

# A Generic Framework of Three Factor Authentication with Optional Bio-metric or Graphical Password

by

**Mohammad Naveed Hossain**

17201018

**Sheikh Fahim Uz Zaman**

18101597

**Tazria Zerine Khan**

18101477

**Sumaiya Azad Katha**

18101447

A thesis submitted to the Department of Computer Science and Engineering  
in partial fulfillment of the requirements for the degree of  
B.Sc. in Computer Science

Department of Computer Science and Engineering  
Brac University  
January 2022

© 2022 BRAC University  
All Rights Reserved.

# Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

## Student's Full Name & Signature:

---

Mohammad Naveed Hossain  
17201018

---

Sheikh Fahim Uz Zaman  
18101597

---

Tazria Zerine Khan  
18101477

---

Sumaiya Azad Katha  
18101447

# Approval

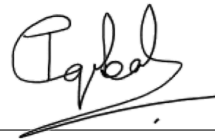
The thesis/project titled “A generic framework of 3FA authentication with optional bio-metric or graphical password” submitted by

1. Mohammad Naveed Hossain (17201018)
2. Sheikh Fahim Uz Zaman (18101597)
3. Tazria Zerine Khan (18101477)
4. Sumaiya Azad Katha (18101447)

Of Fall, 2021 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January, 2022.

## Examining Committee:

Supervisor:



---

Dr. Muhammad Iqbal Hossain  
Assistant Professor  
Computer Science and Engineering  
BRAC University

Co-supervisor:



---

Md. Tawhid Anwar  
Lecturer  
Computer Science and Engineering  
BRAC University

Program Coordinator:  
(Member)

---

Md. Golam Rabiul Alam  
Assistant Professor  
Computer Science and Engineering  
BRAC University

Head of Department:  
(Chair)

---

Sadia Hamid Kazi  
Chairperson and Associate Professor  
Computer Science and Engineering  
BRAC University

## Abstract

We live in a technological era where technology controls our lives in a good way or in a bad way. In today's digital world we cannot imagine a single day without technology and for security for purposes we mostly rely on single-factor authentication or two factor authentication. While using two factor authentication (2FA) our data can still be hacked. 2FA has some weaknesses and for That is the reason our password can be easily cracked or hacked by hackers, even when hackers do not have our OTP. To solve this weakness and make our data more secure and reliable we use three factor authentication so that any unauthorized person cannot easily access our data. We use 5 steps with 3 authentications. First one is username and password after verification, second one is OTP and if both are verified, the last and third one is bio-metric such as fingerprint, voice recognition etc. but not every device supports the bio-metric system for those devices graphical password can be used. Through these three authentications we can protect our data, make it secure and trustworthy for every user.

**Keywords:** OTP; Authentication; 2FA; Hacked; Bio-Metric;

## **Acknowledgement**

All gratitude is due to Almighty Allah, Most Gracious, Most Merciful, who has provided us with the opportunity to study at BRAC University.

Secondly, I would like to acknowledge and give my warmest thanks to our supervisor Dr. Muhammad Iqbal Hossain and Co-supervisor Tawhid Anwar for the continuous support, motivation, enthusiasm and immense knowledge. Their guidance helped us in all the time of research and writing of this thesis.

Besides my supervisor and co-supervisor, I would like to thank the rest of my thesis group members(Mohammad Naveed Hossain, Sheikh Fahim Uz Zaman, Tazria Zerin Khan, Sumaiya Azad Katha) for their encouragement, insightful comments.

Last but not the least we would also want extend our appreciation to those who could not be mentioned here but well played their role to inspire the team.

# Table of Contents

Declaration	i
Approval	ii
Ethics Statement	iv
Abstract	iv
Acknowledgment	v
Table of Contents	vi
List of Figures	viii
Nomenclature	viii
<b>1 Overview</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Research Problem . . . . .	1
1.3 Research Objective . . . . .	2
1.4 Thesis Structure . . . . .	2
<b>2 Related Work</b>	<b>3</b>
<b>3 Proposed Model</b>	<b>8</b>
3.1 Overall Approach of Proposed Model . . . . .	8
3.2 Preliminary development . . . . .	9
3.2.1 Coding Part . . . . .	9
<b>4 Implementation</b>	<b>16</b>
4.1 Login Page . . . . .	16
4.2 OTP sender . . . . .	16
4.3 Graphical password . . . . .	16
4.4 Bio-Metric . . . . .	17
<b>5 Results</b>	<b>19</b>
5.1 Password . . . . .	19
5.2 OTP . . . . .	20
5.3 Bio-Metric System . . . . .	22
5.3.1 Horizontal and Vertical Complexity . . . . .	22

5.3.2	Hamming Distance . . . . .	23
5.4	Graphical Password . . . . .	24
<b>6</b>	<b>Conclusion and Future Work</b>	<b>29</b>
6.1	Conclusion . . . . .	29
6.2	Future Works . . . . .	29
	<b>Bibliography</b>	<b>32</b>



# List of Figures

3.1	Flowchart of proposed model . . . . .	10
3.2	Detailed Flowchart of Login Phase . . . . .	11
3.3	Detailed Flowchart of OTP Phase . . . . .	11
3.4	Detailed Flowchart of 3FA . . . . .	12
3.5	Workflow of OTP Authentication code . . . . .	13
3.6	Workflow of Graphical Password Code. . . . .	14
3.7	Workflow of Fingerprint Authentication . . . . .	15
4.1	Login page . . . . .	16
4.2	OTP sender . . . . .	17
4.3	Graphical password . . . . .	18
5.1	Password Breaking Time . . . . .	20
5.2	OTP Working Process . . . . .	21
5.3	XNOR Truth Table . . . . .	21
5.4	AND Truth Table . . . . .	21
5.5	Sample Matrix . . . . .	22
5.6	Horizontal and Vertical Complexity Calculation . . . . .	23
5.7	Hamming Distance . . . . .	24
5.8	PCCP (Persuasive cued click point) . . . . .	27

# Chapter 1

## Overview

### 1.1 Introduction

The Information Technology sector is getting advanced day by day. People nowadays use the IT sector as a part and parcel of their life. As every coin has two sides people are getting what they need from this sector and also people are getting into trouble because of the vulnerability in the security of this sector. Single factor authentication is not able to keep up with the security breaches so people started to get along with the Two factor authentication which is also not enough to make sure better security. The two-factor authentication uses a physical token which is easily accessible to the unauthorized person. As an OTP is sent to the user in 2FA it can be easily intercepted by the unauthorized person. Other than that social engineering attacks, password-guessing attacks, sim cloning and phishing attacks are common for the 2FA. So, to ensure the best security possible Three factor authentication 3FA is introduced which contains an extra layer of security with biometrics which is something the user possesses sometimes bio-metric is not possible to use in every devices for making the system usable for all graphical password a pattern recognition system has been introduced in this paper . So due to this 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 3FA 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.

### 1.2 Research Problem

2 factor authentication was first introduced on July 4, 1986. In 2011 google and Facebook started using this two factors authentication in their software. At present these 2-factor authentication in the communication-based software has become a very common and old method. As this method has become much more common and outdated, hacking has become much easier nowadays. Software that requires a lot of security, such as software that contains personal information or money transactions, etc. There are many loopholes in these 2-factor authentication, as a result of which a lot of necessary information is insecure. This 2-factor authentication can be hacked in several ways. (SMS-based man-in-the-middle attacks, Supply chain attacks, Compromised MFA authentication workflow bypass, Pass-the-cookie attacks, Server-side forgeries). According to "PCIGURU" 2 factor authentication is 97-98%

secure on the other hand 3 factor authentication is 99.9% secure. Now let's see how we will do 3 factor authentication - for this 3-factor authentication we have first arranged keeping in mind the convenience of the user. For the 3rd authentication, we have the option of biometric, graphical password, we have not kept the option of any kind of password or secret question-answer because if a hacker can hack the password in the 2nd authentication step, he can do it 3rd time. Similarly, in case of secret question-answer, if someone known to the user wants to hack, the hacker can easily guess, so 3 factor authentication will not be effective. On the other hand, we will offer these 3-factor authentication optional for the user, for example, if someone thinks his information is confidential and needs more security then he can use it. Now let's see how this 3rd factor will work - in case of biometric user He will be able to do 3rd factor authentication using his phone and if his camera is not good then he will select the option of graphical password. This graphical password will choose any 3 fruits, flowers or pet from any of the user's favorite things like fruit, flower or pet etc. which will be randomly generated every time because once someone sees someone's pattern he can easily hack with that pattern. But here since every time 9 options will be generated randomly and it is difficult to hack the sequence of patterns so this method is more secure.[14]

### **1.3 Research Objective**

The goal of our research is to make the data more secure. I want to reduce the tendency of data hacking. The objectives of this research are:

1. To deeply understand the concept of three-factor authentication and how it works.
2. To deeply understand the knowledge factor, possession factor and inference factor.
3. Ensure more security to data.
4. Ensure more privacy to private communication.

