RESEARCH ON DIFFERENT USER AUTHENTICATION SYSTEM

A PROJECT REPORT

Submitted by

SHRUTI LAKHARA 20BCY10173

ROHAN KOLHATKAR 20BCY10177

PRAHASITH POLINA 20BCY10142

JOEL FRANKO 20BCY10104

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

CYBER SECURITY AND DIGITAL FORENSICS

VIT®
BHOPAL
www.vitbhopal.ac.in

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

VIT BHOPAL UNIVERSITY

KOTHRIKALAN, SEHORE

MADHYA PRADESH - 466114

APRIL 2022

VIT BHOPAL UNIVERSITY, KOTHRIKALAN, SEHORE MADHYA PRADESH – 466114

BONAFIDE CERTIFICATE

Certified that this project report titled **"RESEARCH ON DIFFERENT USER AUTHENTICATION SYSTEM"** is the Bonafide work of "**SHRUTI LAKHARA (20BCY10173) ROHAN KOLHATKAR (20BCY10177) PRAHASITH POLINA (20BCY10142) JOEL FRANKO (20BCY10104)**" who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

PROGRAM CHAIR

Dr. R. Rakesh, Assistant Professor
School of Computer Science and Engineering
VIT BHOPAL UNIVERSITY

PROJECT GUIDE

Dr. Rajasoundram S., Assistant professor
School of Computer Science and Engineering
VIT BHOPAL UNIVERSITY

The Project Exhibition I Examination is held on 21/02/2022.

ACKNOWLEDGEMENT

First and foremost, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr. Pushpinder Singh Patheja, Head of the Department, School of Computer Science and Engineering for much of his valuable support encouragement in carrying out this work.

I would like to thank my internal guide Dr. Rajasoundram sir for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Computer Science and Engineering, who extended directly or indirectly all support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

LIST OF FIGURES AND GRAPHS

ABSTRACT

One of the challenges faced by our research was the unavailability of reliable training datasets. In fact, this challenge faces any researcher in the field. However, although plenty of articles about predicting phishing websites using data mining techniques have been disseminated these days, no reliable training dataset has been published publicly, maybe because there is no agreement in the literature on the definitive features that characterize phishing websites, hence it is difficult to shape a dataset that covers all possible features.

In this report, we shed light on the important features that have proved to be sound and effective in predicting phishing websites. In addition, we proposed some new features, experimentally assign new rules to some well-known features, and update some other features using some research papers as a reference

TABLE OF CONTENTS (SPECIMEN)

2	**CHAPTER-2:** **RELATED WORK INVESTIGATION** 2.1 Introduction 2.2 Core area of the project 2.3 Existing Approaches/Methods 2.4 Pros and cons of the stated Approaches/Methods 2.5 Issues/observations from investigation 2.6 Summary	
3	**CHAPTER-3:** **REQUIREMENT ARTIFACTS** 3.1 Introduction 3.2 Hardware and Software requirements	

CHAPTER-1:

PROJECT DESCRIPTION AND OUTLINE

1.1 Introduction:

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In doing this, authentication assures secure systems, secure processes and enterprise information security. There are several authentication types. For purposes of user identity, users are typically identified with a user ID, and authentication occurs when the user provides credentials such as a password that matches their user ID. The practice of requiring a user ID and password is known as single factor authentication (SFA). In recent years, companies have strengthened authentication by asking for additional authentication factors, such as a unique code that is provided to a user over a mobile device when a sign on is attempted or a biometric signature, like a facial scan or thumbprint. This is known as two factor authentication (2FA). Authentication factors can even go further than SFA, which requires a user ID and password, or 2FA, which requires a user ID, password ,biometric signature and face id. When three or more identity verification factors are used for authentication for example, a user ID and password, biometric signature and perhaps a personal question the user must answer it is called multifactor authentication (MFA). And now the widely used and most secure authentication system is Token based authentication system it is also a MFA based authentication system.

1.2 Motivation for the work:

With the increased usage of internet and technology the world of cyber crime and the threats we face from it have expanded far beyond so the need of cyber security have been increasing. So the most important and widely used cyber security method is authentication so the need to the improvement of the cyber security has drive us to take the topic of different types of authentication systems and to research about it to know their limitations, benefits and usability.

