NotePass Vault

Prajapati Sarvan Kumar, Vakkala Venkatesh, Pittala Bhaskar,
Polepalli Venkata Medha Shankar and Kiran Macwan

March 27, 2024

NotePass Vault

Prajapati Sarvan Kumar
B.Tech - Cse-Cs
Parul University
Vadodara, India
prajapathsarvan.cool@gmail.com

Vakkala Venkatesh
B.Tech - Cse-Cs
Parul University
Vadodara, India
vakkalavenkatesh2@gmail.com

Pittala Bhaskar
B.Tech - Cse-Cs
Parul University
Vadodara, India
pittalabhasker2@gmail.com

Polepalli Venkata Medha Shankar
B.Tech - Cse-Cs
Parul University
Vadodara, India
shankarpolepalli28@gmail.com

Kiran Macwan
Asst. Professor
PIET-CSE-Dept

***Abstract*— This is proposal for system "Android Based Notes application which can store passwords ,documents and notes with many secure features. This application will be explained later in details. But here, we will explain the general use or concept of this application. The general concept of this application its build based on a problem that user has many a number of digital accounts in this internet era but the problem being that he has to remember many passwords . So in order to make it easy any secure to store our password this application is being developed. User can save as a normal notes, and can save as a secure passwords and documents from anyone else that might use or read the notes and make sure that your notes can be protect from anyone .The application will be designed with security and usability in mind, and will be thoroughly tested to ensure that it is robust and reliable. By the end of this project, it is expected that from this application is will ease the security of our passwords and documents and friendly user. As a problem mention, this application is introduced to solve and secure the notes and passwords. The method used in order to build this application is by using Android Studio, Java , Firebase security.**

Keywords*— Notes , Passwords , Android Studio , Firebase

I. Introduction

This is the era of internet , where whole world has become digitally present .Each and every individual living in the most probably has digital accounts which secured by passwords. People may have many accounts with different passwords which protects their account .So he/she has to manage many passwords because he cannot remember all the Passwords so he will eventually take them in a notes app most probably.

Password managing & note-taking are one of the most overlooked virtual activities in today's digital age. Various companies are constantly adding new features to note-taking and password management. Have you ever considered building your own note-taking and password managing application? So, instead of having and maintaining two different apps in your system, we'll be Developing a single app which can perform both of these activities.

This project aims to develop a password manager with note-taking functionality, providing users with a secure and centralized platform to manage their passwords and notes. The application will be built using modern software development practices and technologies, including encryption and secure authentication mechanisms.

The password manager with note-taking application will feature a user-friendly interface that allows users to easily add, view, and edit their passwords and notes. Passwords will be stored in an encrypted database to ensure maximum security and protection against unauthorized access. Notes will also be encrypted and securely stored, ensuring that users' personal information is protected at all times.

In addition to password and note management, the application will include features such as password generation and password strength analysis, as well as the ability to tag and categorize notes for easier organization. The password generation feature will allow users to generate strong and unique passwords for their accounts, while the password strength analysis feature will provide users with feedback on the strength of their existing passwords and recommendations for improving them .The application will be designed with security and usability in mind, and will be thoroughly tested to ensure that it is robust and reliable.

Overall, the password manager with note-taking application developed in this project will provide users with a convenient and secure platform to manage their passwords and personal notes, making it easier for them to protect their online accounts and personal information while also keeping their notes organized and easily accessible

II. DESIGN

A. Project Flow

The flow of the project in what stages the development of the project need to be done here is a quick flow chat which describes the process.

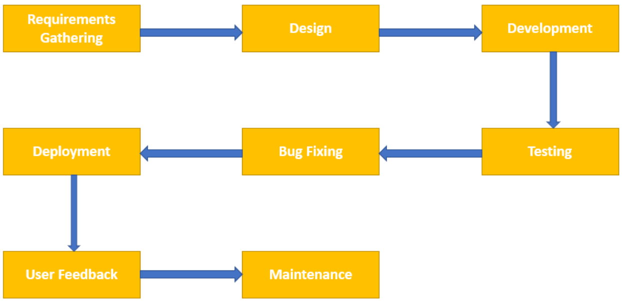


Fig. 1. Project Flow

B. Project Stages

This defines the stages that are involved in developing the application ,What are the step by step process you need to follow for developing the NotePass Application.

