##### IMPROVED SESSION PASSWORD BASED SECURITY SYSTEM

**A PROJECT REPORT**

###### ***Submitted by***

##### ANSHU VERMA (19BCY10021)

**SUBHIKSHA S. (19BCY10123)**

##### RISHABH MAHESHWARI (19BCY10145)

##### CHINNAM SHIMONA CAROLINE (19BCY10165)

*in partial fulfillment for the award of the degree*

*of*

##### BACHELOR OF TECHNOLOGY

*in*

**COMPUTER SCIENCE AND ENGINEERING**

**(specialization in Cyber Security and Digital Forensics)**

****

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRI KALAN, SEHORE**

**MADHYA PRADESH - 466114**

JANUARY,2022

**BONAFIDE CERTIFICATE**

This project report titled **“IMPROVED SESSION PASSWORD BASED SECURITY SYSTEM”** is the bonafide work of “Anshu Verma ( Register No. :19BCY10021), Subhiksha S.(Register No. :19BCY10123),Rishabh Maheshwari (Register No.: 19BCY10145) and Chinnam Shimona Caroline (Register No.: 19BCY10165) **”** 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 PROJECT GUIDE**

Dr. R Rakesh ,Assistant Professor Dr. Vikas Panthi

School of Computer Science and Engineering School of Computer Science and Engineering

VIT BHOPAL UNIVERSITY VIT BHOPAL UNIVERSITY

**ACKNOWLEDGEMENT**

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

We wish to express our heartfelt gratitude to Dr. R. Rakesh, Program Chair - Cyber Security and Digital Forensics for much of his valuable support and encouragement in carrying out this work.

We would like to thank our internal guide Dr. Vikas Panthi, for continually guiding and actively participating in our project, giving valuable suggestions to complete the project work.

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

Last, but not least, We are deeply indebted to our parents who have been the greatest support while we worked day and night for the project to make it a success.

**LIST OF FIGURES AND GRAPHS**

| **FIGURE NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
|  | **System Architecture** | **13** |
| **2.** | **UML Diagram** | **14** |

**ABSTRACT**

Nowadays, data security and recovery are the most important aspects of cyber security. There are many applications where login is required. This means that there is important user data connected with it. This is where two-factor authentication comes in. This ensures that the actual user is logging into its account and not some other person.Our application uses username and a password for the first step of login and an otp (which is sent to the registered mobile number) for the second step. After that the user can select which applications to lock. The locked applications will require a similar two factor authentication process to open. This way only the authorized or authentic user is able to use the application.

**TABLE OF CONTENTS**

| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
|  | List of Figures and Graphs  Abstract | 4  6 |
| 1 | **CHAPTER-1:**  **PROJECT DESCRIPTION AND OUTLINE** Introduction 1.2 Motivation for the work  1.3 [About Introduction to the project  including techniques]  1.5 Problem Statement  1.6 Objective of the work  1.7 Organization of the project  1.8 Summary | 7 |
| 2 | **CHAPTER-2:**  **RELATED WORK INVESTIGATION**  2.1 Introduction  2.2 <Core area of the project>  2.3 Existing Approaches/Methods  2.4 Summary | 9 |
| 3 | **CHAPTER-3:**  **REQUIREMENT ARTIFACTS**  3.1 Introduction  3.2 Hardware and Software requirements  3.4 Summary | 11 |
| 4 | **CHAPTER-4:**  **DESIGN METHODOLOGY AND ITS NOVELTY**  4.1 Methodology and goal | 12 |
| 5 | **CHAPTER-5:**  **TECHNICAL IMPLEMENTATION & ANALYSIS**  5.1Outline  5.2 Technical coding  5.3 Coding Solutions  5.4 Summary | 15 |
| 6 | **CHAPTER-6:**  **PROJECT OUTCOME AND APPLICABILITY**  6.1Outline  6.2 key implementations outlines of the System  6.3 Significant project outcomes  6.4 Project applicability on Real-world applications  6.4 Inference | 20 |
| 7 | **CHAPTER-7:**  **CONCLUSIONS AND RECOMMENDATION**  7.1Outline  7.2 Limitation/Constraints of the System  7.3 Future Enhancements  7.4 Inference | 21 |
|  | **References** | 22 |

**CHAPTER - 1**

**PROJECT DESCRIPTION AND OUTLINE**

**1.1 Introduction**

One-time passwords (OTPs) have become quite familiar in recent times, mainly due to a security requirement that traditional passwords do not guarantee. While the protection of the traditional password is the responsibility of the user,who as we well know often does not care enough, the OTP is practically self-protected because it is generated randomly, and its validity is limited in time.

You can use OTPs instead of traditional passwords, or to reinforce the traditional authentication process with a two-factor authentication (2FA) approach. Actually, you can use OTPs wherever you need a mechanism that ensures a user's identity by relying on a communication medium owned by himself: amailbox, a phone, a specific app, etc.

**1.2 Motivation for the work**

This type of verification ensures that no one other than the actual user can see the information on the applications. This is important because nowadays mobile applications contain a lot of personal information specially social media apps. It can prevent other people from using your social media accounts.