1.3 Introduction to the project and the techniques:

In this paper we have included our research on different types of authentication systems and their limitations. We have explained briefly about different types of authentication systems,

their disadvantages and their rate of success. We have also included some working protocols and framework of the authentication systems. The most important factor for concerns with the authentication systems is how secure it is and how easy to use it is. Taking security as the biggest concern we can easily say that a secure and updated authentication system is the need of every organization. Also our research paper presents some new applications of these authentication systems and models which can be brought into use and is more safe.

1.5 Problem Statement:

The problem statement of our research is to analyze different type of authentication systems we took around six authentication systems namely SIMPLE PASSWORD-BASED, GRAPHICAL OR IMAGE-BASED, TOKEN-BASED, BIOMETRICS BASED, QR BASED and TWO FACTOR AUTHENTICATION. And to differentiate them by three factors usability, security, Deploy-ability and to know each of the authentication systems weaknesses, strengths and usability then we also found in which sector each of the authentication is well suit for.

1.6 Objective of the work:

Our main objective of our research is to analyze the six different typed of authentications and to know their strength and limitations and then to finally know which one of the six authentication is best authentication overall. For that we have used three factors to differentiate them and using the three factory we gave points accordingly the be finally found our best authentication system and also the limitations and the strength of the other authentication systems.

1.7 Organization of the project:

Our Project is organized by our team according to some split-ups of information and data we collected from different research papers. We gathered information about authentication systems and their limitations and strengths through some research papers. By using the three factors namely usability, security and deploy-ability we found out about the limitations and strengths of the six authentication systems and also, we found the best authentication system among them.

1.8 Summary:

In this chapter we have discussed about the introduction of the authentication systems then we saw how do we got the motivation to do this research paper and then we also discussed the basic outline of our research work then we discussed the main problem and the objective of our research work and finally we also have discussed how our research have been organized.

CHAPTER-2:

RELATED WORK INVESTIGATION

2.1 Introduction:

In this chapter we will see about the work and investigation we did to complete our research work. We will also see about the methodology and the issues we faced when we investigate for our research work.

2.2 Core area of the project:

The core area of our research work is based on the authentication systems. Authentication systems are a method used in cyber security to identify or authenticate a user, a product or some logins which needs authentication.

2.3 Existing Approaches/Methods

2.3.1 Approaches/Methods -1;

At first for our research, we collect around two to three research papers for each of the six authentication systems. Then using the research papers of each authentication systems, we found each of their limitations, strengths and usability and we collated each research papers key features and formed notes.

2.3.2 Approaches/Methods -2:

Then after using the formed notes, we created a separate not by differentiating and evaluating each research papers according to some three factors namely usability, security and deploy-ability. Then we created a graph with x-axis as usability and y-axis as security and color code to differentiate the deploy-ability and then we plotted the six authentication systems and found out which has high usability, security, deploy-ability and then we finally found the best authentication system as which has the highest points.

2.3.3 Approaches/Methods -3;

We also have then implemented some of the authentication systems to analyze the real time scenario of the authentication system. For that we first learned the algorithm of the authentication system and then we searched on some webpages and YouTube videos and then using C++, Python, Android Studio and with some help of external modules and websites we created some implementations of authentication systems.

2.4 Pros and cons of the stated Approaches/Methods :

The pros of the methods we use for our research are that is the very easy to understand and they are more applicable and reliable. The cons of our method are that it is so simple it may do not work on advanced level authentication systems such as MFA and so on.

2.5 observations from investigation:

For our research we have had some observations on sone web pages, applications and smart phones which use authentication systems. As for the simple password based authentication, we used an ordinary smart phone and then understood the working of it, then for the graphical or imaged based authentication system we used a website which asks to verify using an image based authentication and then for token-based authentication system we used a app called Wazirx which is a crypto coin investment app which uses token-based authentication to authenticate a user and the for biometrics based authentication system we used a smart phone and a laptop which uses finger print and face reorganization. Then for QR based authentication system we used G-pay app to see how a QR is used to authenticate a transaction. Then for Two Factor Authentication(2FA) we use our college V-top to see as it uses a 2FA authentication and also, we used Gmail to get further understand on 2FA.

