USER FRIENDLY SECURE AUTHENTICATION SYSTEM

A PROJECT REPORT

For

ITE4001- Network and Information Security

in

B.Tech – Information Technology and Engineering

Winter Semester 2021 - 2022

By

RAJANALA SAI BHUVAN (19BIT0170)

RAAVI SHIVA SESHI REDDY (19BIT0173)

Guided By

Dr. JEYANTHI N

Associate Professor Sr, SITE.

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Abstract:

We all know that in current generation whole world is extensively using the services of internet every now and then. For any kind of need there is a solution available on internet. So it is obvious that there will be some people who will be looking to take advantage of this situation. Like by stealing others personal information they can threaten them or may misuse that information for wrong practices etc.

So automatically Security becomes an important factor, as a big concern will raise in every people's mind about their privacy and sensitive information. So here comes the concept of authentication, it is one such domain that offers a lot to be explored. Authentication means giving assurance and confirmation of a user's identity. But authentication is a vast concept, that covers a lot of ideas.

So we thought to develop a authentication process which is user friendly and also gives the assurance for users that, their sensitive data/information is safe and secured.

Literature Review:

AUTHORS	YEAR	TECHNOLOGY	MERITS	DEMERITS
Nat Maysenburg, Ross Schulman	2020	Internet of Things	Helpful for sensitive data	Time consuming process
Andi Wilson Thompson	2020	Multi factor authentication	Supports any kind of data	Complex process
Brian Lennon	2015	Language understanding AI	Simple and cheap	Supports only selected languages
Steven N Peskind	2014	Protocol modification	Fast process	Supports only email accounts
Michael Silverstein	2016	Password length analysis	Cheap process	Works for simple passwords only
George Boone, Jonathan Huang, Tim Sweijs	2020	Biometrics analysis	Efficient security and privacy	Expensive process
Paul W Grimm	2014	Password analysis	Cheap and fast	Less efficiency, less accuracy
Ewa Stanczyk	2017	Photograph analysis	High efficiency	Expensive process
David A Scott	2016	Biometrics analysis	Fast process	Less efficiency, expensive process
Luciana Duranti, Allison Stanfield	2021	Multi factor authentication	Supports all kinds of users	Complex process
Simon Parkinson, Na Liu, Liam Grant	2020	Activity trackers	High efficiency, high accuracy	Works for limited types of data and limited users
Ran Gao, Huawei Tu	2021	Body movement, arm raising gesture	High efficiency, high accuracy	Works only for smartwatch

Karen Renaud, Antonella De Angeli	2014	Biometrics and visual data analysis	Fast process	Expensive process, less efficiency
Tsu Yang Wu, Yuh Min Tseng	2019	Password analysis	Cheap and efficient	Works for simple passwords only
Hung Yu Chien, Jinn Ke Jan	2013	Password length analysis	Cheap process	Works for simple passwords only, less efficiency
lt. Col. Jitender Paul Singh, Dr Mamata, Sunil Kumar	2015	Cloud computing	1.Not required to remember long passwords 2.Provides privacy and confidentially and non-repudiation by symmetric and asymmetric keys	Works for simple passwords and cloud applications
AL Zahra jo Mohammed, Ali. A. Yassin	2019	Iot authentication by multifactor authentication	Proposed protocol is safe and secure against well-known malicious attacks such as eavesdropping and traffic attacks	Designed only based on smart iot mobile devices, time consuming
Subhash Chandra,	2018	Access control using	Proposed	Lengthy

sumit Jaiswal, Ravi Shankar Singh, Jyothi Chauhan		Multifactor authentication in cloud	system and taken steps to implement and provide security was good	process and there can still be a chance of manipulation because of digital OTP generation
Riyadh Abdul Amir, Reham Mustafa, Hazem M.EI. bakry	2016	Authentication using identity detection	The idea of implementing the security by using iris detection is good and it provides some good security	In this methodology they have used only a single pattern of recognition using iris detection, however it is better to have some other options for authentication
Ehinome J. Ikhalia, Dr Chris O. Imafidon	2013	The need for two factor authentications in social media	1.Enchanced security 2.Reduces risk 3.Prevents monetary loss 4.Reduces identity theft 5.Reduces data theft 6.Increases flexibility	1.Costly 2.Inconvenient
Alexandra okada, Denise Whitlock, Wayne Holmes, Chris Edwards	2018	E-authentication for E - education	Strong building methodology for authenticat	Lengthy and costly

			ion in different basis.	
Heather Walker	2017	Digital identity-social media	1. Tokenization 2. Using Restful service end points to facilitate registration	Requires best method of strategy for user credentials security from third party authentication
CA Technologies	2015	CA advanced authentication	1.Reduces the risk of inappropriate access 2.Reduces the risk of employee identity theft 3.Reduces the fraudulent activity	2. Costly and inconvenient.
Aishwarya Mali, Chinmay Mahalle, Mihir Kulkarni, Tejas Nangude, Geeta Navale	2017	Digital authentication and verification on smart phones using CRIPT (cipher random integer procreation and translation) algorithm	Accuracy, efficiency for smart phone, simplicity is high	Security is not too strong, mentioned for mobile only
Sanjoli Single, Jasmeet Singh	2013	Cloud data using authentication and encryption technique	Provides strong security to data with both extensible authenticat	Lengthy process