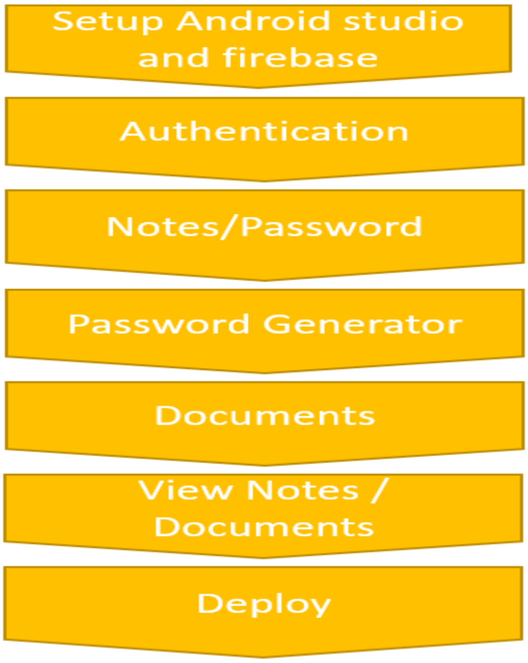


Fig. 2. Project Stages

C. Data Flow Diagram

Here is a data flow diagram of NotePass Application of how the user data is processed.

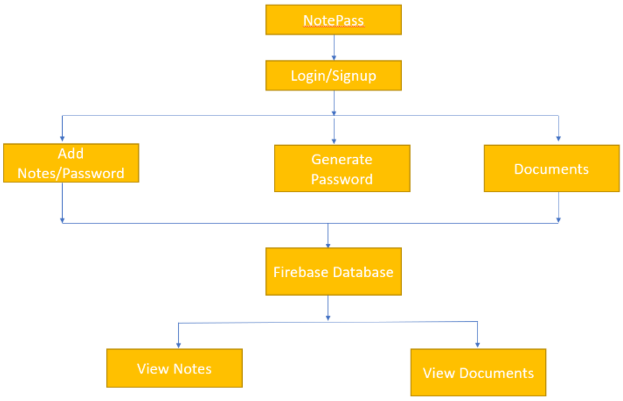


Fig. 3.Data Flow Diagram of Notepass

The diagram shows the flow of data in a notepass vault .At the center of the diagram is the NotePass Manager .Then we can proceed for authentication via login or if new user then sign up .The application has Three main functions: adding new notes or passwords, Generating Passwords and adding documents .When a new note or password is added, the data is stored in the firebase database Securely .Then there is a feature which generates random passwords which you can use in your daliy life which creating multiple accounts online .Similarly to Notes feature there is Document feature where the documents are added and then stored in firebase database .And to view all the added elements View Notes and View Documents section is implemented which collects the data stored in the firebase database and displays them.

III. IMPLEMENTATION

The Development of the application will be in the following stages.

The initial step, once we have our development environment ready, involves configuring Android Studio and Firebase.Once these elements are set up, we can proceed to create the application, beginning with the establishment of the login authentication system.

Following this, we will move on to constructing the home page. In this project, we will maintain simplicity by offering options such as Notes, Password Generator, Documents, and View Notes & View Documents.

Our project will require management of four primary states: Note (for handling notes and passwords), Password Generator (for password generation), Documents (for adding and storing documents, (including files and credit/debit card images), and View (for reviewing added notes, passwords, and documents).

To display all notes or passwords, we will utilize Listviews. The handling of our database and authentication requirements will be supported using Firebase.Essentially, the database will serve to store user login information, but it can also be used to store notes and password-related data.

The successful implementation of these requirements will mark the core completion of our application. Our next step - deployment!

A. Tools and Technology

1. Front-End Technologies

- Android Studio:

Android Studio is the primary Integrated Development Environment (IDE) for building Android applications. It provides the tools to design, develop, and test the front-end user interface of your app.

- XML and Java:

Android apps are typically developed using XML for layout and Java for coding. we used XML is used for designing the user interface, and Java is used for implementing functionality.

- Firebase Authentication SDK:

Firebase offers a robust authentication system that you can integrate into your Android app to handle user registration and login securely. You will need to include the Firebase Authentication SDK in your project.

2. Back-End Technologies

- Firebase Realtime Database or Firestore:

Firebase offers two database options: Realtime Database and Firestore. You can choose either based on your specific needs.

- Security Rules:

Firebase allows you to define security rules to control who can access and modify data in your database. Ensure you set up appropriate rules to protect user data.