2.6 Summary:

In this chapter we have seen about the core area in which our research is related and then we discussed about the methodology of how our research is done and their implementations. Then we have discussed about the pros and cons of our methods and then finally we have discussed about the observation we have did for our research paper. This chapter will give a clear idea about the word we have did related to our research paper.

CHAPTER-3:

REQUIREMENT ARTIFACTS

3.1 Introduction

We are implementing 4 Authentication systems, namely

1. simple password

2.OTP authentication

3.Fingerprint authentication

4. QR authentication

3.2 Hardware and Software requirements

We have implemented all these authentication systems using C++, and Python modules

- In the OTP based authentication we have used the software “TWILLO” for sending OTP for verification purposes
- In simple password authentication is implemented using language C++, where for storing the username and the password we have used the **“STL”** function map
- The QR based authentication we have used the Python modules open **CV** for generating the QR image and decoding it
- In the fingerprint authentication, it is implemented using A**ndroid studio** and language **java** and it will work only if the fingerprint is already set up in your android device

CHAPTER-4:

DESIGN METHODOLOGY AND ITS NOVELTY

4.1 Methodology and goal

We always came across many authentications but we never try to get the knowledge why they have implemented that particular authentication system. So, the main goal here is to know why such authentication system is chosen for the particular case and which is the best authentication system.

4.2 Functional modules design and analysis

We can analyze the system the implementations of the systems as that the simple password one is too easy to use. Also, it has less security and can be brute forced. The OTP one is bit secured and it can be used as the second factor in two factor authentication. The limitation with the biometrics and QR one is that it it requires a device well with has the camera and fingerprint sensor. Also the fingerprint one only works if the user has already setup his fingerprint in a device.

CHAPTER-5:

TECHNICAL IMPLEMENTATION & ANALYSIS

5.1 Outline

The research papers deal with the six user authentication types out of which 4 we have implemented. The names of those authentication systems are simple password, OTP based, biometrics based and QR code based.

5.2 Technical coding and code solutions

Implementation of simple password.

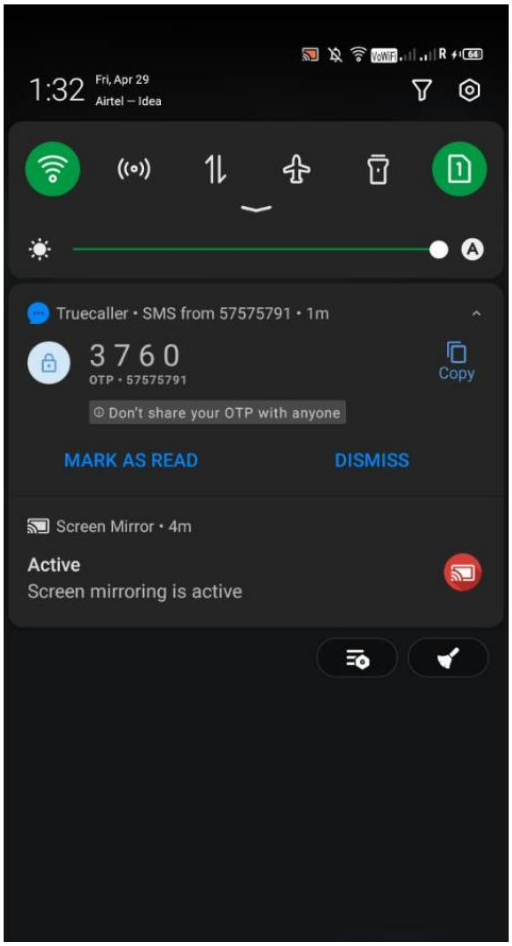
```cpp
// Online C++ compiler to run C++ program online
#include <bits/stdc++.h>
using namespace std;

int main() {

    cout<<"signup -01 or login-02";
    int x;
    cout<<"choose 1 or 2\n";
    cin>>x;

    map<string, string> mp;

    if(x==1){
        string x;
        cout<<"enter a username to signup   ";
        cin>>x;

        string y;
        cout<<"enter a password to signup   ";
        cin>>y;

        mp.insert({ x, y });
        cout<<"signup succesfully done: now can now login using your
            credentials \n";
```

```
        x=2;

    }

        string x1;
        cout<<"enter a username for login   ";
        cin>>x1;

        string y1;
        cout<<"enter a password for login   ";
        cin>>y1;

        bool flag = true;

        if(flag == true){
            for (auto itr = mp.begin(); itr != mp.end(); ++itr) {
                if(itr->first == x1 ){
                    if(itr->second == y1){
                        cout<<"you are succesfully logged in";
                    }else{
                        cout<<"Username or password is incorrect: Login Failed"
                    }
                }
                else{
                    cout<<"Username or password is incorrect: Login Failed";
                }
            }



        }



    return 0;
}
```