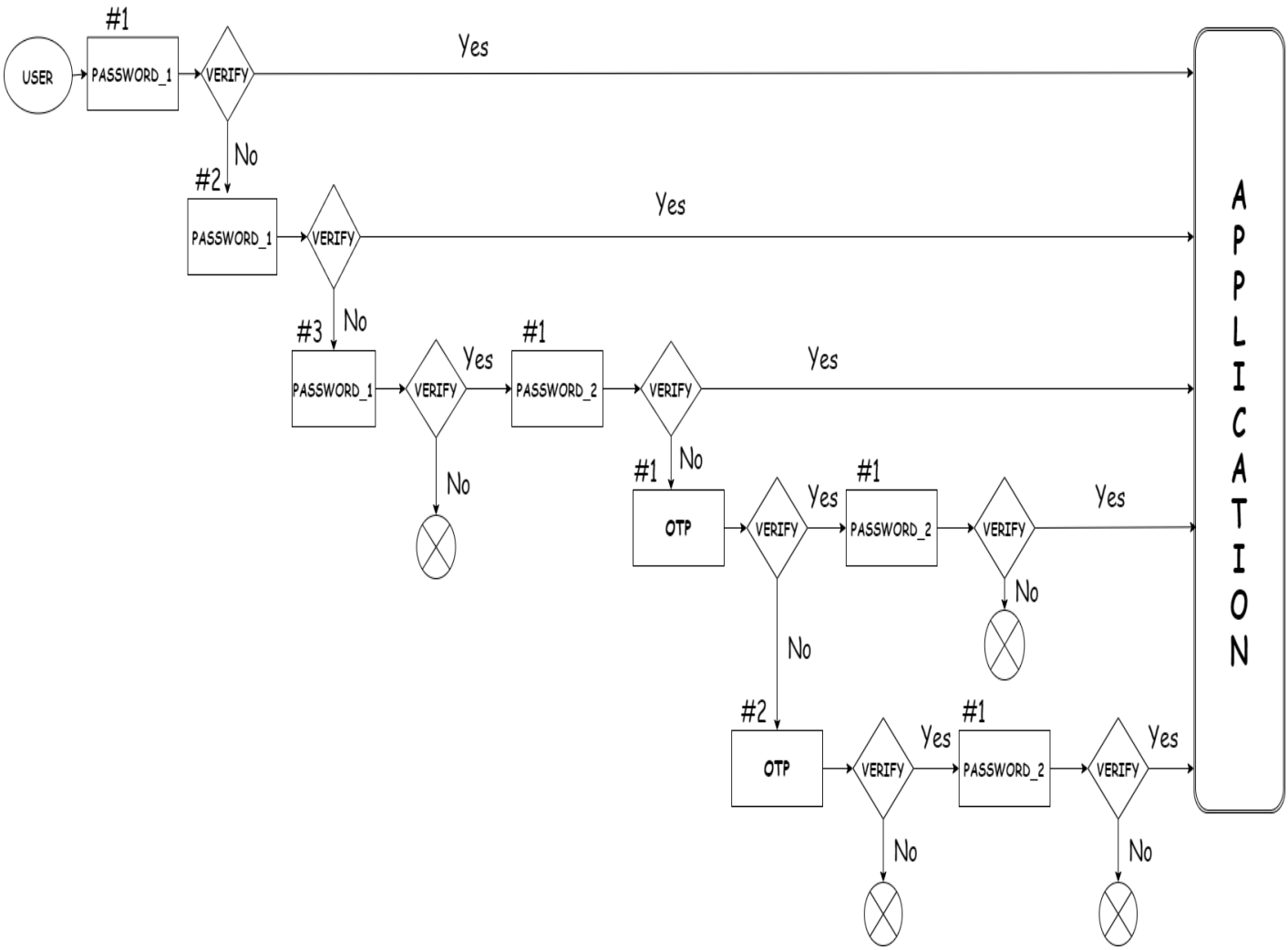
			ion protocol and Rijndael encryption algorithm	
M.Yildirim, Mackie	2019	Improve password security and memorability	The proposed methods are good and efficient	Moderately difficult process
Aleksandr Ometov, Sergey Bezzateev, Niko Makitalo, Sergey Andreev, Tommi Mikkonen, Yevgeni Koucheryavy	2018	Survey: Multi factor authentication	Considering their survey password, token, voice, facial, ocular-based, finger print these authentication methods mostly possess higher – medium significance and behaviour, beam-forming, ocs, ecg, eeg, possess medium to low	1. Poor Task efficiency, age, cognitive abilities etc. 2. Poor probabilistic behaviour 3.Poor security 4.Poor integration 5.Poor robustness 6.Poor privacy

			significance and DNA, hand geometry, location, vein, thermal image are at medium	
Ganorkar, Vyawahare	2018	Graphical password analysis	User friendly and reduces the brute force, dictionary, spyware attacks	Involves in too lengthy process in both registration and as login proceeds
Kalaikavitha.E, Juliana Gnanaselvi	2013	Encrypted OPT	Good idea of implementing user login through mail reading without opt entering	Low accuracy, There may be a chance of third-party user access
Woong Go, Kwang Woo Lee, Jin Kwak	2014	Biometric analysis with password	Best way of designing the authentication process for strong secure and privacy	Very much complex

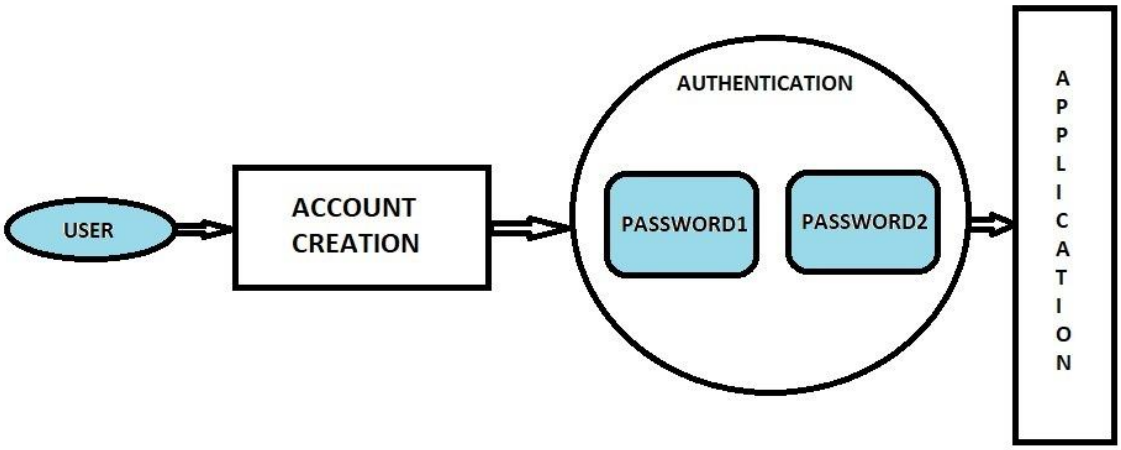
Problem Statement:

As we discussed in above abstract, network security is a must and should aspect in this era. But still inspite of such improved technology, daily we are watching in social media, tv channels, newspapers that several user accounts are being hacked, or some sensitive information is been leaked to wrong people etc. If we still rely on the traditional techniques to tackle above problems/issues it won't be enough to stop them. So new updated techniques are required to overcome this current situation.

Flow Diagram:



Architecture diagram:



Methodology :

We are building a user friendly authentication system, which is easily understandable for every individual and also provides utmost security to their private data.

- In our authentication system, first user will try to attempt a login through his credentials, if he succeeds to enter correct details he will be redirected to his desired application.
- If he fails to enter correct password in his first attempt, he will get another chance of entering details, if he succeeds he will be reaching his desired homepage of application.
- In case of failing to enter his correct password in even second attempt, then he will get a last and final chance of entering right password. In case of third unsuccessful attempt his login page will be closed as he will be considered as an unauthorised user.
- If he enters the correct password in third attempt then in this scenario because of his third attempt he will have to enter his second password (let's consider as password_2) in order to get authorised and access application.

- If he enters his password_2 wrong, then an OTP will be generated to his email and using that OTP only he can get access to the application. In case of entering wrong OTP he will get second chance of entering right OTP which was sent to his email. If he fails he will be considered as unauthorised user.
- If he enters correct OTP then again he will be asked to enter his password_2 to get access.