3. Additional Technologies

- Password Generator Algorithm:

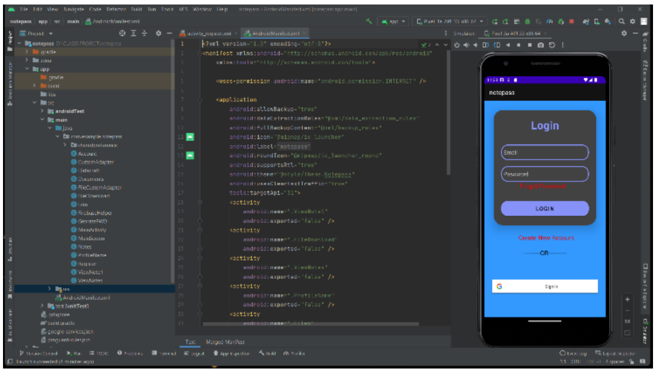
To create a password generator feature, we need to implement a password generation algorithm in Java.

- Dependency Management:

Use Gradle for managing dependencies in your Android project. It makes it easy to include libraries like Firebase SDKs.

B. *Implemented Work*

The Following images will show case you the work we implemented while developing the application.



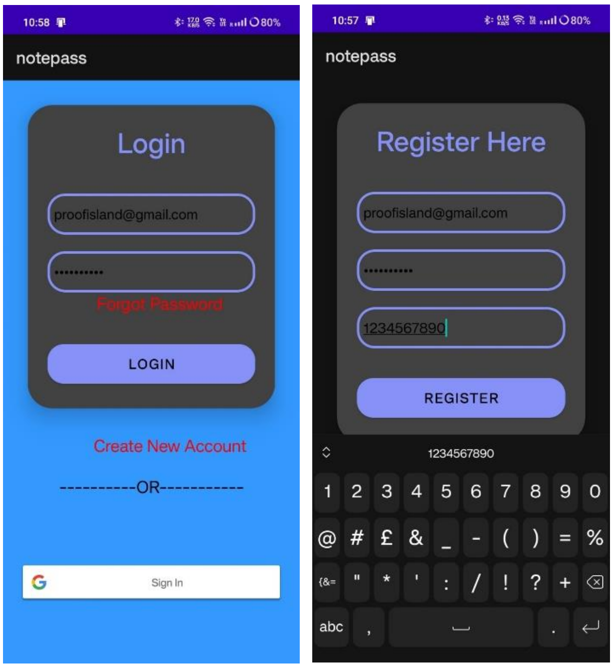
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">