### **1.4 Thesis Structure**

In chapter 1 it mainly tries to give a short introduction about the topic, research problem and research objective. Moreover, in chapter 2 a detailed related work is shown. Furthermore, chapter 3 contains a proposed 3-factor authentication model with proper procedure, primary development process and also contains some flowchart regarding the proposed model. Also, chapter 4 contains an implemented idea with proper explanation. On top of that, chapter 5 contains the results of each step. Lastly, chapter 6 the conclusion and future works related to this field.

# Chapter 2

## Related Work

The research paper [2] analyzes and addresses the security in mobile apps and websites, by implementing three-factor authentication. At first, it shows the methods of two factor authentication which is basically the combination of single-factor authentication mechanisms. This paper presents an app that can provide a method for three factor authentication and ensure security of the authentication without any loss of convenience. This paper tries to solve the problem of unauthorized use of resources and databases by proposing a generic framework for three-factor authentication. The survey shows that the framework fulfils all the security requirements for three factor authentication and it has many user-friendly properties. End of the work is to completely distinguish the practical threats on three-factor authentication and create concrete three factor authentication conventions with superior performances.

The research work [5]. “Three-factor authentication (3FA)” shows the importance of three-factor authentication in a security system and shows how multi-factor authentication is important to ensure proper security in different applications. In our modern technology we need to keep our database safe and the security concerns are rising day by day in all areas like different types of industries, banks, health care institutions etc. In recent times, Due to the multiplication of portable gadgets and the increased interaction between versatile applications and web administrations, the verification of clients is more frequent for mobile devices than for desktop clients. In numerous occurrences of multi-factor verification, both a mobile device and a desktop are fundamental and go hand in hand for satisfactory confirmation. Three-factor authentication uses bio-metric and all other authentication methods like password and OTP and increases the reliability of a more secure platform. But there is an issue as three-factor authentication is much more costly than two factor authentication because it uses bio-metric which is costly. Besides that three-factor authentication is hard to ignore as it gives better security.

The research work [11] C.Lakshmi Devasena has proposed an MFA(Multi-factor Authentication) model which is a three-layered approach that is able to ensure the safety of the user. As most of the users have a tendency to use apparent passwords, easily guessable passwords, simple passwords and moreover, the same password is used in multiple accounts. Also, people try to store the password in the system so that they can use it for future use which really puts them into a more hack prone zone. So, in this proposed MFA system for authentication it uses two more diverse factors in addition to the normal authentication which helps to authenticate the

user with more security. The new proposed scheme consisted of an Alphanumeric password, a graphical password and a security question which the user selects and only the user knows the answer to. The scheme mainly works with the First Factor as Alphanumeric password (password that was set by the user while making the account) if the password matches than it moves to the Second Factor that is the Graphical password (such as click points, Pass faces, image and picture-based data) and if it matches than it moves to the Third and Final Factor where the security question set by the user is asked if it matches than there will be successful authentication of user and that user will get logged in to the system. The author didn't use any kind of biometrics for three factor authentication to make the scheme more cost effective and user friendly. She also added some benefits of the scheme as it increased the privacy preservation of the user. Also, it had three layered protections so it increased the depth of security. Other than that, she also highlighted some weaknesses as there are three steps to be followed to login so it's really tough to remember all of the passwords. Also, as it has to store three types of data so the memory management was not that much efficient. Lastly, the author talked about the part as it is three layered so users needed to spend some additional time to get logged in.

The research work [21] Wireless sensor Network (WSN) is composed of sensor nodes that are self-organizing through the application of wireless network technology. It requires higher security but during the transmission data may get exposed. To solve this problem researchers proposed numerous security authentication protocols. The recent scheme that was proposed was by Wu et al. it is a 3FA protocol. But in this paper the authors proposed a model which is better than the 3FA proposed by Wu et al. In this paper the author described how Wu et al.'s Protocol is subject to key compromises such as impersonation attack and temporary information attacks. It also highlighted how the messages passed using Wu et al.'s Protocol can be eavesdropped, intercepted and modified. Moreover, the interceptor can guess the password and identity of a user. Now in the proposed model by the authors they proved the correctness of their scheme using the BAN (Burrows–Abadi–Needham) logic. Also, they used the ProVerif simulation tool to ensure whether their model had any kind of vulnerabilities or not because the ProVerif tool can simulate and return the attack sequence. Furthermore, the authors compared their scheme with Wu et al. protocol and how it failed to provide user anonymity, was more prone to temporary information attack and also violated perfect forward backward security. Lastly, the authors pointed out how their proposed scheme was more efficient and secured compared to the Wu et al. protocol.

The research work [3] shows the authentication which is considered as the primary step of security prerequisite for any framework environment against plausible dangers. This paper introduced an authentication system which is three factor authentication and it has password, user ID, biometric and OTP. This three-factor authentication can be used for bank account transactions which need more security and it is proposed to use Rfid for embedded security, face recognition for biometric security and for password security using GSM. The identity communication person or device information gained by the remote system, in remote authentication schemes. Many proposals have been proposed for improving two factor authentication since Lamport's scheme was introduced. The adversary is modeled, at first during the login and authentication phase, the adversary can tap the communication

channel between user and server and also can take information by using the user's password, fingerprints or by obtaining a smart card but the adversary can not do it at the same phase. Moreover, three-factor authentication is the improvement of two factor authentication. Three factors are smart card, password and biometric. Biometric is introduced for improving the security in remote authentication. The characteristics of biometric is unique and it is suitable for user authentication. Also, it reduces problems in two factor authentication like smart card and password but biometric is not cost effective like password or smart card.

The research work [15] Using oBWNs (On body distant frameworks), the basic physiological information of the steady can be amassed from the wearable sensor centers and gotten to by the approved customer actually like the prosperity capable or the subject matter expert. Open nature of distant correspondence and the affectability of physiological information, secure correspondence has persistently been a critical issue in oBWNs-based structures. The proposed plan gets a one-time hash tie methodology to ensure forward mystery, and the pen name technique is used to supply customer anonymity and face desynchronization attacks. There are four kinds of individuals: enrollment subject matter expert (RA), the customer, entryway center (GWN), and wearable sensor center points. The (RA) might be an outsider who are trusted by oBWN individuals, who is responsible for delivering structure enlistment of the relative multitude of customers, GWN, and wearable sensor center points. The customer, for example, a prosperity capable or the trained professional, can get to the life-basic data of the objective calm and give constant reinforce and intercessions. (GWN), which has tall calculation and correspondence abilities, is the fundamental center individual between the customer and the wearable sensor center points. The wearable sensor centers, cardio sensor, and beat sensor, send around/on the patient's body and gather basic physiological information of the objective patient. Using oBWNs, it is possible to supply the constant and continuous checking of the calm, in any case of the patient's region. The security of the proposed scheme is shown by exhaustive proper check using the Boycott rationale model. Through the heuristic, we have shown that the proposed plan can't as it was giving a couple of spectacular security and utilitarian features, yet also face diverse noxious attacks, for example, desynchronization attack and flexible contraption adversity attack. Contrasted and the cutting-edge designs, the moo calculation and correspondence costs just as tall security make the proposed plan more sensible for distant calm seeing in oBWN.

