [13] A Kurniawan. Easy ways to implement automatic sms verification in android. 04 2020.
- [14] K. Garska. Why sms 2-step verification won’t keep you safe. 09 2017.
- [15] Nemanja Maćek, Sran Barzut, and Saša Adamović. A novel fingerprint biometric cryptosystem based on convolutional neural networks. 9(7):730, 2021.
- [16] Mr.Jadhav Rajesh S., Chandole Durgesh K., and Mr.Wani Milind D. Graphical password authentication system. *Graphical Password Authentication System*, 3(4):353–375, 2014.
- [17] Research India. A three-factor authentication scheme in atm. 2018
- [18] Soumitra Sudip Bhuyan, Umar Y Kabir, Jessica M Escareno, Kenya Ector, Sandeep Palakodeti, David Wyant, Sajeesh Kumar, Marian Levy, Satish Kedia, Dipankar Dasgupta, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, 44(5):1–9, 2020.