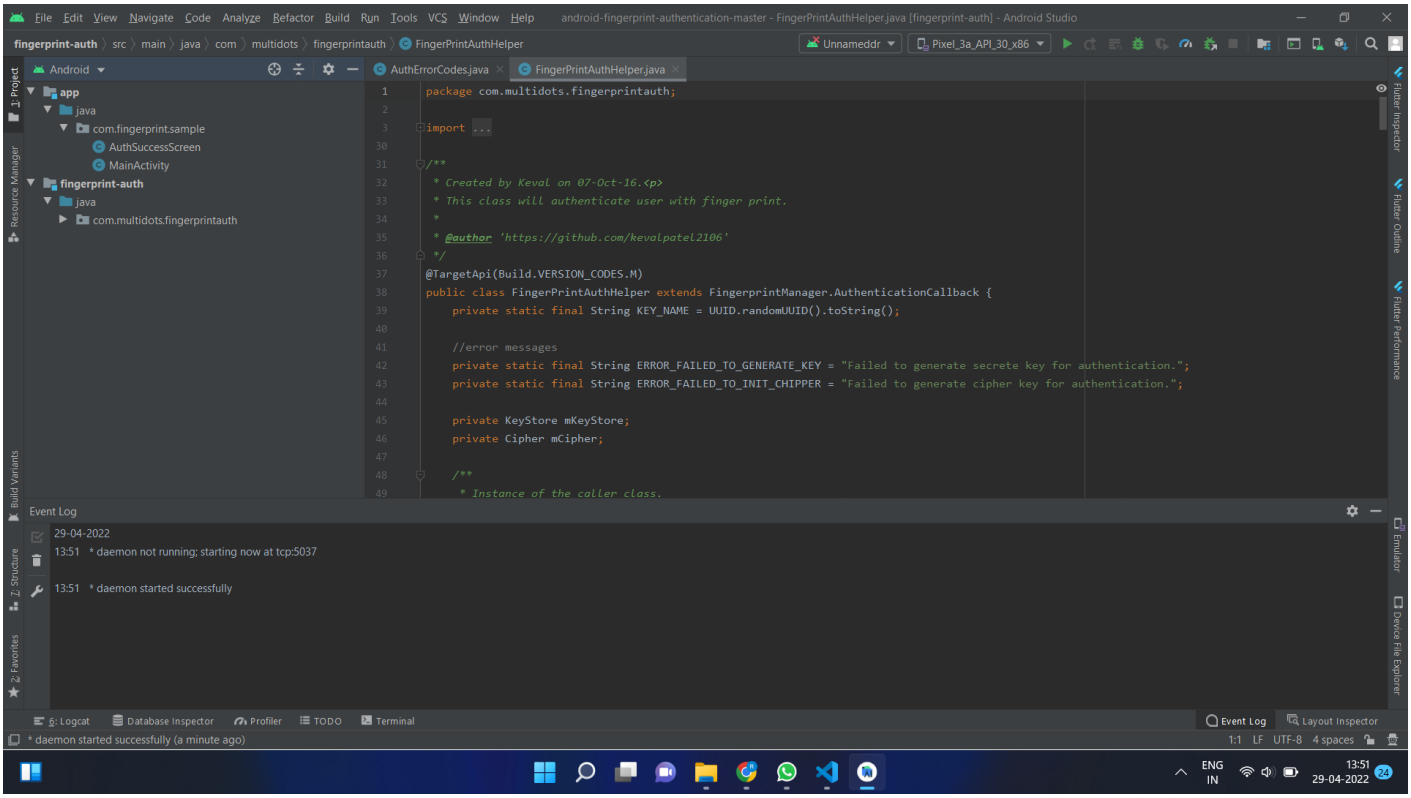
```
/tmp/exlOV1DG54.o
signup -01 or login-02choose 1 or 2
1
enter a username to signup   rohan
enter a password to signup   rohan132
signup succesfully done: now can now login using your credentials
enter a username for login   rohan
enter a password for login   rohan930
Username or password is incorrect: Login Failed
```