**1.3 About Introduction to the project including techniques**

One-time password (OTP) systems provide a mechanism for logging on to a network or service using a unique password that can only be used once, as the name suggests.The OTP feature prevents some forms of identity theft by making sure that a captured user name/password pair cannot be used a second time.

Typically the user's login name stays the same, and the one-time password changes with each login. One-time passwords (aka One-time passcodes) are a form of strong authentication, providing much better protection to [eBanking](https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking), corporate networks, and other systems containing sensitive data. Authentication answers the question: "Are you indeed Mr or Mrs. X?"​ Today most enterprise networks, e-commerce sites, and online communities require only a user name and static password for login and access to personal and sensitive data.

**1.4 Problem Statement**

Normally entering username and password is one layer of protection and anyone can breach it easily. So to avoid this king of breaching we made this two layer protection.This double layer protection helps us to lockout selected apps and taken under this two layer protection so that even there is any breach then it will not be easy to pass through it

**1.5 Objective Of the work**

Online transactions as well as social medias and apps are rife with security threats.With the availability of powerful password cracking software, even novice users can now crack thousands of passwords in a very short time, typically hours

Other attacks that enable unauthorized access to web applications and result in identity thefts include phishing attacks, pharming attacks, and various social engineering techniques. The existence of such threats behooves web applications to use defense in depth and implement at least a second factor of authentication to protect against intruders. This is where we come in.

**1.6 Summary**

We are contributing to open source as this app is free. The application works with all apps where API is available and Integrable. It helps users to login into their account more securely. Any stalker won’t be able to collect the password via shoulder surfing.Complex password technique is used along with character matrix with easy user interface.

**CHAPTER - 2**

**RELATED WORK AND INVESTIGATION**

**2.1 Introduction**

* Simple methods such as transaction number lists and grid cards can provide a set of one-time passwords. These methods offer low investment costs but are slow, difficult to maintain, easy to replicate and share, and require the users to keep track of where they are in the list of passwords.
* A more convenient way for users is to use an [OTP token](https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/tokens), a hardware device capable of generating one-time passwords. There's more. Some of these devices are PIN-protected, offering an additional level of security. The user enters the one-time password with other identity credentials (typically username and password), and an authentication server validates the login request. Although this is a proven solution for enterprise applications, the deployment cost can make the solution expensive for consumer applications. Because the token must be using the same method as the
* server, a separate token is required for each server logon, so users need a different token for each Web site or network they use.
* More advanced hardware tokens use microprocessor-based smart cards to calculate one-time passwords. [Smart cards](https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/smart-cards-basics) have several advantages for strong authentication, including data storage capacity, processing power, portability, and ease of use. They are inherently more secure than other OTP tokens because they generate a unique, non-reusable password for each authentication event, store personal data, and do not transmit confidential or private data over the network. [Display payment cards](https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/payments/display-interface) can even integrate an OTP generator for 2-factor authentication.

**2.2 Core Area of the project**

Two-factor authentication is used by :

### Finance -The finance industry has long used 2FA technology. In fact, each time you use an ATM, you are using 2 - Factor Authentication—you need both your PIN (something you know) and your ATM card (something you have) to access your bank account. As more financial services become online, financial organizations need this added layer of security to protect customers and their assets.

### Government - For several years, 2 - Factor Authentication has been a [mandatory requirement for accessing government websites](https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan).

**2.3 Existing Methods**

Method -1 : Session Based Authentication:

Advantages: Cookies are small-sized values, easy to use and implement.

Disadvantages: Cookies are prone to XSS and CSRF attacks and the sessions are stored in the server’s memory. Thus scaling becomes an issue when a large number of users log in.

Method -2 : Token Based Authentication:

Advantages: A token is stored on the client-side, so there is no problem with scaling and there is no need to store session information in the server.

Disadvantages: Since JWT contains more user information, the size of JWT is much bigger when compared with the session ID stored in a cookie and it can’t revoke access to a user.

Method -3 : One-Time Password (OTP):

Advantages: SMS based token. Secured as they are encrypted by network providers. Save development time and cost.

Disadvantages: Rely on mobile network carrier, Difficult to find OTP, Tedious retyping.

**2.4 Summary**

Above is explained our research or investigation about the project which we are doing and also the already existing work and we took those existing works into consideration and try to add unique features to it

**CHAPTER -3**

**REQUIREMENT ARTIFACTS**

**3.1Introduction**

Software and Hardware requirements are the essential parts for the implementation of a project model. Here, we used Android studio for the application coding and Java is the programming language used.

**3.2 Hardware and Software requirements**

Software Requirements:

1. Eclipse
2. Android Studio
3. Github
4. Java and XML

App Integration:

1. SDK and API Keys
2. Firebase Service

**3.4 Summary**

This information explained all about the minimum hardware and software requirements for running the project.