    <uses-permission android:name="android.permission.INTERNET" />

    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="notepass"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.Notepass"
        android:usesCleartextTraffic="true"
        tools:targetApi="31">
        <activity
            android:name=".ViewNote1"
            android:exported="false" />
        <activity
            android:name=".FileDownload"
            android:exported="false" />
        <activity
            android:name=".ViewNotes"
            android:exported="false" />
        <activity
            android:name=".ProfileName"
            android:exported="false" />
        <activity
```

Fig. 4.Android Studio

The above image showcases the environment we used in developing the application i.e. Android studio and the sample code in development process.



notepass

Login

proofisland@gmail.com

••••••••••

Forgot Password

LOGIN

Create New Account

----------OR-----------

Sign In

notepass

Register Here

proofisland@gmail.com

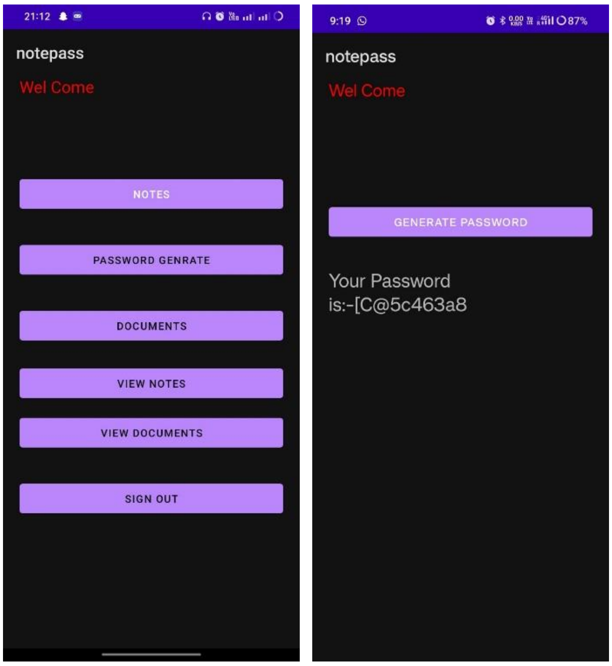
••••••••••

1234567890

REGISTER

Fig. 5. User Authentication

This picture shows the user authentication frame work developed using xml and Google firebase in android studio



notepass

Wel Come

NOTES

PASSWORD GENRATE

DOCUMENTS

VIEW NOTES

VIEW DOCUMENTS

SIGN OUT

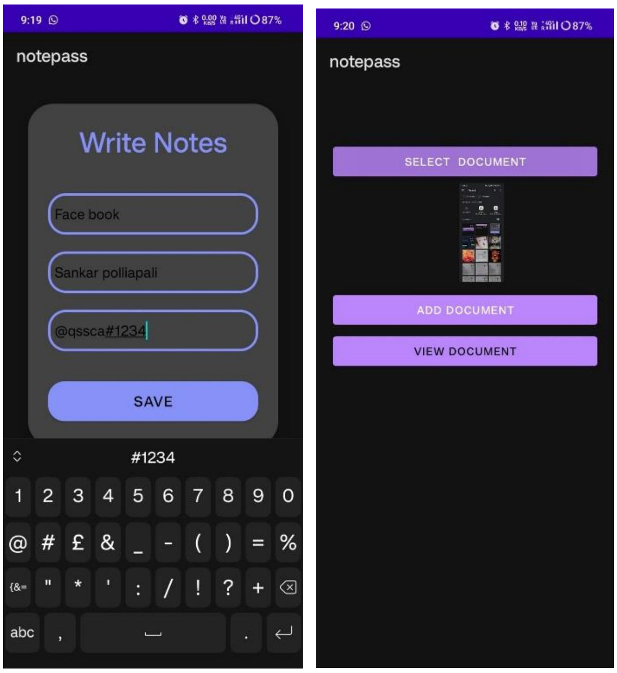
notepass

Wel Come

GENERATE PASSWORD

Your Password is:-[C@5c463a8

Fig. 6.Home Page and Password Generator



notepass

Write Notes

Face book

Sankar polliapali

@qssca#1234

SAVE

notepass

SELECT DOCUMENT

ADD DOCUMENT

VIEW DOCUMENT

Fig. 7. Add and Save Notes ,Passwords ,Documents

NotePass provides you with wide range of features that cater to the needs of our users. It allows users to create, organize, and edit notes effortlessly. The password management feature simplifies the process of storing and retrieving passwords securely. Additionally, the document management feature streamlines the storage and accessibility of important documents, ensuring users have all their vital information at their fingertips.

IV. LITERATURE SURVEY

The literature survey for the development of the NotePass application involved a thorough analysis of various research papers in the fields of mobile application development, information security, and user experience. We meticulously examined existing solutions, best practices, and emerging trends to shape the features and functionality of NotePass.

Through this comprehensive review, we were able to identify key challenges and opportunities in the domain of note, password, and document management applications, which informed our decision-making process.

[1] Author: Vidya Shankar.G.S , Yasasw.Kumarakalva [2019] – “A Secure Password Manager”

"A Secure Password Manager" by Yasasw.Kumarakalva and Vidya Shankar.G.S proposes a secure password manager that incorporates several security features to protect against various attacks such as dictionary attacks, phishing attacks, and keylogging attacks. The proposed password manager uses a combination of encryption, hashing, and salting to protect passwords from unauthorized access, and includes features such as two-factor authentication, random password generation, and password strength analysis to enhance password security.

[2] Author: Samruddhi Patil , Kumund Wasnik [2018] – “A Survey on Existing Password Storage Method and Their Security”

Password managers were found to be the most secure option as they generate and store strong, unique passwords for each account and encrypt them with strong encryption algorithms. However, the authors noted that even password managers are not immune to attacks and users should still take additional security measures such as enabling two-factor authentication and regularly changing their master password.Overall, the study emphasizes the importance of using secure password storage methods and taking appropriate measures to protect personal information from unauthorized access.

[3] Author: Shivam K. Shinde , Mohit V.Deshpande [2022] – “AStudy for an ideal Password Management System”

Password management systems are digital tools that store and manage passwords for various online accounts in an encrypted format, eliminating the need for users to remember or write down multiple passwords. The growing number of online accounts and the increasing sophistication of cyber-attacks make password management systems a necessity for individuals and businesses alike. However, not all password management systems are created equal, and some may have security vulnerabilities or lack essential features. This study aims to identify the key features that an ideal password management system should possess and suggest improvements to existing systems.

[4] Author: Abdulaziz Alrushaid, Reem Algarwai [2020] – “Security Analysis on Password managers Applications”

Password managers have become essential tools for managing the increasing number of online accounts and maintaining strong password practices. They store passwords in an encrypted format, preventing unauthorized access to sensitive information. However, the security of password managers relies on several factors, such as the strength of encryption algorithms, the authentication process, and the user's behavior. A breach in a password manager application can have severe consequences, including identity theft and financial loss. Therefore, its crucial to understand the security features and vulnerabilities of password managers applications.