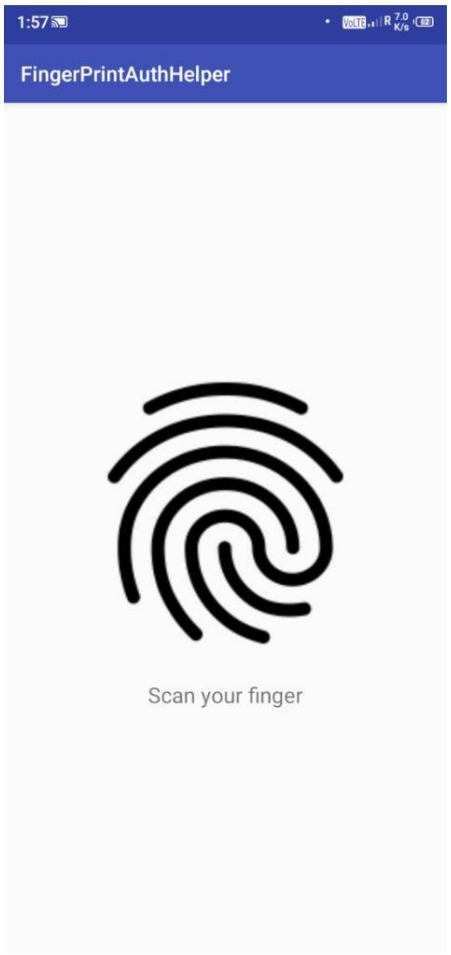
Implementation of OTP based authentication.

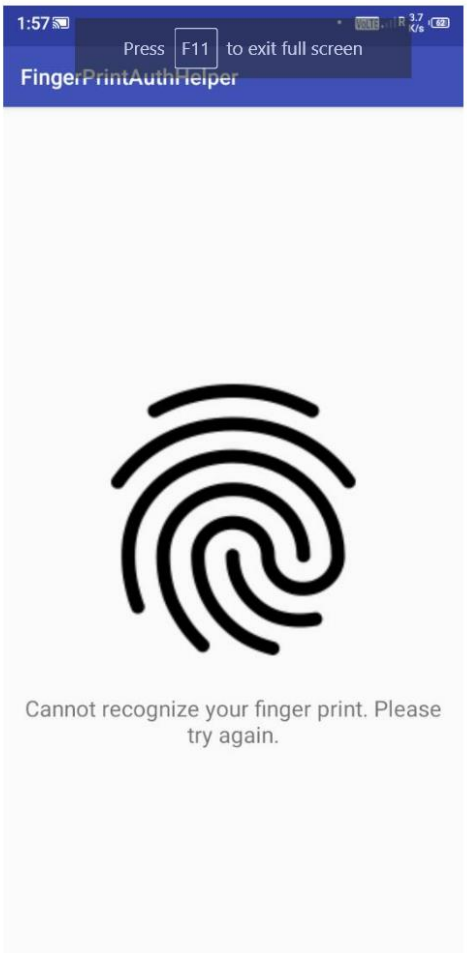
```python
# RECEIVING OTP using twillio

import random
from twilio.rest import Client

# // using my client twillio client id to send otps

otp = random.randint(1000,9999)
account_sid = "AC97057989246d93d0256e7872426c3e4a"
auth_token = 'bf2134bab0a1be59d86c7fc50c3fff7b'
client = Client(account_sid,auth_token)


msg = client.messages.create(

  body = f"your otp is {otp}",
  from_ = "+19206774932",   #this is yours own twillio phone number given after account creation

  to = "+918770792399"   #to any phone number


  )