**CHAPTER-4:**

**DESIGN METHODOLOGY AND ITS NOVELTY**

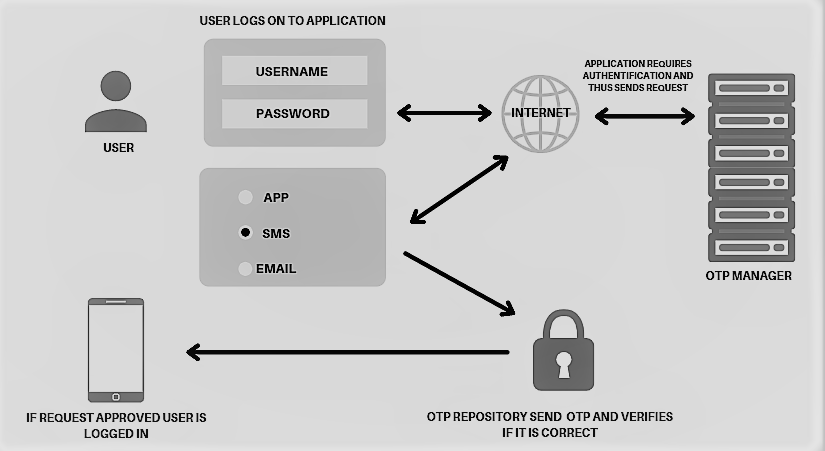
**4.1 Methodology and goal**

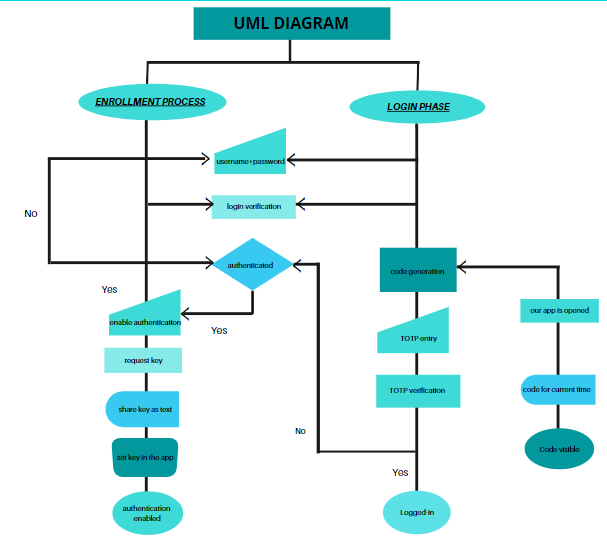
The user first makes an account using an email address and a mobile number. When the user needs to lock the applications , he will need his username, password and his mobile phone to access the application. He will then be able to decide which apps to lock. To open the locked applications, the user will have to undergo the 2 process login mentioned above.

**4.2 Functional modules design and analysis**

Once you have the project’s code on your computer, you need to install its dependencies by moving into the project’s folder and typing the following command: npm install It will then allow you to assign phone numbers and/or links to external accounts for services like Messenger, WhatsApp, or Viber so that you can send SMS or messages through the Message andDispatch API.Once you have configure, you have to configure the OTP serviceside in order to make them communicate with each other.Now,It’s time to run your OTP service.If everything is OK, you should see the message “This is the OTP service”.The OTP service will generate an OTP composed of 5 digits and will send it to the specified Messenger identifier. If the user does not read it within a given amount of time, the OTP will be sent via SMS to the phone number. Regardless of the medium by which the message was received,the user should verify the OTP by submitting a GET request to the second API