The research work [10] Security vulnerabilities of conventional single factor authentication have ended up a major concern for security professionals and analysts. Online client nearness expanded impressively within the final decade, where in 2018, 89% grown-ups within the U.S. detailed utilizing the web every day. Such exponential growth in clients and information has justified security professionals to be more concerned with online information security and to control issues Independent of expanded information security, MFA instruments have a few ease-of-use challenges, such as a user's need of inspiration, hazard trade-off understanding, and nearness of non-intuitive client interfacing. Conducting client considerations to supply appropriate hazard arrangement have been demonstrated to be successful in progressing computerized security through adoption. Considerations on the ease of use of verification strategies is frequently underestimated by security specialists. Hence, a nitty gritty orderly writing audit is basic to get it where we will progress as an investi-

gating community To our shock, our inquiry uncovered that 9.1% of our collected thoughts, which centered on MFA, conducted any client assessment. The point of our thinking is to make strides in client selection of MFA and how to utilize the pre-existing inquiry to make strides in future thinking about designs.

The research work [9] “Access to Network Login by Three-Factor Authentication for Effective Information Security ” works on security that can protect our data, keep it trustworthy and make more trouble for unauthorized people to login and excess data. In the present world, our data is not secured and can be easily hacked by hackers even though we have single factor authentication or two factor authentication. This paper aims to secure that problem by using three factor authentication(3FA). They used three approaches. First approach is the password which is an alphanumeric password and the components are what you know. The second one is ATM cards (Something the user knows) or PIN (something the user possesses) and the component is what you have. And the last and third approach is bio-metrics such as unique identity, retina scan, fingerprints and the component are what you are. 3FA improves our security rather than two factor or single factor authentication as the last method is bio-metric so every person will have a different identity which cannot be easily hacked by any users and our data will be safe. But this approach has some drawbacks. The main issue is cost. Three factor authentication is more costly than other approaches as for (3FA) in the last step we need bio-metric fingerprint impression, palm right, and retinal output. Apart from the cost thing, three factor authentication is very useful for security purposes and it can be more efficient if we can find a way to reduce the cost.

The research work [6] “On the (In)Security of Mobile Two-Factor Authentication” finds out drawbacks and weaknesses of two factor authentication. Facebook, Google, Twitter, Dropbox uses 2FA and this paper investigates how it can be hacked easily even if it uses 2FA. In two factor authentication first authentication is password and secondary authentication is ATM cards or PINS. Even though your ATM card or PIN is unique and only you can know and if the secondary authentication (PIN) is not in hackers’ control still hackers can hack it. In this paper, they present a general attack against 2FA and use both mobile phone and PC for authentication. For attacking purposes, they use TAN and 2FA. Though 2FA is reasonable, easy to manage and largely usable, still lack of security is a major issue here. So, for better results we can implement three factor authentication (3FA) instead of two factor authentication (2FA) as it is a much more reliable, trustworthy and safe authentication system.

The research work [16] the author Greg Barrow has pointed out why two-factor authentication 2FA is not possible anymore. The 2FA authentication is a two-step process for the user to sign in. In the first step the user inputs their password and on the second step there is a physical token such as a debit card or a pass code or OTP code that is sent to the user’s cell phone by a third-party security system. Here, the author added that 2FA could make the users annoyed and cut corners and take shortcuts that makes the system more vulnerable. In addition, 2FA doesn’t even provide identity authentication. Instead, it authenticates the device under this assumption that it is under the control of the user. Moreover, the hacker can crack this 2FA only by stealing a physical token or cell phone which can be done virtually by using sim cloning that was done in 2019 with the Twitter CEO Jack Dorsey the author added. Moreover, Social Engineering attacks other than these phishing

attacks are commonly seen nowadays. Lastly, other than discussing the problems of the 2FA the author also talked about some solutions to solve this problem with Bio-metric Authentication which only the user can possess. Bio-metric technologies have shown a lot of vulnerabilities but at this moment it has made it more challenging for the hackers to hack into the system.



# Chapter 3

## Proposed Model

The purpose of the Three Factor Authentication is to make the data more secure and increase the privacy of the software.

### 3.1 Overall Approach of Proposed Model

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

1. At step 1 user has to login with username and password. User has to enter a valid username and a strong password
2. At 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 with the database the system will forward to step-3. If the user enters the wrong username or password the system will looped to step-1 again and will ask the user to enter username and password correctly.
3. At step 3 the second step verification will be started which is known as possession factor. In this step OTP or similar kind of employee id will be used to verify. In 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 user will get the open platform if the user selects the three-factor authentication or not. If the user is not interested in three-factor authentication then the sequence will be ended and user can login at step 4 from second time when will they use.
5. If the user selects three factor authentication there will be two options available for them. If the users have a well featured smartphone, then they can choose Bio-metric password otherwise they can use Graphical password. If the user selects Graphical password step 1,2 and 3 will work in the same pattern step 5 will be the new step if user enter the Graphical password correctly then it will go to step 7 and user can login successfully otherwise it will go step 5 again and ask the user to re-enter the Graphical password again. If the user selects bio-metric password step 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 above five steps user can have a secure login by three factor authentication.

## 3.2 Preliminary development

### 3.2.1 Coding Part

#### **2 factor authentication:**

After the user is logged into the system there will be an OTP authentication system the model is proposing. The 2 Factor authentication must have some criteria that is the password that will be used should be a onetime used code that is it can't be used again. As we will be making an Android app, we will use the SMS Retriever API. The first step of our code would be to gain a phone number where we will send our OTP code. After we got the phone number, we will send a onetime use code to that number which the user will be able to use for up to 5 mins that is after 5 minutes the user won't be able to use that code again and the user will need to resend for a new code again. After the code is received the user will be able to enter that unique OTP code and be able to login to the system, else it will show wrong OTP code and the user will be asked to resend the code again. A workflow diagram for the OTP Authentication is given below.

#### **Graphical User Password:**

The Graphical User Password lets users set a pattern over some random image in our case it is a set of fruits. This Feature is only available for the users whose phone doesn't support Biometrics (Fingerprint Scanner, Iris Scanner etc.). And this will work as the Third factor for Authentication and the user will be given an option to whether they want to enable this feature or not and remain with the Two factor Authentication. Every time the user logs in, the user will find a random Matrix which contains the fruits. The user will select a pattern over those fruits in a sequential manner. So, whenever the Matrix of fruits is randomized, only the user knows the sequence in which the user has chosen the fruits. The code will randomize the Matrix every single time and remember the sequence that the user selected while making the account. A workflow diagram is shown below.

#### **Fingerprint Scanner:**

Fingerprint is also used as Third Factor Authentication for the users who have a good configuration handset which contains the fingerprint sensor for bio-metric verification. For this the user will be asked whether the user wants to stay with the Two factor OTP authentication or make it more secure. The user can choose if he/she wants to have the bio-metric authentication. After agreeing the terms and conditions the user will train one of it's fingers first which the user will use to get logged into the system and it will get registered for that user. Fingerprint is more secure compared to any other authentication if we consider it cause it's unique and can't be matched with any other person or individual. A workflow diagram for the Fingerprint Authentication is shown below.