```

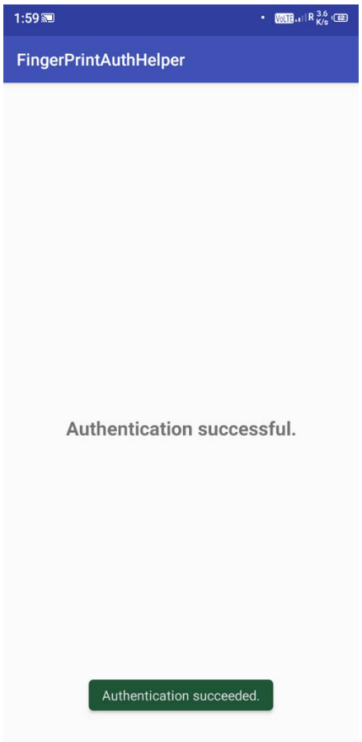


Implementation of biometrics based

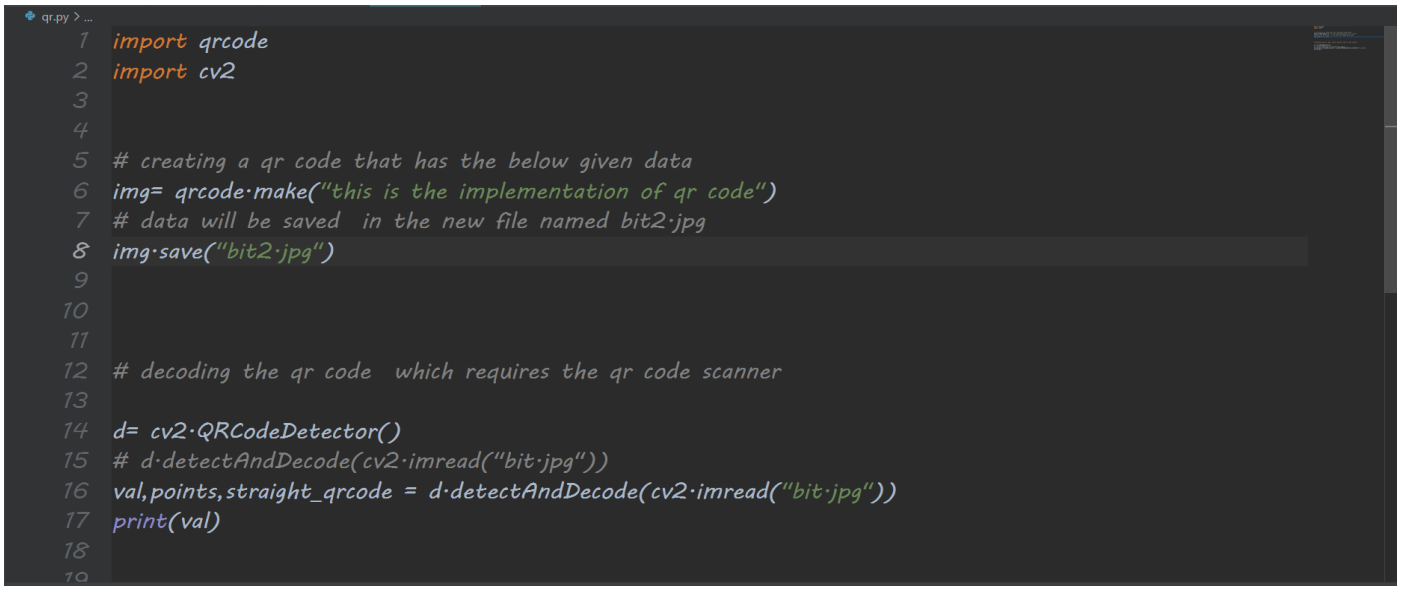



1:57
FingerPrintAuthHelper
Scan your finger


1:57
Press F11 to exit full screen
Cannot recognize your finger print. Please try again.


1:59
FingerPrintAuthHelper
Authentication successful.
Authentication succeeded.