Codes :

Authentication code

```java
try{
    if (count < 3){
        Class.forName("com.mysql.cj.jdbc.Driver");
        Connection con = DriverManager.getConnection("jdbc:mysql://localhost:3306/authenticationsystem", "root", "shiva@123R");
        PreparedStatement s = con.prepareStatement("select * from userdetails where email = ? and password1 = ?");
        s.setString(1, email);
        s.setString(2, password1);
        ResultSet r = s.executeQuery();
        if(r.next() == true){
            l1.setText("Login successfull");
            Parent root = FXMLLoader.load(getClass().getResource("Home.fxml"));
            Stage stage = (Stage)((Node)event.getSource()).getScene().getWindow();
            Scene scene = new Scene(root);
            stage.setScene(scene);
            stage.show();
            System.out.println("success!");
        }
        else{

            l1.setText("invalid details" + count);
            count = count + 1;
        }
    }
    else if(count == 3){
        Class.forName("com.mysql.cj.jdbc.Driver");
            Connection con = DriverManager.getConnection("jdbc:mysql://localhost:3306/authenticationsystem", "root", "shiva@123R");
            PreparedStatement s = con.prepareStatement("select * from userdetails where email = ? and password1 = ?");
            s.setString(1, email);
            s.setString(2, password1);
            ResultSet r = s.executeQuery();
            if(r.next() == true){
                Parent root = FXMLLoader.load(getClass().getResource("secondLogin.fxml"));
                Stage stage = (Stage)((Node)event.getSource()).getScene().getWindow();
                Scene scene = new Scene(root);
                stage.setScene(scene);
                stage.show();
            }
            else{
```

OTP generation code

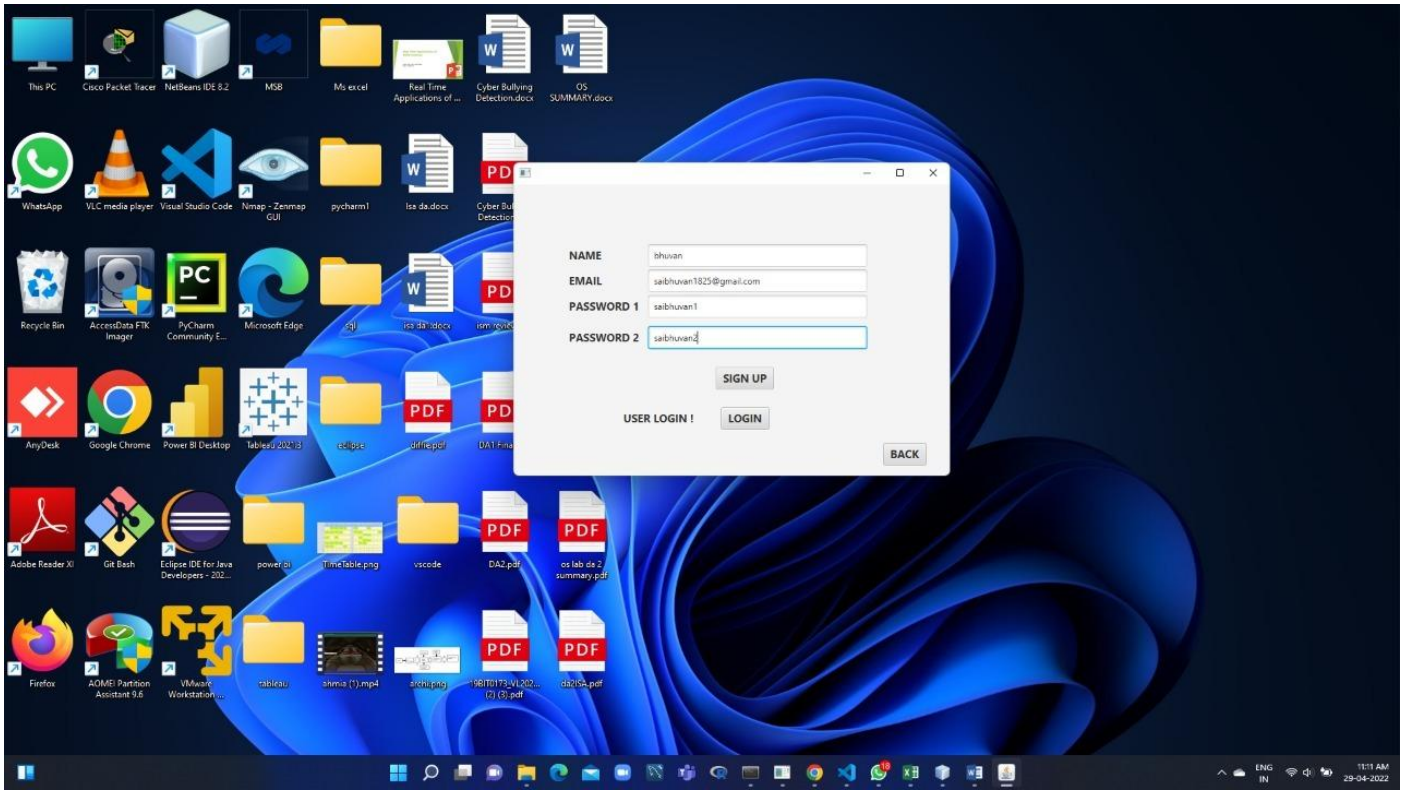
```java
String otp_s = otp_t.getText();
System.out.println("otp_s: " + otp_s);
if(otp_t.getText().isEmpty()){
    msg_l.setText("otp required");
}
if(count < 3){
    if(otp_s.equals(sbf.toString())){
        Parent root = FXMLLoader.load(getClass().getResource("finalLogin.fxml"));
        Stage stage = (Stage)((Node)event.getSource()).getScene().getWindow();
        Scene scene = new Scene(root);
        stage.setScene(scene);
        stage.show();
    }
    else{
        count = count + 1;
        msg_l.setText("invalid OTP -" + count);
    }
}
else{
    count = count + 1;
    System.exit(0);
}
}

public static char[] generateOTP(){
    int len = 6;
    int count = 1;
    char[] otp = new char[len];
        String Capital_chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
        String Small_chars = "abcdefghijklmnopqrstuvwxyz";
        String numbers = "0123456789";
        String symbols = "!@#$%^&*_=+-/.?<>)";

        String values = Capital_chars + Small_chars + numbers + symbols;

        // Using random method
        Random rndm_method = new Random();

        for (int i = 0; i < len; i++){
```