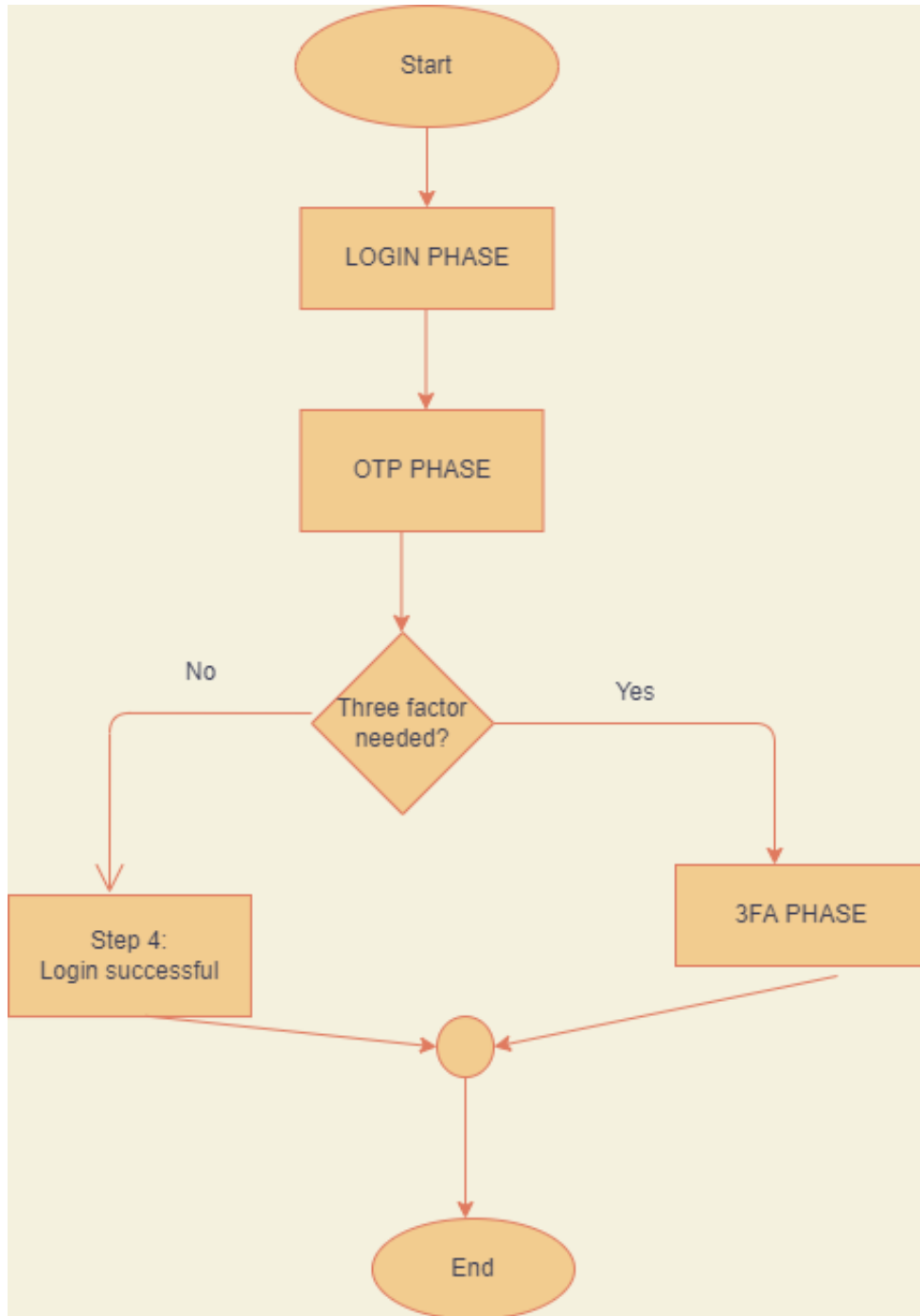


Figure 3.1: Flowchart of proposed model

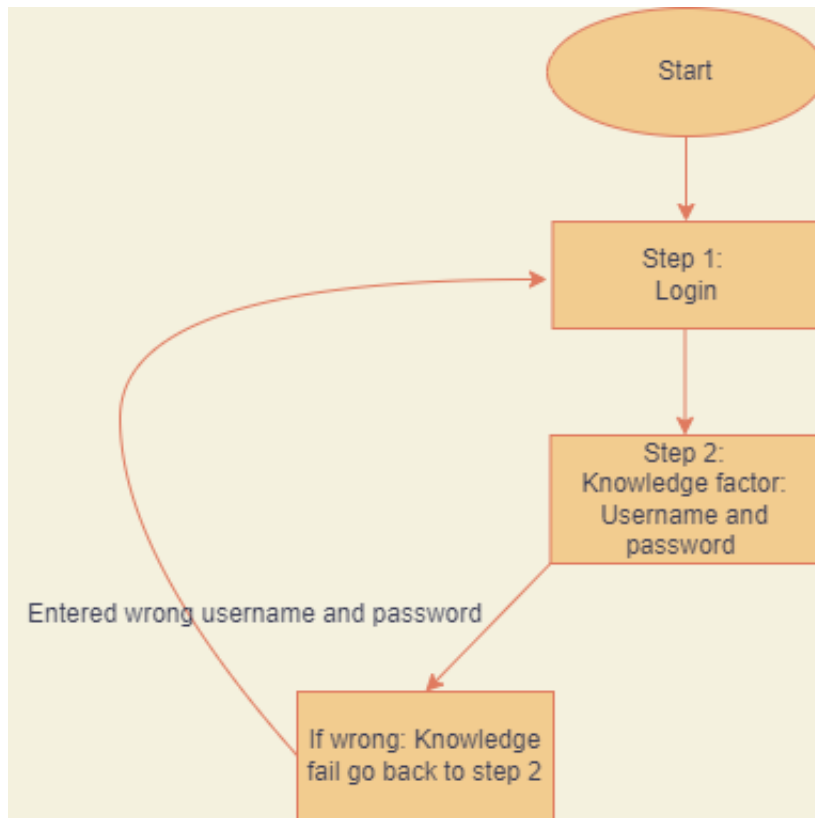


Figure 3.2: Detailed Flowchart of Login Phase

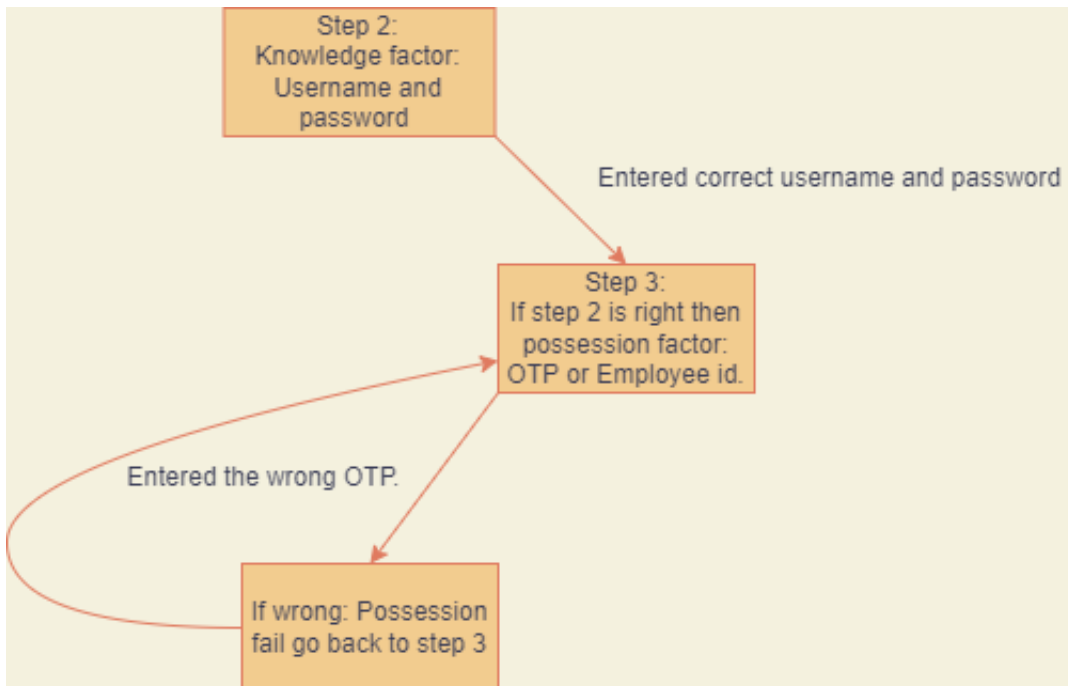


Figure 3.3: Detailed Flowchart of OTP Phase

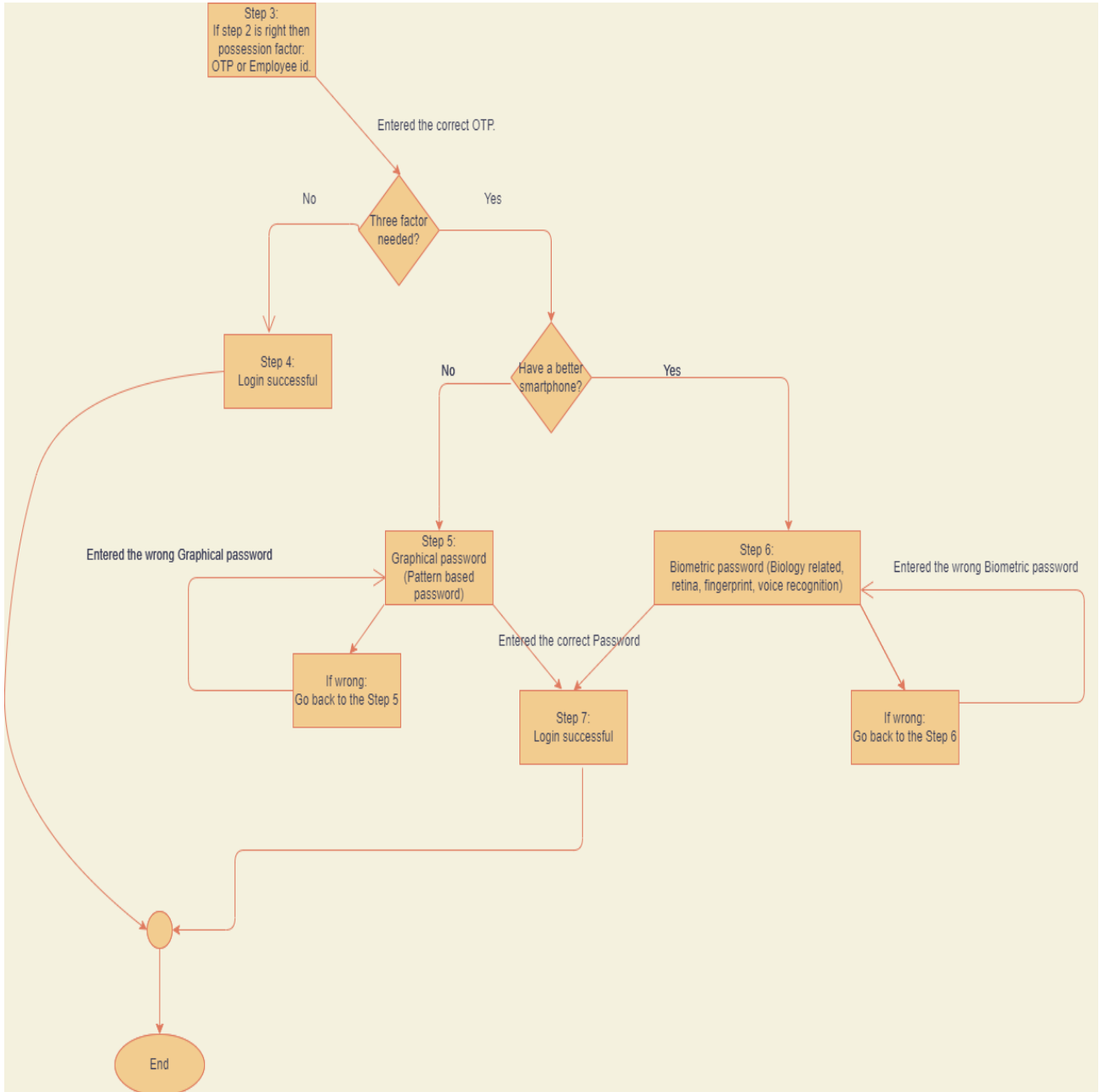


Figure 3.4: Detailed Flowchart of 3FA

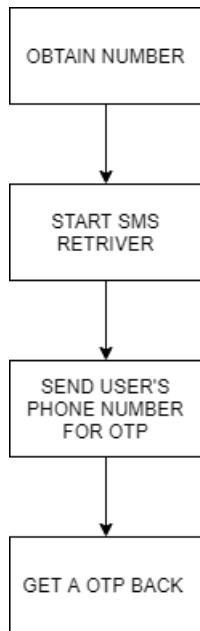


Figure 3.5: Workflow of OTP Authentication code

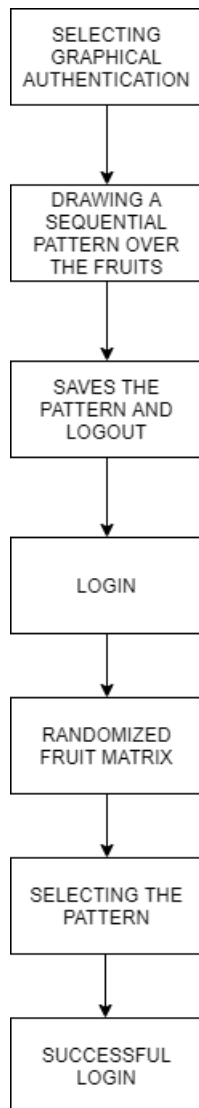


Figure 3.6: Workflow of Graphical Password Code.

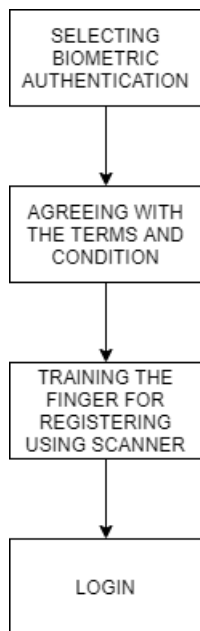


Figure 3.7: Workflow of Fingerprint Authentication



# Chapter 4

## Implementation

### 4.1 Login Page



The image shows a login form on a blue background. It has two input fields. The first is labeled 'Username :' and contains the text 'teamprethesistwo@gmail.com'. The second is labeled 'Password :' and contains seven asterisks '\*\*\*\*\*'. Below these fields is a button labeled 'Submit'.

Figure 4.1: Login page

At the first stage there will be regular login page. On that page there will be 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 the it will stay in the same page ask for correction. After correction it will move to next stage which is OTP sender stage.

### 4.2 OTP sender

Second stage of authentication is OTP sender. If our first step of authentication is successful the it will move on to OTP stage and a four-digit pin will be sent in the user's phone number. Then the user has to enter the pin in the correct place then it will move to third step of authentication if the user selects the third factor. Otherwise, it will stop here and the user can successfully login via two factor authentication. [18]

### 4.3 Graphical password

If the user selects the three-factor authentication, then there can be two possible outcomes one is graphical password and the other one is bio-metric password. In graphical password system then, random patterns will be generated. We can see the random patterns from the above figure.[8] For example, if a user selects the sequence