**4.3 Software Architectural designs**

****

****

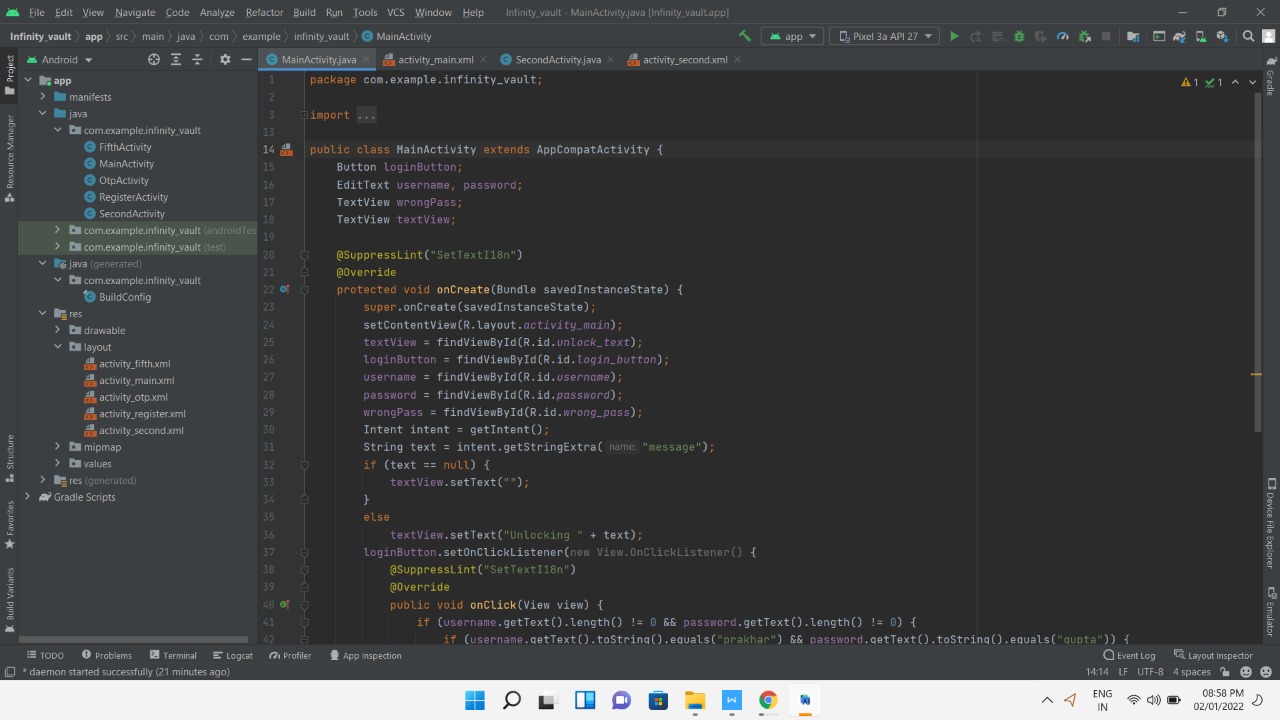
**CHAPTER-5:**

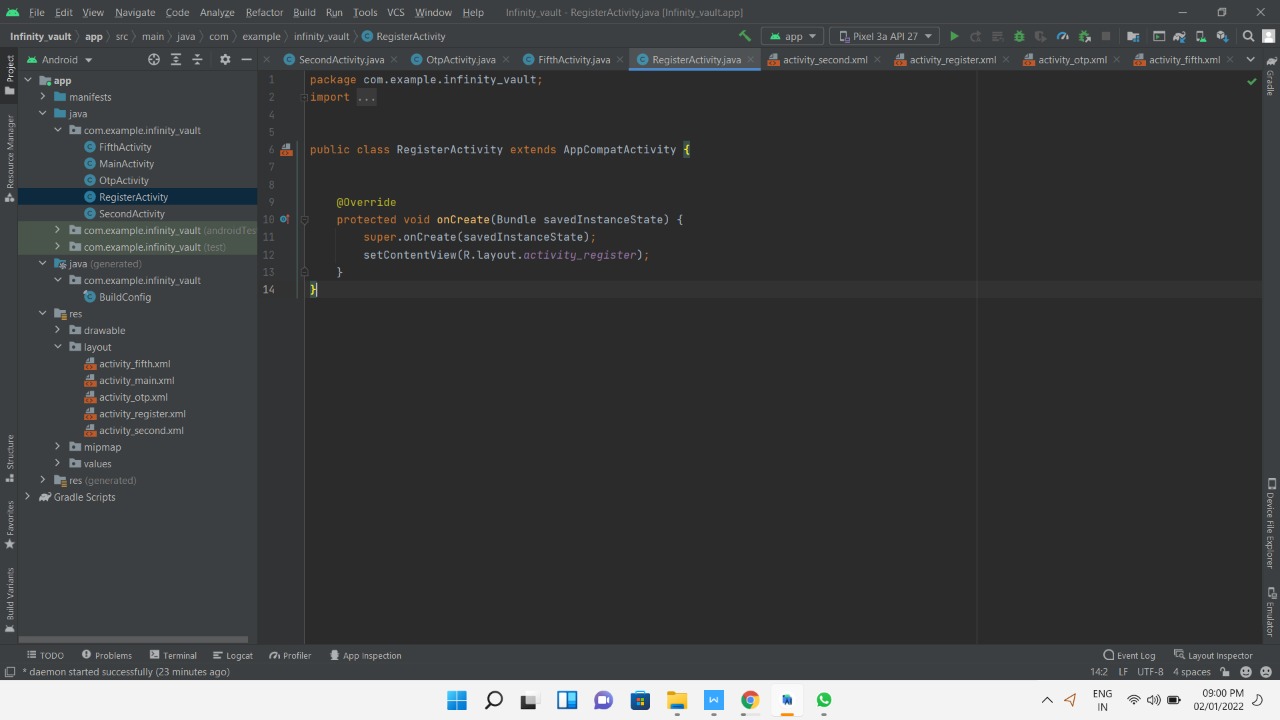
**TECHNICAL IMPLEMENTATION & ANALYSIS**

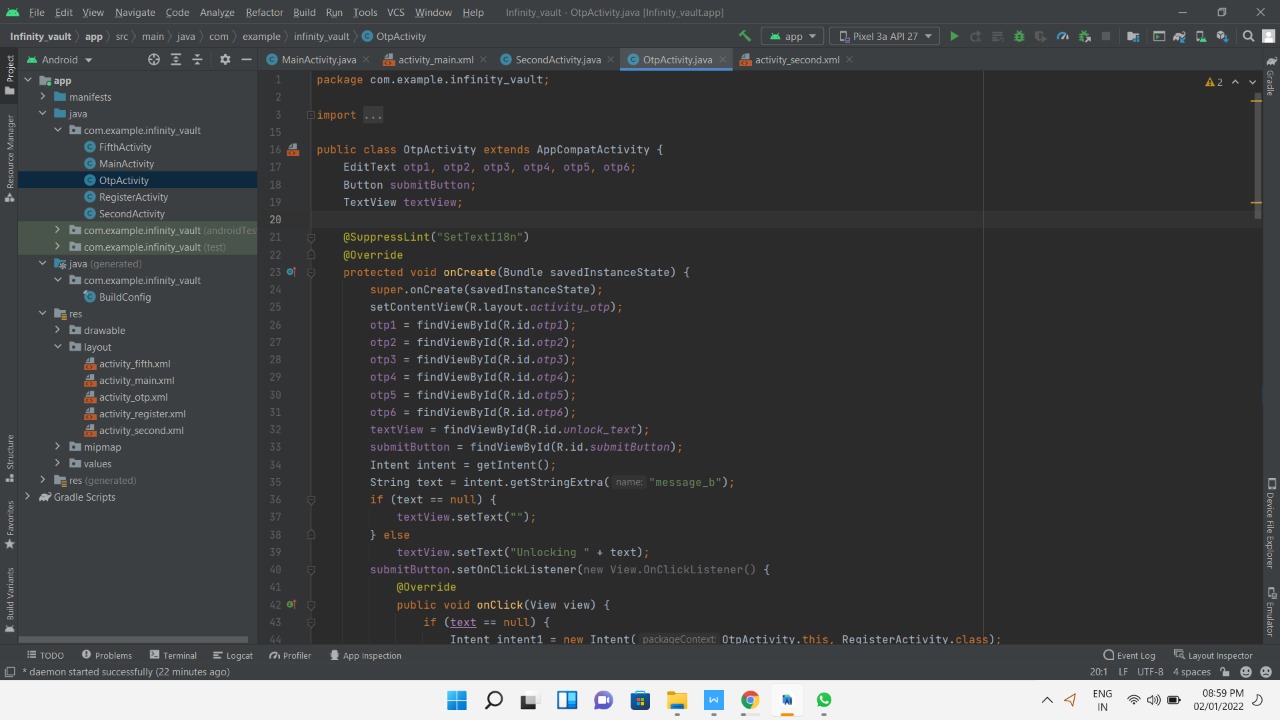