Second password authentication

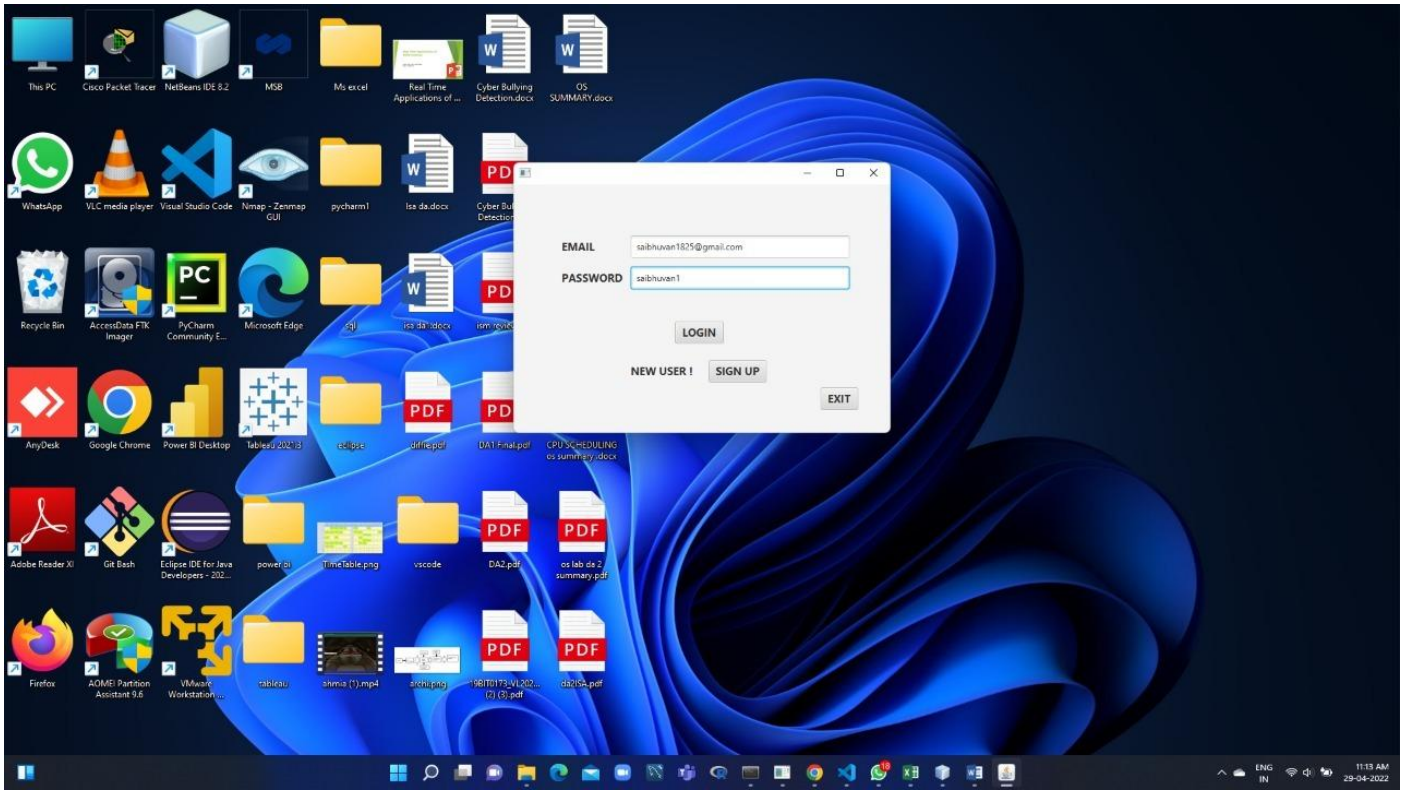
```java
    @FXML
    private void getLogin(ActionEvent event) {
        String password2 = password2_t.getText();
        if(password2_t.getText().isEmpty()){
            l1.setText("required password");
        }
        if(count < 2){
            try{
                Class.forName("com.mysql.cj.jdbc.Driver");
                Connection con = DriverManager.getConnection("jdbc:mysql://localhost:3306/authenticationsystem", "root", "shiva@123R");
                PreparedStatement s = con.prepareStatement("select * from userdetails where password2 = ?");
                s.setString(1, password2);
                ResultSet r1 = s.executeQuery();
                if(r1.next() == true){
                    l1.setText("Login successfull");
                    Parent root = FXMLLoader.load(getClass().getResource("Home.fxml"));
                    Stage stage = (Stage)((Node)event.getSource()).getScene().getWindow();
                    Scene scene = new Scene(root);
                    stage.setScene(scene);
                    stage.show();
                    System.out.println("success!");
                }
                else{
                    count = count + 1;
                    Parent root = FXMLLoader.load(getClass().getResource("OTP.fxml"));
                    Stage stage = (Stage)((Node)event.getSource()).getScene().getWindow();
                    Scene scene = new Scene(root);
                    stage.setScene(scene);
                    stage.show();
                }
            }
            catch(Exception e){
                System.out.println(e);
            }
        }
    }
}
```

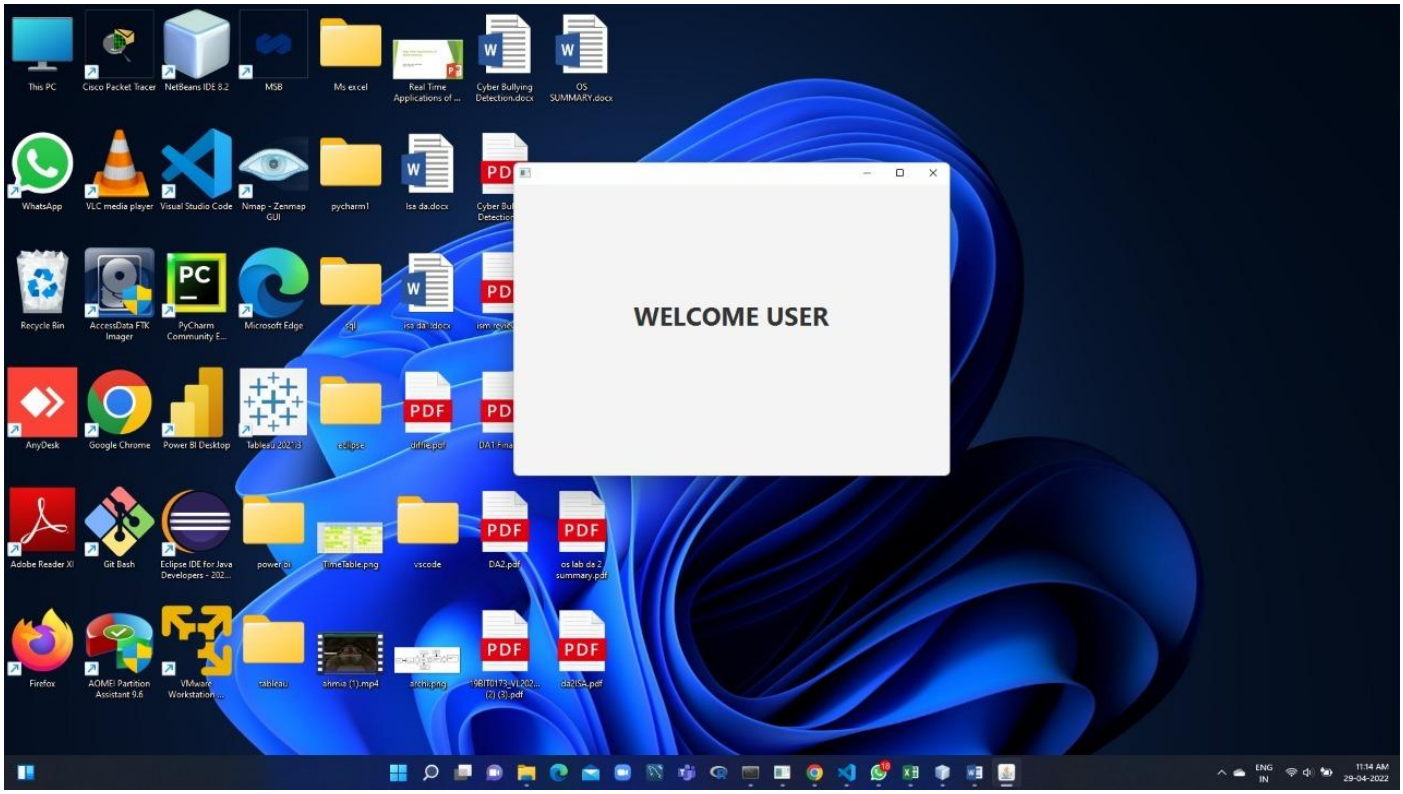
Results (Snapshots):