Implementation of QR code based



```python
import qrcode
import cv2


# creating a qr code that has the below given data
img= qrcode.make("this is the implementation of qr code")
# data will be saved  in the new file named bit2.jpg
img.save("bit2.jpg")



# decoding the qr code  which requires the qr code scanner

d= cv2.QRCodeDetector()
# d.detectAndDecode(cv2.imread("bit.jpg"))
val,points,straight_qrcode = d.detectAndDecode(cv2.imread("bit.jpg"))
print(val)
```


Press F11 to exit full screen
1:42
Google Lens
Translate
Text
Search
Homework
Shopp
QR code: Text
Search
Copy text
Translate
this is the implementation of qr code


bit.jpg

5.3 Test and validation

The implementations shown above are just the showcases of how an authentication system can be implemented. The QR code one has the limitations like it can't be used if the device doesn’t have qr code scanner. The biometrics one also has the same limitations that device must have a fingerprint scanner or camera for face recognition.

5.4 Summary

The research paper counts the limitations of each and every authentication system. After we have done implementations, we have compared the system based upon there usability, deployability and security for finding the best one suited for the general case.

CHAPTER-6:
PROJECT OUTCOME AND APPLICABILITY

6.1 Outline

The research papers have account of all the authentications system. Out of which four are implemented and compared.

6.2 key implementations outline of the System

We have briefly explained about all the authentications systems available and also tried to explain how those systems can be made more efficient using some new technologies and some shown their simple implementations.

6.3 Significant project outcomes

The most significant outcome is upon comparison we have concluded two factor one as the best system that too if it contains token as one of the factors

6.4 Project applicability on Real-world applications

The research paper will help the people to decide which system is best suited according to their needs. For an example if they have the most focus on the security of their authentication, they can prefer two factor authentications. If they know that their user has devices well equipped with camera and fingerprint, they may

prefer the biometrics one. Otherwise on the usability side the simple password is the best suited and mostly used one. So, like this the research paper will help them knowing Indepth of all the user authentication system.

CHAPTER-7:

CONCLUSIONS AND RECOMMENDATION

7.1 Outline

We compared and mentioned the contrast between six authentication systems. Out of which we even implemented 4 authentication systems namely simple password, QR, fingerprint, and biometrics.

7.2 Limitation/Constraints of the System

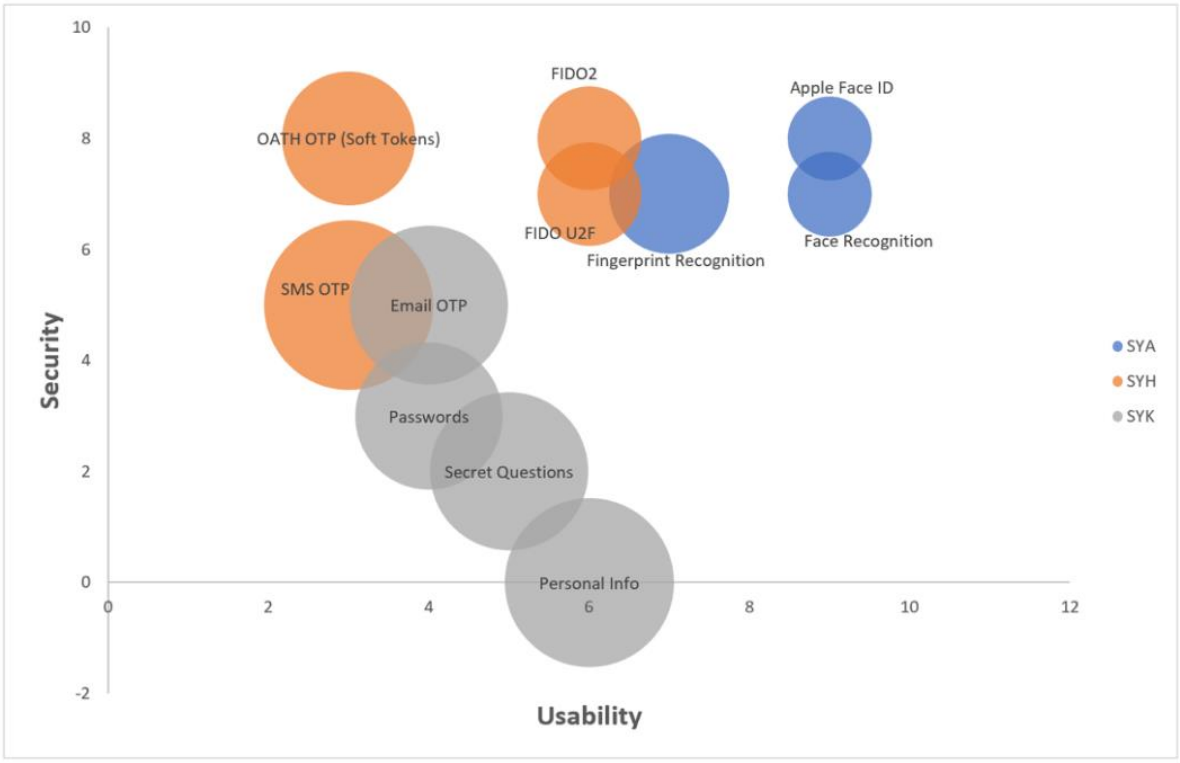
There can not be a single authentication system consisting of all the types. We have implemented them individually and have compared the system.