**5.1 Outline**

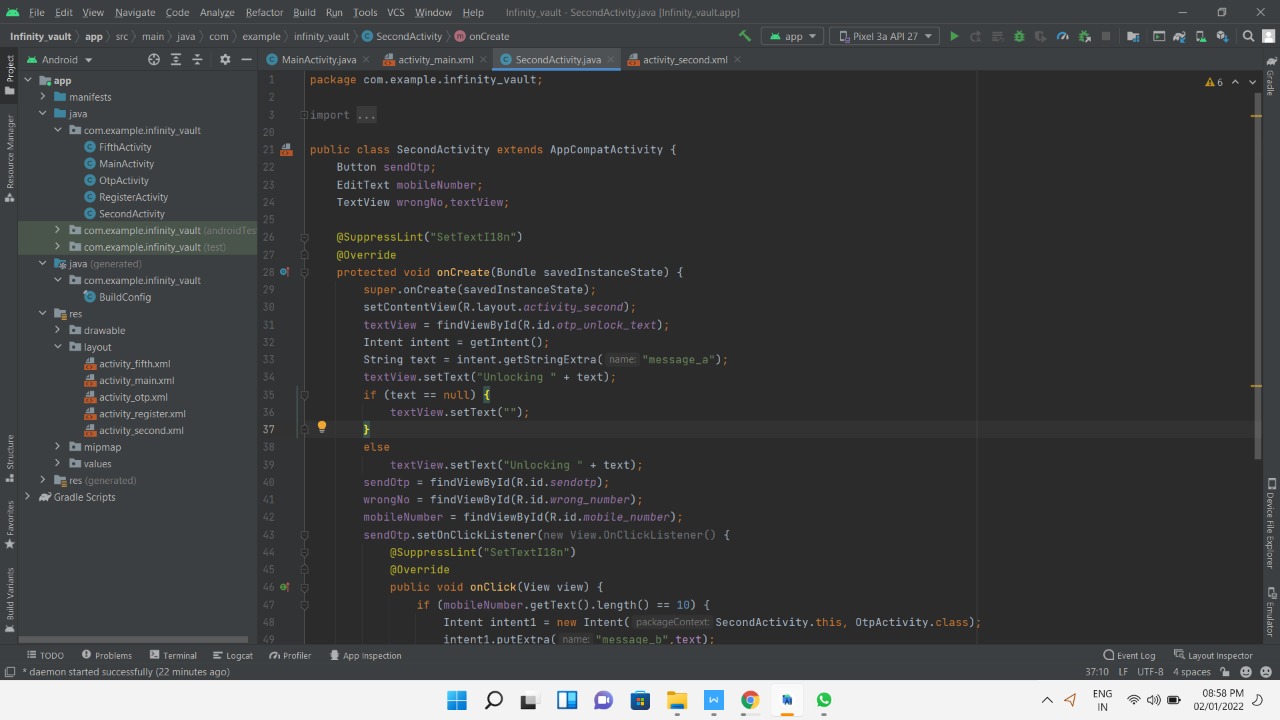
The app will ask the user whether to login or signup. It will then ask the user to verify the account using an otp. After the verification is done the user will be able to use the application.