Creating new user:

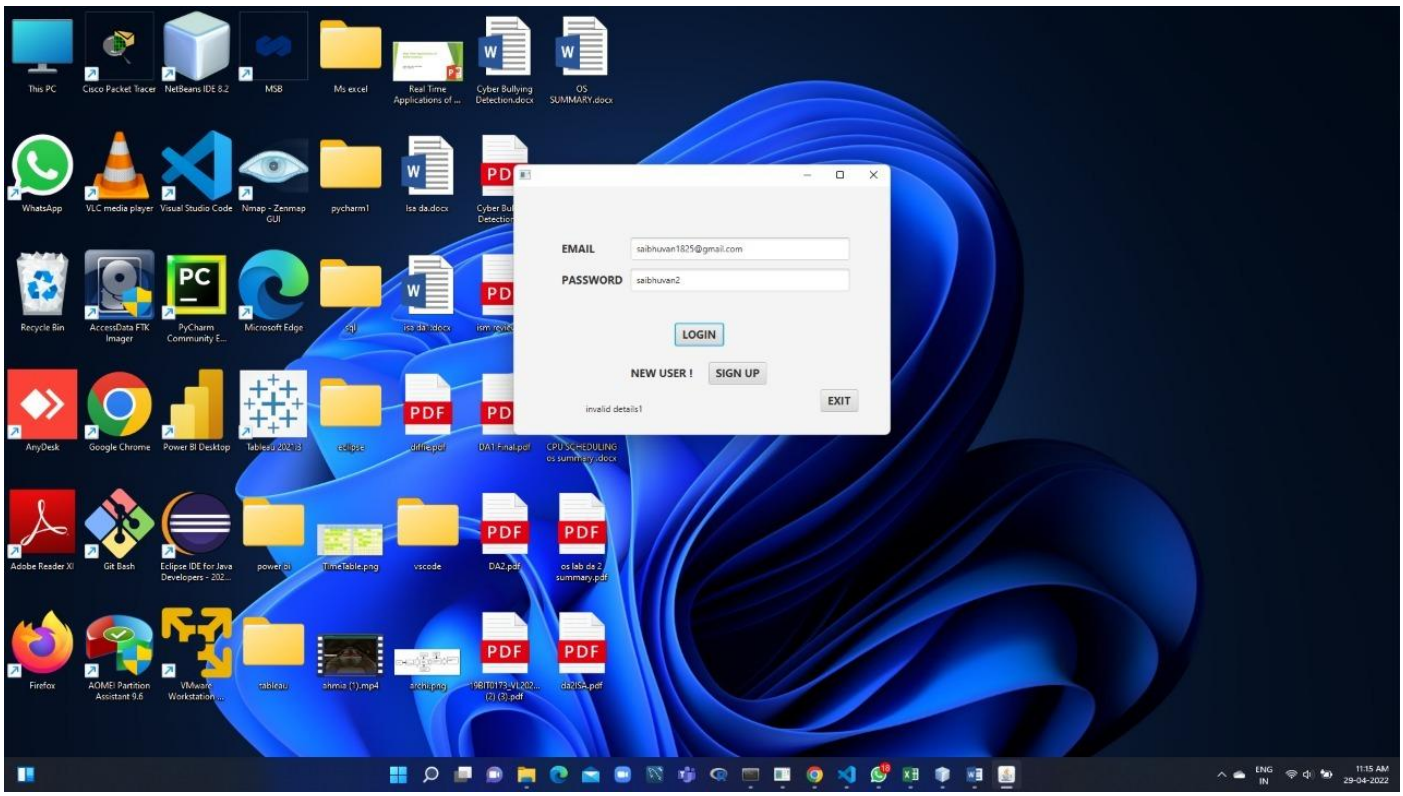


System will give you 2 chances to enter correct password:

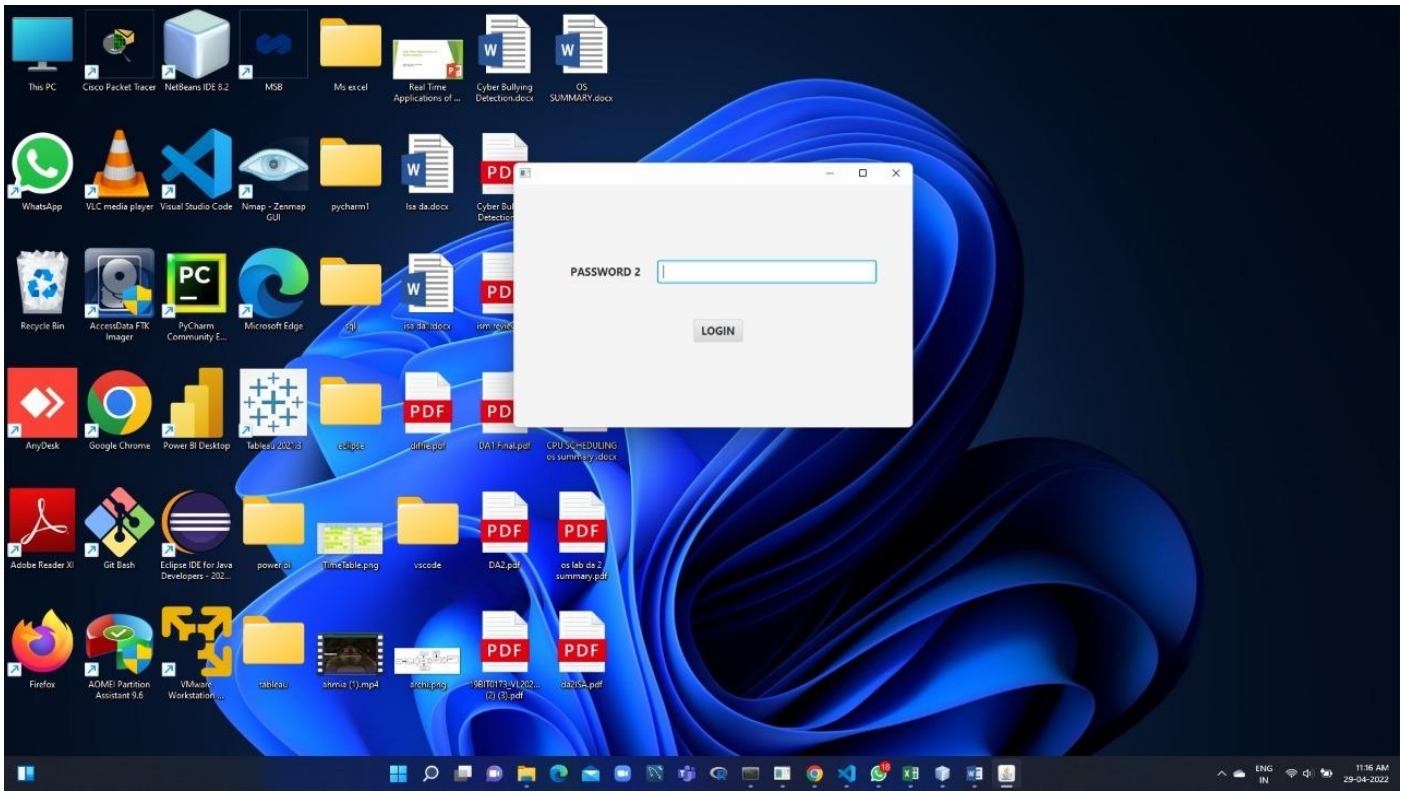


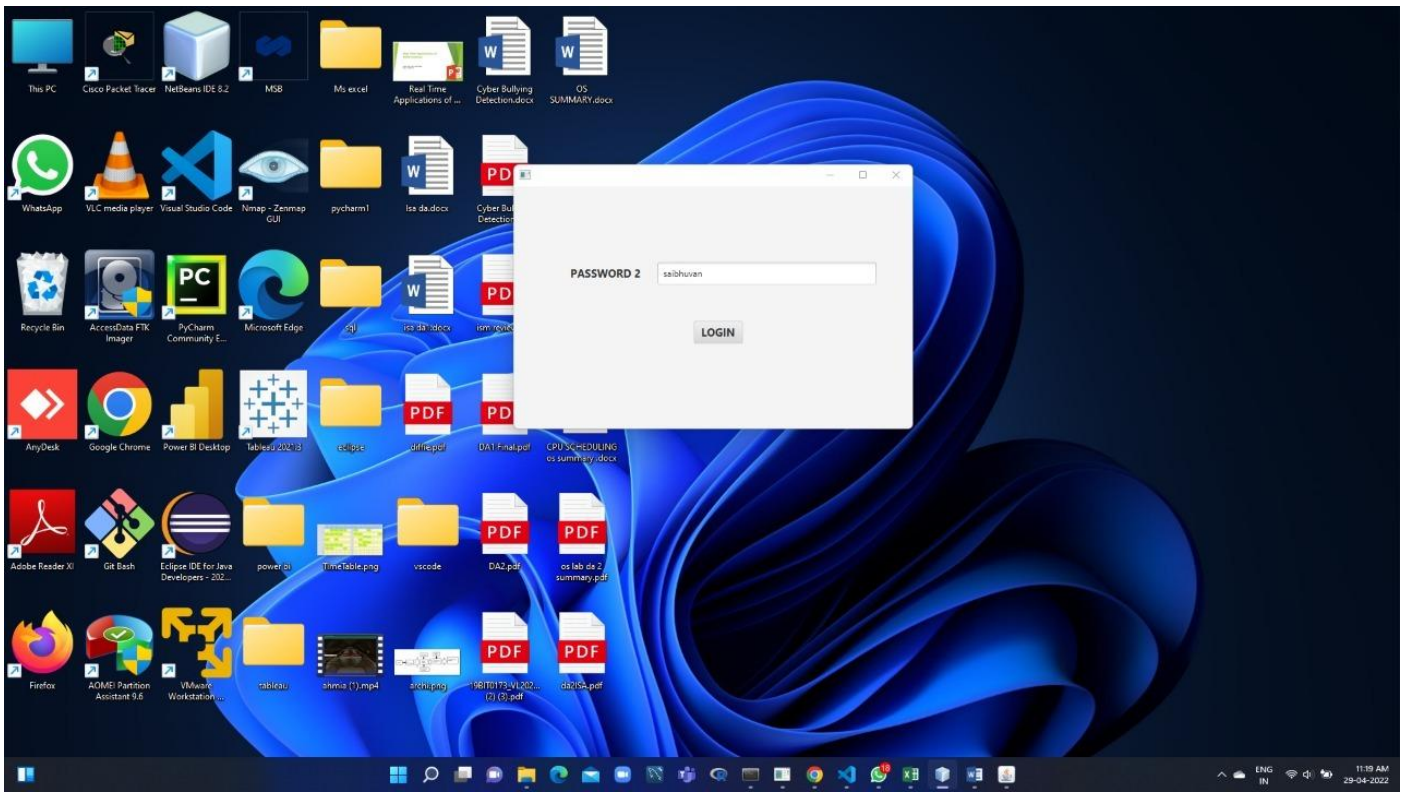


If you enter wrong password in your first two attempts system will display “Invalid details!” as shown below:

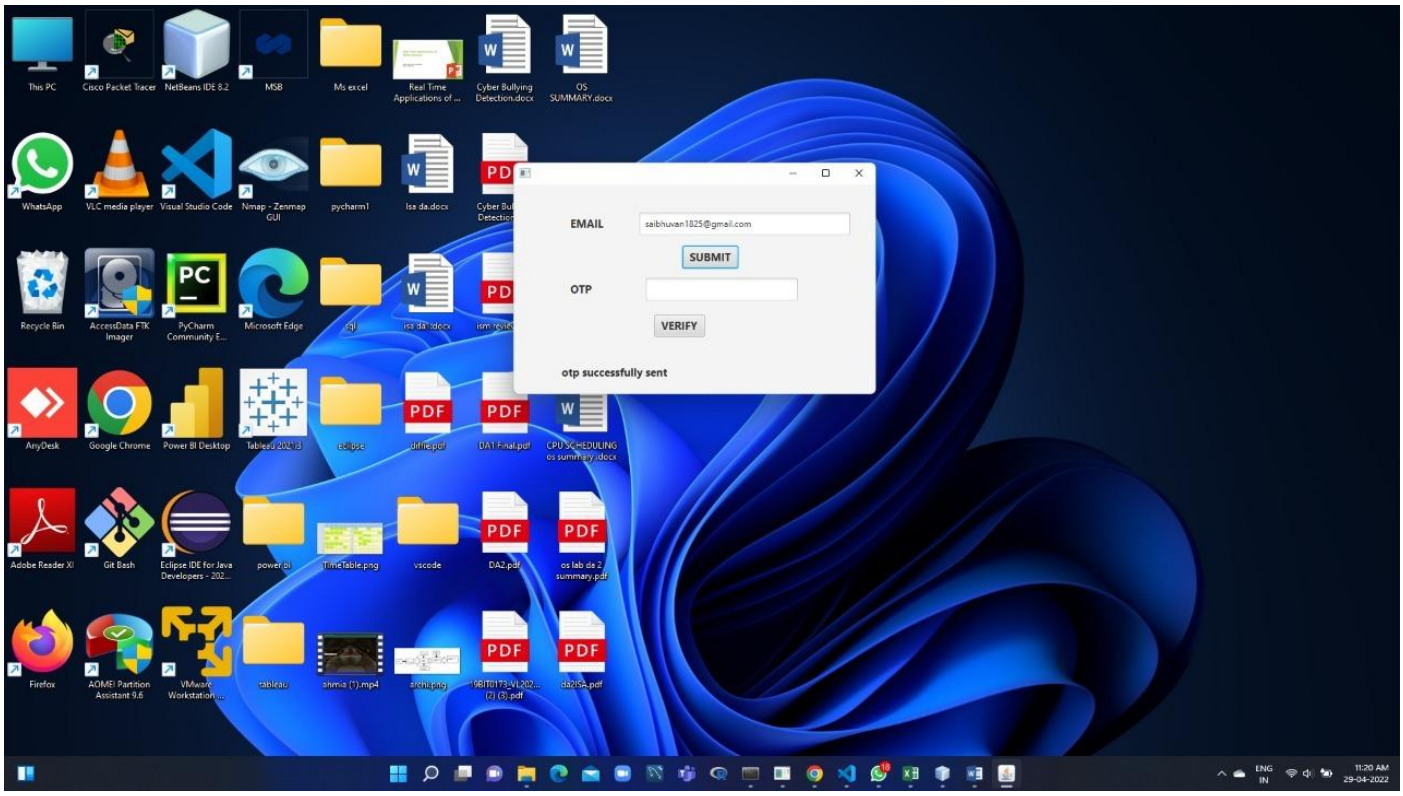


If you enter your correct password in your third attempt then system will ask to enter our second password (Password 2):

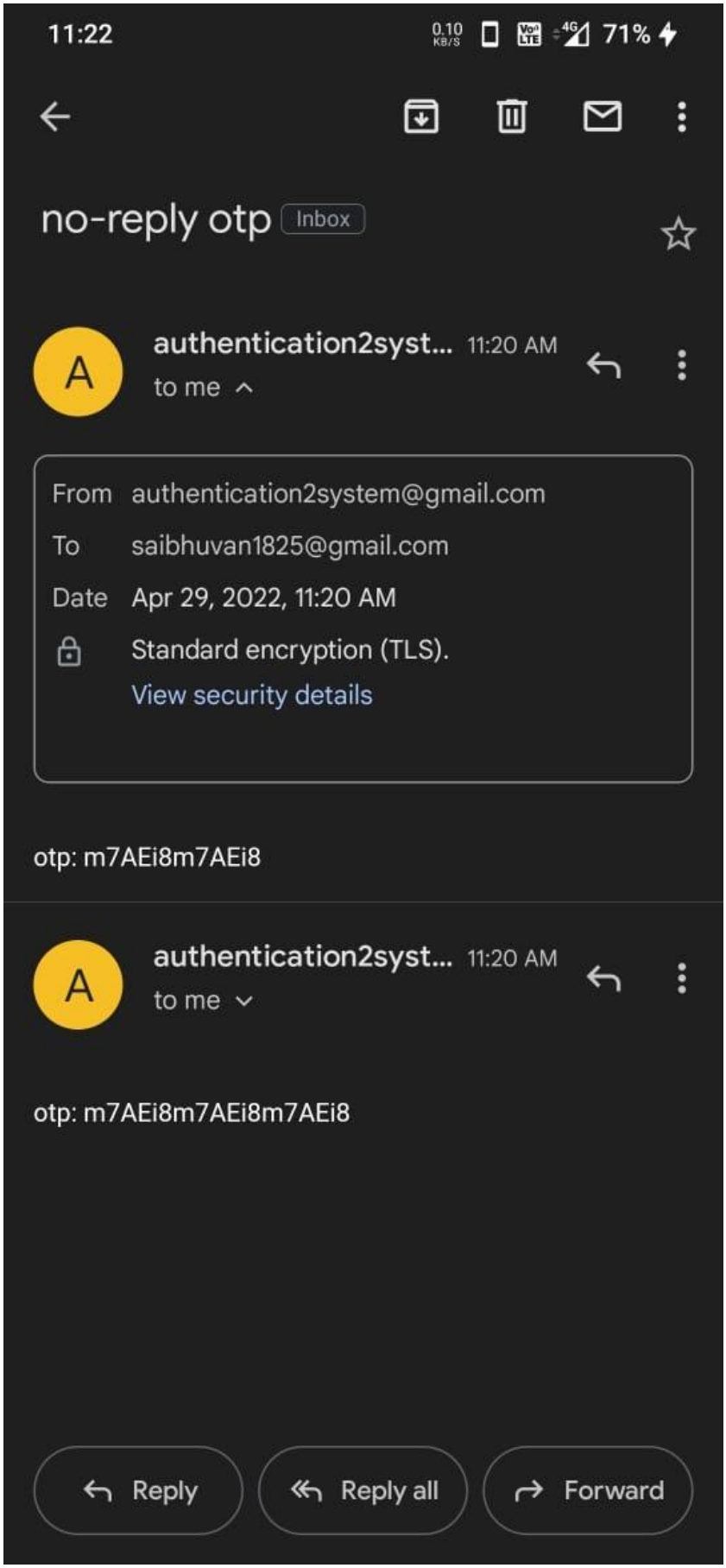




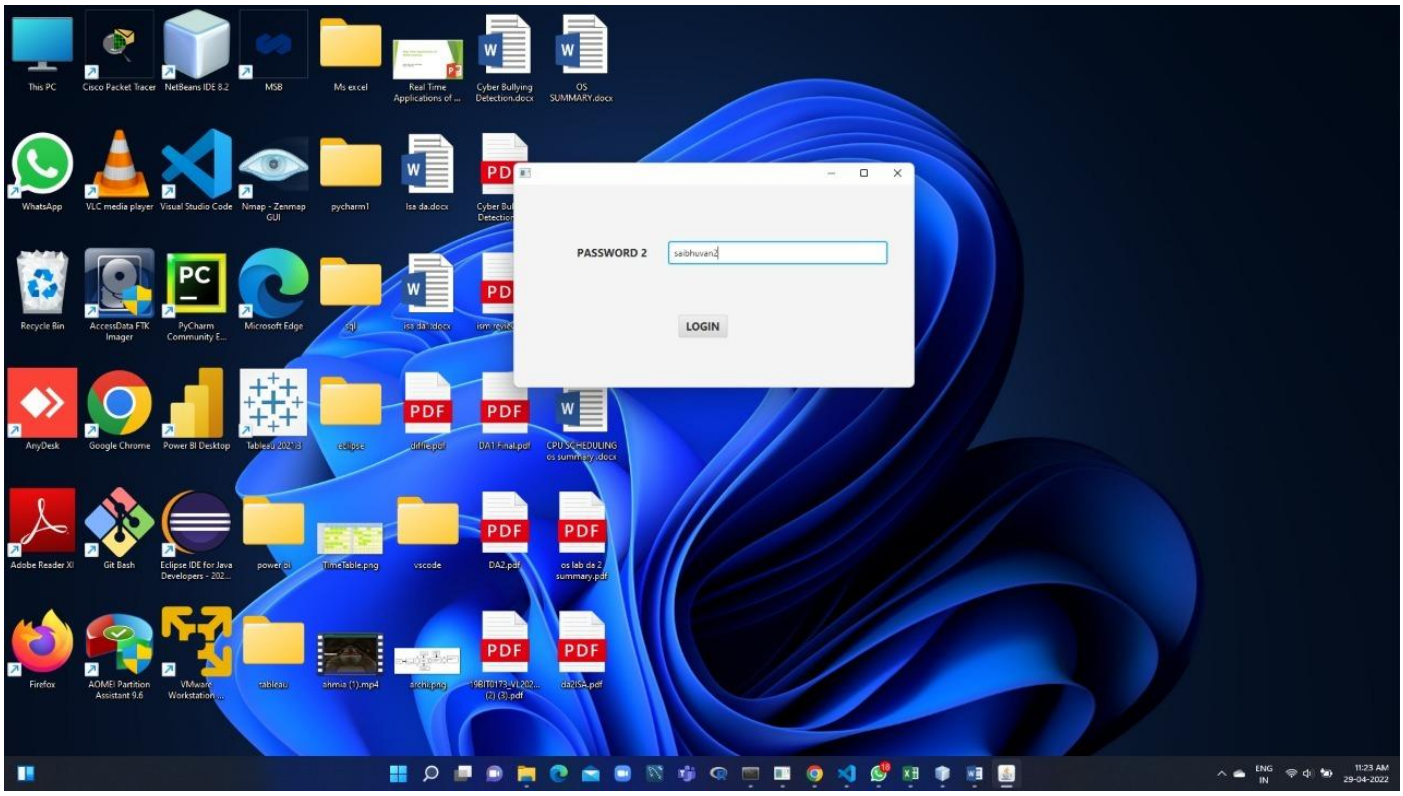
If you fail to enter your correct Password 2 then an OTP will be sent to the email address which you'll provide.