7.3 Future Enhancements

The systems which are less secure can be made more secure by applying more layers of security in the code. The research paper can be used for knowing the best references paper and the more about all the authentication systems.

7.4 Inference

In reference to the given diagram Apple face ID based authentication system is the most secure and convenient to use. Simple password is the least secure system. The term SYA – Something You Are; SYH – Something You Have; SYK – Something You Know are used in the chart. We can conclude from the research that the token based and the two factor authentication can be regarded as the best possible authentication methods todays considering the security factor today.


10
8
6
4
2
0
-2
0
2
4
6
8
10
12
Security
Usability
OATH OTP (Soft Tokens)
FIDO2
FIDO U2F
Fingerprint Recognition
Apple Face ID
Face Recognition
SMS OTP
Email OTP
Passwords
Secret Questions
Personal Info
SYA
SYH
SYK

REFERENCES

1. Mushtaq Ali , Amanullah Baloch, Abdul Waheed , Mahdi Zareei , Rimsha Manzoor1, Assam Sajid, And Faisal Alanazi “A Simple And Secure Reformation-based Password Scheme”

2. Nizamani, Shah, Hassan, Raheel, Shaikh, Riaz, Abozinadah, Ehab Mehmood, Rashid “A Novel Hybrid Textual-graphical Authentication Scheme With Better Security, Memorability, And Usability “

3. Takayuki Kawamura , Tadashi Ebihara , Naoto Wakatsuki , And Keiichi Zempo , “Eyedi: Graphical Authentication Scheme Of Estimating Your Encodable Distorted Images To Prevent Screenshot Attacks”

4.Syed Shabih Ul Hasan; anwar Ghani; muhammad Bilal; alireza Jolfae “Multifactor Pattern Implicit Authentication”

5.Ruben Tolosana; Ruben Vera-rodriguez; Julian Fierrez; Javier Ortega-garcia : Touchscreen Password Biometrics Using Time-aligned Recurrent Neural Networks

6.Ba Ajeethra; Sv Gautham Prasath; R Arun Balaji; Kakelli Anil Kumara” Cryptography Based Face Authentication System For Secured Communication”

7.N.R. Pradeep; J Ravi “An Efficient Machine Learning Approach For Fingerprint Authentication Using Artificial Neural Networks”

8. Yang-waichow ,Willysusilo, Jianfengwang, Richardbuckland, Joonsangbaek, Jongkilkim, Nanli” Https://Www.Sciencedirect.Com/Science/Article/Pii/S1084804520303040”

9. Chow, Yang-wai,susilo, Willy, Yang, Guomin,au, Man Ho, Wang, Cong “Authentication And Transaction Verification Using Qr Codes With A Mobile Device”

10. Abdelouahid Derhab; Mohamed Belaoued; Mohamed Guerroumi; Farrukh Aslam Khan”two-factor Mutual Authentication Offloading For Mobile Cloud Computing”

11. Yossi Oren; Dan Arad “Toward Usable And Accessible Two-factor Authentication Based On The Piezo-gyro Channel”

12. Petrova, K. Romaniello, Beatriz, Medlin, B.Vannoy, Sandra “Https://Www.Researchgate.Net/Publication/307879267_qr_codes_advantages_and_dangers”