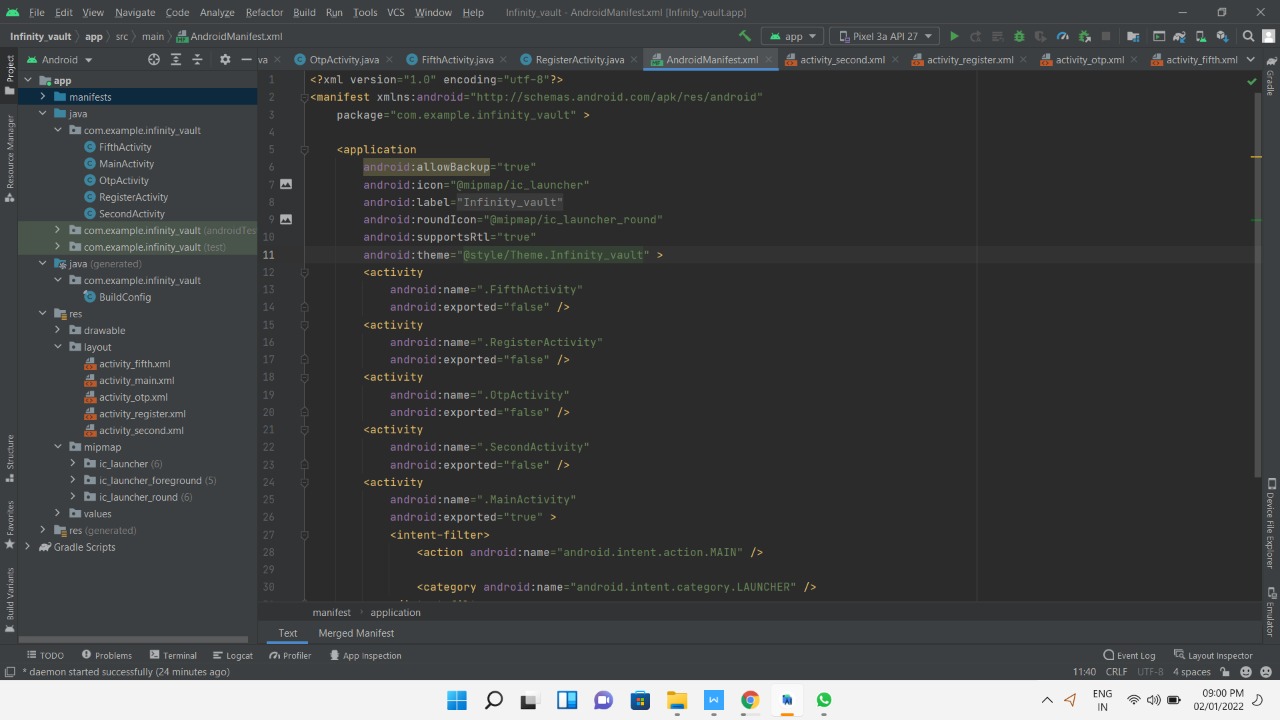
**5.2 Technical coding**

****

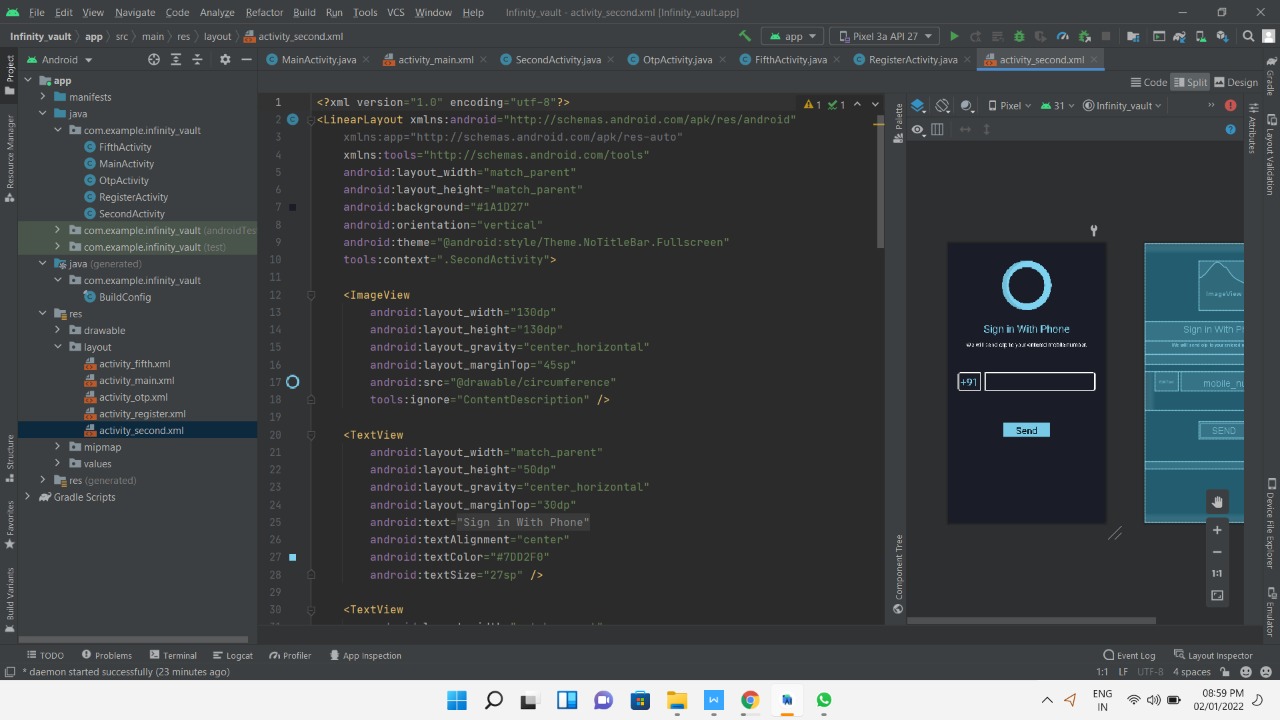
****

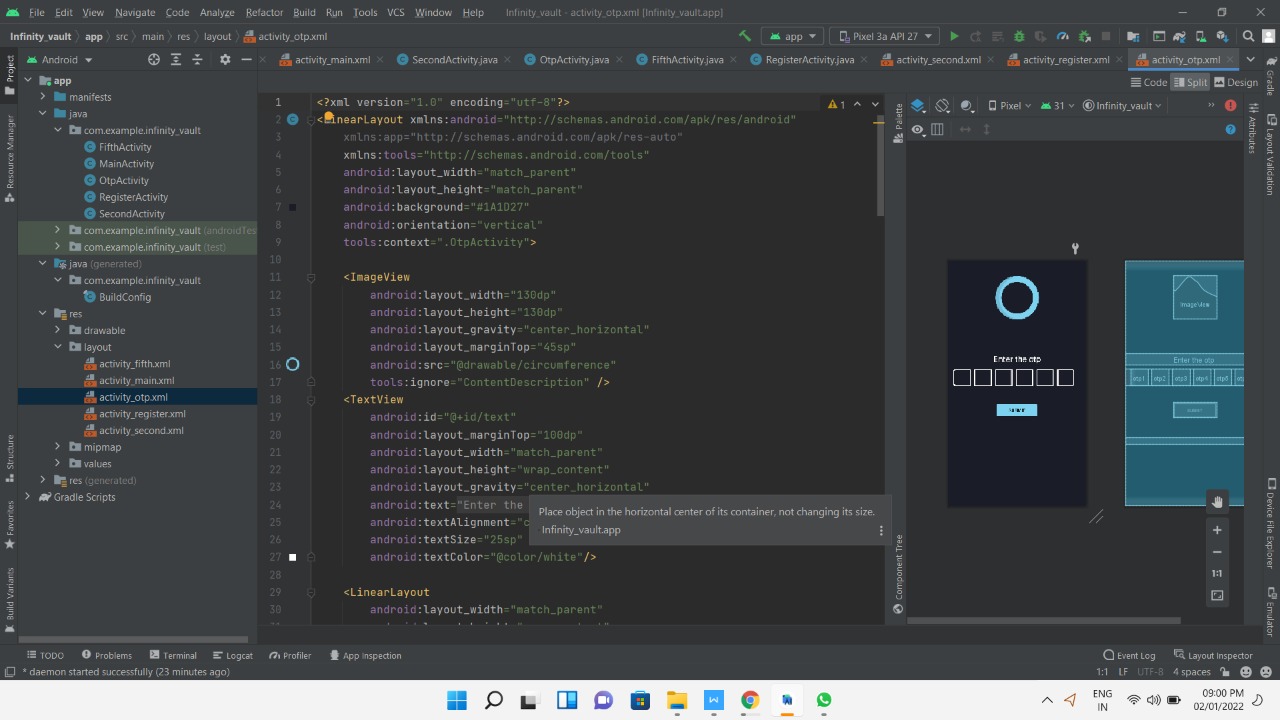
****

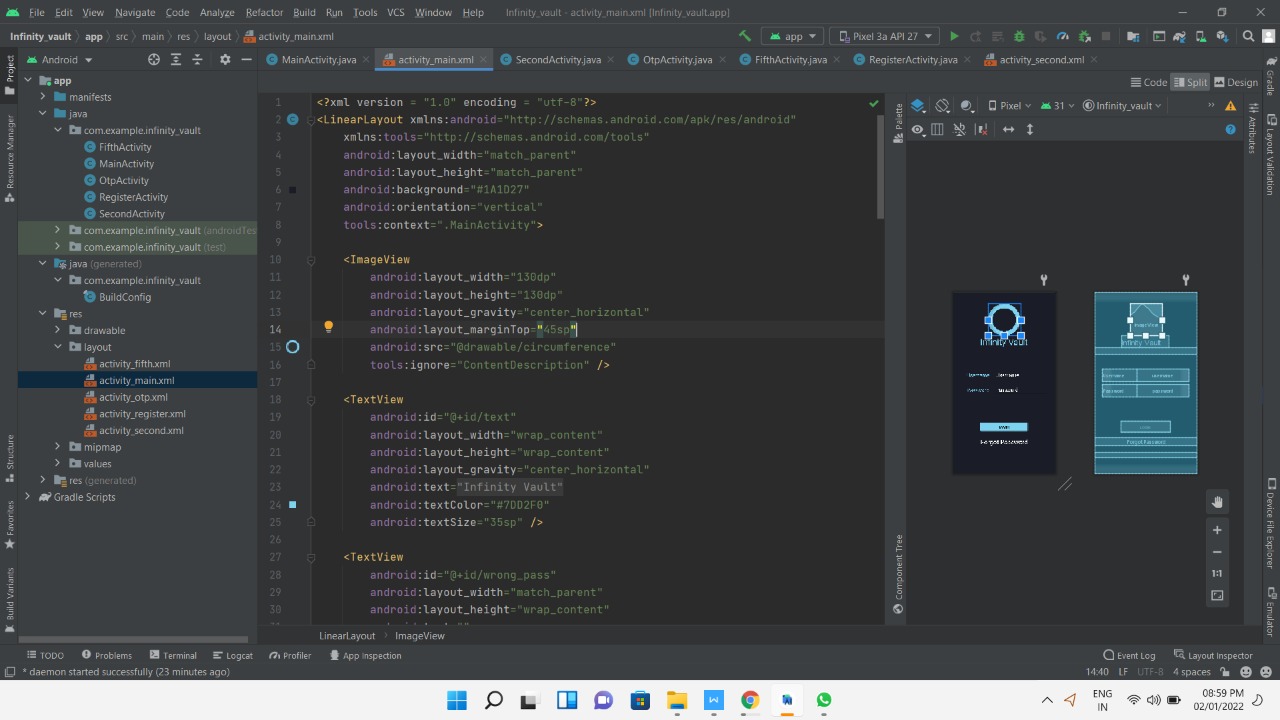
****

****

**5.3 Coding solution**

****

****

****

**5.4 Summary**

the code will run and will enable the application. It will then show a user interface for creating a new account or logging into an existing one along with an otp service.

**CHAPTER-6:**

**PROJECT OUTCOME AND APPLICABILITY**

**6.1 Outline**

The main objective of this document is to illustrate the requirements of the project Infinity Vault .Nowadays using only one layer of verification does not provide adequate protection.

**6.2 key implementations outlines of the System**

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check. Strong authentication is necessary to increase access [cybersecurity](https://www.techradar.com/in/best/best-online-cyber-security-courses) for accounts and online services. Passwords alone provide weak protection because they can be guessed and phished and, once stolen, tried against a range of accounts in the hope of securing a hit.