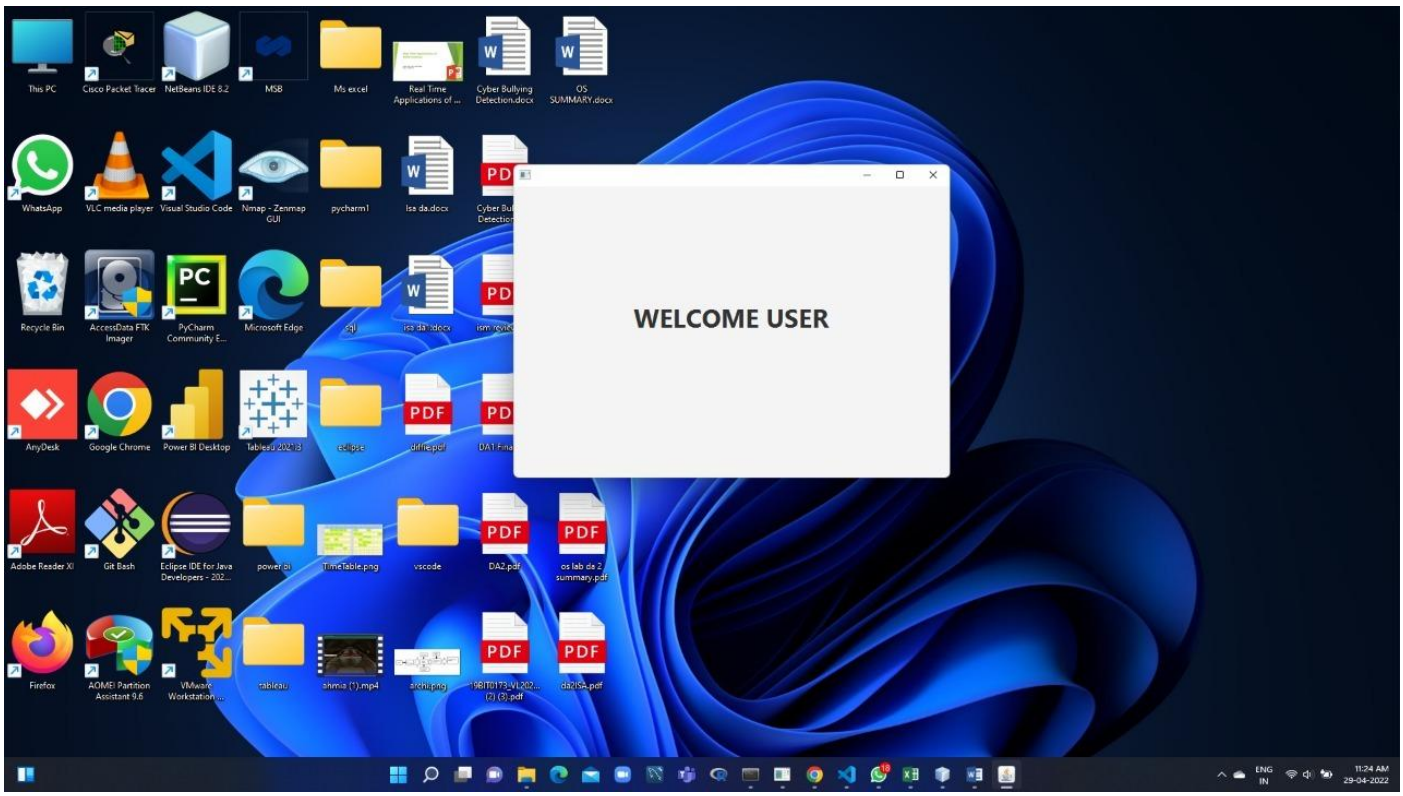


As we can see an OTP is sent successfully to the provided email address (saibhuvan1825@gmail.com) from email address (authentication2system@gmail.com)



Then as above said user have to again enter his Password 2 in order to get access to his desired application:





Conclusion & Future Work:

As we have discussed above about the importance of the strong and secure authentication system, we tried to develop a user friendly authentication system. In the developed system we have added the aspect of second password for authentication.

And we also incorporated the concept of OTP (One Time Password) generation to the user's registered email. Made the system in such a way that the user can get authenticated to access the application if and only he enters his OTP and second password correctly.

As a, part of our project , in future we would like to develop more secure features to our authentication system by using encryption techniques and by considering more secure standard techniques.

References:

[1] https://www.newamerica.org/oti/reports/evaluating-digital-standard-methodology/

[2] https://link.springer.com/article/10.1007/s10845-012-0669-y?noAccess=true

[3] https://issuu.com/researchinventy/docs/c0210014017/1

[4]https://www.ijmh.org/wp-content/uploads/2017/08/Abstarct_Book_IJEAT_v4i4_April_2015.pdf

[5] https://link.springer.com/article/10.1007/s10207-019-00429-y

[6] https://core.ac.uk/download/pdf/231151959.pdf

[7]https://www.researchgate.net/publication/347617665_Low-cost_fitness_and_activity_trackers_for_biometric_authentication

[8]https://www.researchgate.net/publication/347617665_Low-cost_fitness_and_activity_trackers_for_biometric_authentication

[9]https://link.springer.com/referenceworkentry/10.1007/978-94-024-1555-1_34?noAccess=true

[10] https://www.tru.ca/its/infosecurity/mfa.html