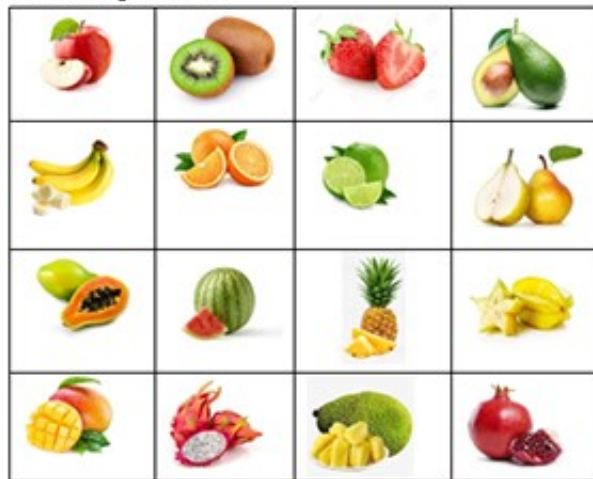
Figure 4.2: OTP sender

apple → lemon → pineapple → mango. In first figure we can find the pattern in row one column one (apple), row two column three (lemon), row three column three (pineapple), row four column one (mango). In the second figure we can see same fruits are in different pattern pineapple in row one column two, apple in row two column two, lemon in row two column three and mango in row four column four. Same type of randomize pattern we can see in the third figure as well.[12]

## 4.4 Bio-Metric

If the users have a better-quality smartphone, then he can choose bio-metric as their third factor authentication. Mainly when the user registers his/her account they will provide their fingerprint. Those finger print will be updated on the database later it will be used in further authentication. In the place of fingerprint many other ways can be implemented as well like voice recognition, iris scan, face recognition. But they are few loops whole in those process. In voice recognition a false user can record the genuine users voice and easily break the third factor. 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. From the above situations we made a conclusion that fingerprint scan will be the most preferable among rest of procedures.[19]

Random pattern 1



Random pattern 2



Random pattern 3



Figure 4.3: Graphical password

# Chapter 5

## Results

### 5.1 Password

To identify the total complexity of a password we found a formula from. Here S is the possibility space is based on the length. A is a list of total number of valid characters in the password. N is the size of the password. T is the time to break or hack the password. D computing hour to hack a password. For calculating the value of D divided the S value by  $10^9$  because computer can explore a billion possibilities per seconds.