**6.3 Significant project outcomes**

It ensures that only the registered user is able to access the applications. It also provides an additional layer of protection against hackers or against shoulder surfing.

**6.4 Project applicability on Real-world applications**

It is used to ensure the safety of phone and personal info. The safety of social media apps ensures that no other person can post on behalf of the original user. Locking apps like gallery, messenger, call log ensures privacy protection. Moreover the user can customize which apps to lock or not.

**6.4 Inference**

This project outlines the importance of two factor authentication. In today's world using only a single layer of protection is not sufficient as the forgot password option can be utilized by malicious hackers. The additional layer of security ensures the proper verification of the user

**CHAPTER-7:**

**CONCLUSIONS AND RECOMMENDATION**

**7.1 Outline**

Infinity Vault is a type of software application that first registers the user with the help of email and a mobile number and then only allows the user to access the application. Locked apps can only be accessed after the user has undergone the 2-step verification process.

**7.2 Limitation/Constraints of the System**

When we open this app, infinity app, we will select the apps which we want to lock. Only those apps will be needing the otp to open and the ones not selected will not be protected

**7.3 Future Enhancements**

Can be linked with websites in the future and also desktop apps

**7.4 Inference**

The 2-step authentication provided by the app ensures the confidentiality and integrity of the personal information and also makes it difficult for a hacker to break it. It also ensures that the user is genuine.

**REFERENCES**

1. https://learn.vonage.com/blog/2019/02/07/build-an-otp-service-dr/#configure-the-application
2. http://www.warse.org/IJACST/static/pdf/file/ijacst01942020.pdf
3. https://sibernet.southindianbank.com/corp/htmls/Snorkel.pdf
4. https://eprint.iacr.org/2012/190.pdf
5. https://www.odysseytec.com/index.php/snorkel-tx-lay1/