*Formula :*

$$S = A^N$$

$$D = S/(10^9 \times 3600)$$

$$T = 2 \times \log_2[S/(10^9 \times 3600)]$$

Result 1:

$$A = 62 \text{ (A-Z, a-z and 0-9)}$$

$$N = 7$$

$$S = 62^7 = 3521614606000$$

$$D = 0.9782 \text{ computing hour}$$

$$T = 0$$

Result 2:

$$A = 72 \text{ (A-Z, a-z,0-9,10 symbols)}$$

$$N = 12$$

$$S = 72^{12} = 1.94 \times 10^{22}$$

$$D = 5391224989 \text{ computing hour}$$

$$T = 64.65$$

Password is the most common secure procedure to maximum of us.[13] But when it's a matter of a high security then password is not much alone. From the chart we can see different of combination of password and their breaking time. Most of the case we use the password between 6 to 8 digits and the combination of those passwords are maximum time digits or alphabets. In rare cases it is shown that a person is using the symbol, alphabet and numbers to protect the password. Sometimes it difficult to remember those passwords. To get the better security system with the addition of password we added more few steps. Then next stage is the OTP.

Number of characters	Numbers only	Upper or lower case only	Upper- and lower-case letters	Numbers, Upper- and lower-case letters	Numbers, Symbols, Upper- and lower-case letters
4	0 Seconds	0 Seconds	0 Seconds	0 Seconds	0 Seconds
5	0 Seconds	0 Seconds	0 Seconds	3 Seconds	10 Seconds
6	0 Seconds	0 Seconds	8 Seconds	3 Minutes	13 Minutes
7	0 Seconds	0 Seconds	5 Minutes	3 Hours	17 Hours
8	0 Seconds	13 Minutes	3 Hours	10 Days	57 Days
9	4 Seconds	6 Hours	4 Days	1 Year	12 Years
10	40 Seconds	6 Days	169 Days	106 Years	928 Years
11	6 Minutes	169 Days	16 Years	6000 Years	71000 Years
12	1 Hour	12 Years	600 Years	108K Years	5M Years

Figure 5.1: Password Breaking Time

Based on the formula the time to hack a password will be:

## 5.2 OTP

OTP stands for One Time Password. In stage 1 the password is collected from the user. In stage 2 the bit-by-bit password is being separated. In stage 3 the bit-by-bit password is collected from user and XNOR's with the computers database bit-by-bit password. In stage 4 AND operation is perform. In stage 5 it gives the result 1 or 0. If the result is 1 then the OTP matches with computer otherwise the OTP entered by the user was wrong. In every stage the is a complexity its is fast when the input is given according but this process is difficult to break if the input is not up to the point. In this there is total 5 stages. In the first stage of the system, it different each bit both from the user side and the computer side. In the second stage each of the bits are sent to its same index representative bit of the computer side in a XNOR gate. The XNOR gates truth table is given bellow. From the truth table we can see only if the inputs are equal then the output is showing 1. In stage 2 the same things will occur. If the software finds that the bit that came from the user side and the bit from computer side crosschecks. Then it moves to stage 3 the result bits from the stage two will be put into the and gate. The truth table of AND gate is given below:

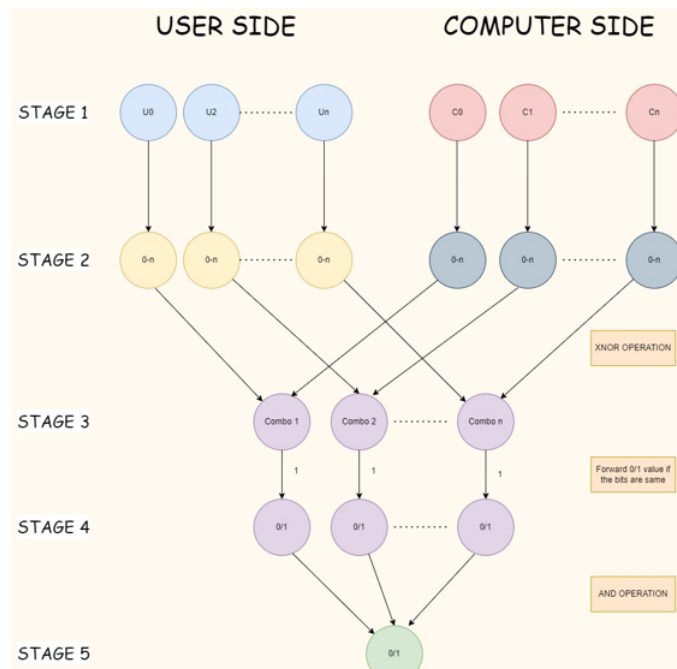


Figure 5.2: OTP Working Process

Input A	Input B	Output
0	0	1
0	1	0
1	0	0
1	1	1

Figure 5.3: XNOR Truth Table

Input A	Input B	Output
0	0	0
0	1	0
1	0	0
1	1	1

Figure 5.4: AND Truth Table

## 5.3 Bio-Metric System

### 5.3.1 Horizontal and Vertical Complexity

Mainly the fingerprint will be stored in matrix form. In every index the numerical pixel of the fingerprint will be stored.

2	-1	-2
1	0	3
5	-4	-5

2	1	5
-1	0	-4
-2	3	-5

Figure 5.5: Sample Matrix

In the process of Bio-metric the finger print store in matrix. In our example we have considered the 3x3 matrix. The data updated in every cell of the matrix. During the finger print scan, the finger can be either put in horizontal or in vertical. The verification should result the same in both ways both of the samples are from the same person. The data collection the sample will cover the entire finger. Our process will cover that in both ways. If the fingerprint is given in vertical the then the complexity will be calculated in double derivative of  $u$  and  $v$  with respect to  $x$  and double derivative of  $u$  and  $v$  with respect to  $y$  will be subtracted from that. The summations will be in a limit from  $u = i - w/2$  and  $v = j - w/2$ . The horizontal calculation will be calculated almost in the same way but this time derivative of  $u$  and  $v$  with respect to  $x$  and derivative of  $u$  and  $v$  with respect to  $y$  and 2 will be multiplied. Individual complexity will be calculated by this way. The total complexity of this entire process will be calculated in the third formula which is  $O(i,j)$ , and half of tan inverse vertical complexity divide by the horizontal complexity. The total complexity in a sum of password, OTP and bio-metric password is almost impossible to break. Each individual state has it's won complexity level. The sum will be near to 98-99% to break complexity. The total complexity in a sum of password, OTP and bio-metric password is almost impossible to break. Each individual state has it's won complexity level. The sum will be near to 98-99% to break. [20]

In this process the fingerprint needs to be almost 95-97% correct. But many of the smartphone does not provide that much accuracy. For keeping the accuracy level

Horizontal calculation:

$$V_x(i, j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} 2\partial_x(u, v) \partial_y(u, v)$$

Vertical calculation:

$$V_y(i, j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} (\partial_x^2(u, v) - \partial_y^2(u, v))$$

Total Complexity:

$$O(i, j) = \frac{1}{2} \tan^{-1}(V_y(i, j)/V_x(i, j))$$

Figure 5.6: Horizontal and Vertical Complexity Calculation

lower we can implement Hamming Distance. By this procedure we can manually control lower the accuracy.

### 5.3.2 Hamming Distance

By the use of Hamming Distance, we can manually consider the accuracy. So, if the fingerprint 90% matches with the sensor, then only the security system will unlock. If the d.min is less than 2 then the system will accept it and unlock the application. [4] [1]



$1\ 2\ 2\ -1\ 2\ 2\ 2\ 3\ 4\ 1 \oplus 1\ 2\ 2\ -1\ 2\ 1\ 2\ 3\ 4\ 1 = 1$   
 [Difference in 1 bit it will be accepted]

$1\ 2\ 2\ -1\ 2\ 2\ 2\ 3\ 4\ 1 \oplus 1\ 2\ 2\ 4\ 2\ 2\ 2\ 3\ 4\ 1 = 1$   
 [Difference in 1 bit it will be accepted]

$1\ 2\ 2\ -1\ 2\ 2\ 2\ 3\ 4\ 1 \oplus 1\ 2\ 2\ -1\ 1\ 1\ 2\ 3\ 4\ 1 = 2$   
 [Difference in 2 bits it won't be accepted]

$1\ 2\ 2\ -1\ 2\ 2\ 2\ 3\ 4\ 1 \oplus 1\ 2\ 2\ 0\ 2\ 2\ 2\ 3\ 4\ 1 = 1$   
 [Difference in 1 bit it will be accepted]

$1\ 2\ 2\ -1\ 2\ 2\ 2\ 3\ 4\ 1 \oplus 1\ 2\ 2\ 3\ 4\ 5\ 2\ 3\ 4\ 1 = 3$   
 [Difference in 3 bits it won't be accepted]

$1\ 2\ 2\ -1\ 2\ 2\ 2\ 3\ 4\ 1 \oplus 1\ 2\ 3\ -1\ 2\ 4\ 2\ 3\ 4\ 1 = 2$   
 [Difference in 1 bit it won't be accepted]

Figure 5.7: Hamming Distance

## 5.4 Graphical Password

In authentication systems, text-based passwords are a very popular and widely used method. But the problem can be easily cracked by the hacker within a very short time. So, it is not secure that much at all. However, there is an alternative way which is much more secure and reliable than text-based password and that is graphical password. There are different types of graphical password but mainly there are two groups, one is recognition-based scheme another one is recall base scheme. Nowadays users prefer passwords which are secure as well as user friendly. Some possible attack methods can be applied on graphical passwords. Such as, brute force search attack, dictionary attack, then guessing attack, another one is shoulder-suffering attack, spyware attack and lastly social attacks etc. Some graphical passwords can defend multiple attacks. There are six security features on graphical passwords. First one large password space, second one randomly assigns images, then hash function, after that image variation and decoy images are applied on the existing graphical password scheme. Jansen et al. scheme is a recognition-based scheme. It does not have a large password space but it has a hash function, randomly assigning images and decoy images. This scheme can defend against dictionaries, spyware and social attack. It is not very efficient but it is a grid-based system which is easy and fun to use. However, in Passfaces scheme, it can defend against only spyware and social attack and it has 2 features one is randomly assigned images and another one is decoy images so it is not very efficient but it has input reliability and accuracy. It is also a grid based easy and fun to use system which uses human faces and user assigned image memorability. Next scheme is Triangle, it is a recognition scheme which has the largest password space, decoy images and randomly assigned images and it can defend against 4 attacks: dictionary, spyware, shoulder suffering and

social attack. It is icon based with no efficiency but easy and fun to use. Next two schemes, Moveable Frame and Intersection have exacted the same security features like Triangle and those can defend the same 4 attacks. Also, their usability features are the same as the Triangle scheme. Another scheme is Pict-O-Lock scheme and it has the highest security features and a large password space, besides that it has randomly assigned images, image verification, decoy image and also repeat verification. It is the only one which can defend against guessing attacks, also shoulder suffering, social and dictionary attacks. Still for usability it is not very efficient but this is an icon and grid-based scheme with input reliability and accuracy. Déjà vu scheme has the same security features like Jansen et al. and also the same defending possible attack methods. It is a recognition scheme that uses abstract image memorability. Then comes four types of recall schemes Blonder, Viskey SFR, Passlogix v-Go and PassPoints and they can defend the same types of attacks and those attack methods are dictionary attack, spyware attack and social attack. But among these four Blonder and PassPoints have large password space and PassPoints has another hash function security feature. None of them are efficient but their usability features are different. Such as Blonder has meaningfulness, user assigned image and freedom of choice memorability. Viskey SFR has the same memorability as Blonder with extra input reliability and accuracy. Passlogix v-Go has meaningfulness, organized by theme and navigation image memorability. PassPoints is the only scheme which is efficient. It is because it takes very little time for authenticating users. Also, it has input reliability and accuracy with a grid base scheme and is easy and fun to use. Last one is the DAS scheme which is the only scheme that can defend against brute force attacks and also spyware and social attack. It has a large password space which is the reason to defend against brute force attack. The larger the password length and size, the more it is difficult for guessing and brute force to attack the password. DAS also has a hash function. DAS is a recall scheme which has a drawing password and it is grid based. So, for selecting a graphical password one should consider both of the usability and security features so that it can be user friendly as well as protect our security and authentication. Graphical password schemes cannot be easily cracked like text-based passwords. Some graphical passwords have some special security features such as large password space, hash function, decoy images to protect against attack methods dictionary, social engineering, brute force search and spy attacks. Also, users can easily remember graphical passwords rather than text-based passwords. Humans have some difficulties regarding remembering passwords. So, some preferred short texted based passwords but unfortunately those short passwords can be easily cracked by the hacker within a few times. So, some of them chose difficult lengthy passwords which are hard to crack but the problem in that case is that users often forget their password. As humans can remember pictures better than text so graphical password DAS can be an alternative solution for that. The Draw-a-Secret (DAS) scheme has an independent alphabet and it is a simple picture that is drawn on a grid. So, users don't need to remember alphanumeric strings. On the other hand, DAS schemes are more difficult to crack than texted base passwords because of the length and size of the password space, memorability and lack of knowledge of the distribution. Let's consider that users can pick any element as their passwords. Let's assume some fixed values have probability zero rather than all greater passwords of total length. The size of the space password of total length  $(L_{max}, G)$  is smaller than or same as  $L_{max}$  on a size of

a  $G \times G$  grid. Here, the number of the password with total length  $L$ ,  $P(L, G)$  and it can be defined as  $N(l, G)$  here  $l$  is the number of the stroke length. For making

$$\prod(Lmax, G) = \sum_{L=1}^{Lmax} P(L, G)$$

$$\prod_1^L(Lmax, G) = \sum_{L=1}^L P(L-1, G)N(L, G)$$

total length password new stroke  $l$  length added to length of a shorter password  $(L-1)$ . Assume number of the stroke length  $l$  is  $n(x, y, l, G)$  ending  $(x, y)$  cell in a  $G \times G$  grid size. So, in terms of  $n$ ,  $N$  can be defined as: by this we can calculate

$$N(l, G) = \sum_{(x,y) \in [1..G] \times [1..G]} 1 n(x, y, l, G)$$

$$\forall (x, y) \in [1 \dots G] \times [1 \dots G], n(x, y, 1, G) = 1. \text{ In Addition, } \forall (x, y) \notin [1 \dots G] \times [1 \dots G], n(x, y, 1, G) = 0.$$

**The function  $n$  will be:**

$$n(x, y, l, G) = n(x-1, y, l-1, G) + n(x+1, y, l-1, G) + n(x, y-1, l-1, G) + n(x, y+1, l-1, G)$$

the length of the password space. The raw size of the graphical password space is greater than textual password for reasonable password configuration. The greater the password length the more it can defend brute force attack. So, DAS is a more secure method than a text-based password. In this part we are going to introduce our proposed model. Our graphical password system will be provided to the users who really want the extra security layer provided over the 2FA. Here the user will be given a matrix structure suppose in the given Figure 1 an  $4 \times 4$  matrix which contains pictures of fruits. The user will serially select the fruits suppose in a sequential way a combination of 4 fruits. So, the user will be prompted with matrix of  $4 \times 4$  for the training of a password that will be used later by the user for logging in. Suppose the user sets a pattern by choosing the fruits in an order like Jackfruit  $\rightarrow$  Watermelon  $\rightarrow$  Apple  $\rightarrow$  Banana. Now when the user logs in for the second time the user will be prompted with a  $4 \times 4$  matrix containing the fruits again so the user can select the fruits according to the pattern the user set during the training time that is Jackfruit  $\rightarrow$  Watermelon  $\rightarrow$  Apple  $\rightarrow$  Banana and the user will be able to successfully log in to the system. If the user fails to choose the fruits according to the pattern set before it will show an incorrect password error and again will ask for the pattern of the fruits. The error prompt for wrong password will be given for around 5 time if the user fails to give the right pattern the 5th time the user will be sent to the first log in phase that is the normal password phase and the user will need to make an

OTP Authentication again to get successfully logged in to the system.

Now the most renowned problem of the pattern or graphical based password system is the shoulder surfing problem which is if anyone just has a glimpse of the password or the point that the user is touching anyone can easily break the password and get logged in to the user's account. Thus it is still a vulnerability to the existing graphical or pattern based password system. So, to fix this in the graphical pattern section the model has a unique solution. That is every time the user logs in for the graphical based pattern system the matrix elements are randomized, that is the fruits that were in the matrix  $[1] \times [1]$  once it is not there anymore. It might be in another grid cell of the matrix in  $[2] \times [3]$ . So, if anyone tries to shoulder surf once or assume the pattern by just watching the user draw the pattern over the phone won't be able to break through the system because the system that has been proposed follows a sequence of the selected elements in our case it is the fruit pictures. Furthermore, if we consider we have 16 cell for a  $4 \times 4$  matrix and 4 unique types of fruits. There is a combination of 4294967296 combinations which is impossible to break.

There is an Algorithm named PCCP (Persuasive cued click points) in this algorithm the user is prompted first to select some points in a picture highlighted in a grid view the user needs to select those point for a single picture first and then to the second picture and to the third in 5 stages. These points will need to be touched by the user when the user needs to authenticate to the same point that the user registered at first setting the password. If any of the points is wrong i.e selected by the user that is it does not match with the point once set by the user it will start showing wrong pictures that were never set by the user with a click point and thus the user won't be able to authenticate to get logged into the system. Suppose in the given figure 5.8 in the first picture of the bus there is some green click points set by



Figure 5.8: PCCP (Persuasive cued click point)

the user by selecting those points the user will be given the right pictures sequence and thus the user will be able to successfully login to the system else it will take the user to the wrong picture sequence and the user won't be able to successfully get logged in. If we compare the model that we have suggested with this PCCP model

our model has solved most of the vulnerabilities that this model possessed. Time Complexity: If we compare the time complexity of the PCCP Algorithm with our model. Suppose we have set the pattern limit to  $n=4$  that is the user needs to select 4 grid cells to get authenticated. So, the time complexity will stand around  $O(n)$  here  $n$  is the number of grids to be selected by the user. But in case of PCCP the user has to select cued points which are unknown and the user selects but it does not match with our model. But in our model, we just need to do it once but in case of PCCP every stage for the pictures there are the same number of selected points so if we consider the number of stages for pictures is  $k$  and the number of selected points be  $n$ . Therefore, the Time Complexity becomes  $O(k*n)$ . If we apply our model and PCCP with same number of click points the PCCP will take more time as there is a factor of  $(k)$  that is with the algorithm which is connected with the number of stages the cued points process will be divided and thus will have a final Authentication. Space Complexity: If we consider the space complexity of our model in our model, we just need to select values for the number of unique elements that we want in our matrix let it be  $n$  and the matrix which will be  $i*j$  so the complexity can be written as  $O(n*j)$ . On the other hand, for PCCP we are storing images for every single step which contains those cued click points. Each stage has a new picture that is to be selected by the user. And both for the right selection we will have the same number of pictures and for the wrong selection we will have the same number of pictures and it will be divided in the same number of stages. Suppose the stage number is  $n$  and the size of each picture be  $k$  and for both right and wrong selection process we have exact same number of pictures so the space complexity becomes  $O(2*(n*k))$ . [7]

# Chapter 6

## Conclusion and Future Work

### 6.1 Conclusion

Advancement in validation 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 prominent standard of security. 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 easily predicted like reformation in computation. On the other hand, some challenges are hard to predict like 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 a good solution for the security problem. Integrated three-factor authentication gives the best expediency for better security. Moreover, it gives users multiple options according to users' abilities and preferences. So, 3FA can be applicable in many applications. For example, online banking system, online shopping system, online money transactions and many other applications. 3FA has two options for users in their third authentication step.[17] If a user has a good quality smartphone and cost is not an issue for him, the user can easily use a biometric password as third authentication for the security purpose. It can be biology related, retina, finger print, 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 be also solved by 3FA. Instead of bio-metric they can choose graphical password as third authentication. It will be a pattern-based password. So, cost problem can be easily solved by giving 2 options to the customers in three factor authentication. It is user friendly and user can easily choose their type of authentication. By this process, our database will be much more secure than before. The main purpose of three factor authentication is to give better security.

### 6.2 Future Works

In our above proposed model we tried our best to make sure the model was theoretically right. But we still wanted to implement this model practically with companies like IBM , SOPHOS. As, 2FA has various types of security breaches that are discussed above so 3FA has a strong security which can fix this security breach. Also for future we want to make a app to offer it to the companies for their testing pur-

pose. Moreover, we will start a beta testing phase for the app to get an understanding how the people are using it or getting used to the new 3FA. Furthermore, there could arise some amount of problems related to the graphical password section also there is a lot to improve about the space and time complexity of the whole model when it will be implemented practically.

# Bibliography

- [1] A. Bookstein, V. A. Kulyukin, and T. Raita, “Generalized hamming distance,” *Information Retrieval*, vol. 5, no. 4, pp. 353–375, 2002.
- [2] E. F. Gehringer, “Choosing passwords: Security and human factors,” 2002, pp. 369–373.
- [3] S. R. R. J. K. Lee and K. Y. Yoo, “Fingerprint - based remote user authentication scheme using smart cards,” 2002, pp. 554–555.
- [4] M. Norouzi, D. J. Fleet, and R. R. Salakhutdinov, “Hamming distance metric learning,” in *Advances in neural information processing systems*, 2012, pp. 1061–1069.
- [5] T. T. Contributor, “Three-factor authentication (3fa). retrieved from tech,” Nov. 2014. DOI: <https://searchsecurity.techtarget.com/definition/three-factor-authentication-3FA>.
- [6] R. C. Dmitrienko A. Liebchen C., “On the (in)security of mobile two-factor authentication,” 2014. DOI: [doi.org/10.1007/978-3-662-45472-5\\_24](https://doi.org/10.1007/978-3-662-45472-5_24).
- [7] M. R. S., C. D. K., and M. M. D., “Graphical password authentication system,” *Graphical Password Authentication System*, vol. 3, no. 4, pp. 353–375, 2014.
- [8] M. A. S. Gokhale and V. S. Waghmare, “The shoulder surfing resistant graphical password authentication technique,” *Procedia Computer Science*, vol. 79, pp. 490–498, 2016.
- [9] D. S. S. Vaithyasubramanian A. Christy, “Access to network login by three-factor authentication for effective information security,” 2016. DOI: [doi.org/10.1155/2016/6105053](https://doi.org/10.1155/2016/6105053).
- [10] K. Garska, “Why sms 2-step verification won’t keep you safe.,” Sep. 2017. DOI: <https://blog.identityautomation.com>.
- [11] R. India, “A three-factor authentication scheme in atm,” 2018. DOI: [www.ripublication.co](http://www.ripublication.co).
- [12] NevonProjects, “Smart android graphical password strategy.,” 2018. DOI: [projects.com/smart-android-graphical-password-strategy/](https://projects.com/smart-android-graphical-password-strategy/).
- [13] J.-P. 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.
- [14] M. S. Jalali, B. Russell, S. Razak, and W. J. Gordon, “Ears to cyber incidents in health care,” *Journal of the American Medical Informatics Association*, vol. 26, no. 1, pp. 81–90, 2019.



- [15] M. Shuai, “Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks,” 2019, pp. 14–14.
- [16] G. Barrow, “What’s wrong with two-factor authentication? retrieved from securityscorecard,” Nov. 2020. DOI: <https://securityscorecard.com/blog/whatswrong-with-two-factor-authentication>.
- [17] S. S. Bhuyan, U. Y. Kabir, J. M. Escareno, *et al.*, “Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations,” *Journal of medical systems*, vol. 44, no. 5, pp. 1–9, 2020.
- [18] A. Kurniawan, “Easy ways to implement automatic sms verification in android,” Apr. 2020. DOI: [medium.com/gits-apps-insight/easy-ways-to-implement-automatic-sms-verification-in-android-2b5d8040afbd](https://medium.com/gits-apps-insight/easy-ways-to-implement-automatic-sms-verification-in-android-2b5d8040afbd).
- [19] G. for Geeks, “How to add fingerprint authentication in your android app,” 2021. DOI: [www.geeksforgeeks.org/how-to-add-fingerprint-authentication-in-your-android-app](http://www.geeksforgeeks.org/how-to-add-fingerprint-authentication-in-your-android-app).
- [20] N. Maček, S. Barzut, and S. Adamović, “A novel fingerprint biometric cryptosystem based on convolutional neural networks,” vol. 9, no. 7, p. 730, 2021.
- [21] T.-Y. Wu, “A provably secure three-factor authentication protocol for wireless sensor networks,” 2021, pp. 15–17. DOI: [doi.org/10.1155/2021/5537018](https://doi.org/10.1155/2021/5537018).