[5] Author: Sarah Pearman [2016] – “ Why people (don’t) use password managers effectively : Results from a comprehensive public survey ”

The research by Sarah Pearman demonstrates that many individuals do not use password managers effectively due to various factors, such as poor usability, lack of trust, and perceived lack of control over their passwords. However, the study also suggests that user education and improved design and interface can lead to better password manager usage. Organizations that promote the use of password managers as a security measure should consider these findings in order to encourage effective usage of password managers by their employees and customers.

[6] Author: Michael Fagan [2017] – “ An Investigation into Users’ Considerations towards using password Managers ”

Password managers offer significant benefits for users, including increased security and convenience. However, this study identified several barriers to their adoption, including concerns about privacy, trust, and cost. To address these barriers, user education is needed to increase awareness of the benefits of password managers and to educate users on how to use them effectively. Additionally, improvements in the design and security of password managers are necessary to increase users' trust and confidence in their use. Overall, this study provides insights into users' attitudes towards using password managers and highlights the need for further research and development in this area.

[7] Author: Carlos Luevanos [2018] – “ Analysis on the Security and use of Password Managers ”

The use of password managers can improve password security, but users should be aware of potential risks and challenges associated with their use. Password manager companies should take steps to improve the security and usability of their products, including conducting regular security audits and addressing any vulnerabilities that are identified. Users should carefully evaluate password manager options and choose tools that use strong encryption, offer two-factor authentication, and are regularly updated.

[8] Author: Bian Yang [2021] – “ Cloud Password Manager Using Privacy – Preserved Biometrics”

The proposed cloud password manager using privacy-preserved biometrics is a secure and privacy-preserving solution for managing passwords. The system addresses the limitations of traditional password-based authentication methods by using biometric authentication and homomorphic encryption to protect the user's biometric data. The system also includes additional security features such as two-factor authentication and password strength checks to enhance security.

[9] Author: Zhiwei Li, Warren He, Devdatta Akhawe [2014] – “ Security Analysis of Web-based password Managers ”

The paper "Security Analysis of Web-based Password Managers" highlights the importance of evaluating the security features of web-based password managers. While these managers offer a convenient way to manage and generate strong passwords, the study identifies several vulnerabilities and weaknesses in their design and implementation that could compromise the security of users' passwords. The authors recommend taking steps to mitigate these vulnerabilities, such as using strong and unique master passwords, ensuring that passwords are stored in an encrypted form, and enabling two-factor authentication where possible. Users should also be aware of the risks associated with password managers and take measures to protect themselves, such as regularly changing their master password and monitoring their accounts for suspicious activity.

[10] Author: Joshua Gray [2018] – " Forensically – Sound Analysis o Security Risks of Using Local Password Managers "

The study provides recommendations for improving the security of local password managers, including implementing stronger encryption algorithms, improving password strength requirements, and educating users about best practices for password management. The study emphasizes the importance of regularly reviewing and updating password manager security measures to address new and emerging threats.

CONCLUSION

In conclusion, the development of the NotePass application has been a rewarding and transformative journey, leveraging the power of Android and Firebase technologies to provide a comprehensive solution for managing notes, passwords, and documents. This project has successfully addressed the need for a secure and user-friendly platform to organize and protect valuable information, and it has delivered on its promise of enhancing productivity and security for our users.

Throughout this project, we have achieved several significant milestones:

Feature-rich Functionality: NotePass boasts a wide range of features that cater to the needs of our users. It allows users to create, organize, and edit notes effortlessly. The password management feature simplifies the process of storing and retrieving passwords securely. Additionally, the document management feature streamlines the storage and accessibility of important documents, ensuring users have all their vital information at their fingertips.

Password Generation: The ability to generate strong and unique passwords is a valuable addition to our application. Users can now rely on NotePass to create robust passwords for their accounts, bolstering their overall online security.

Firebase Integration: Firebase has played a pivotal role in ensuring the scalability, real-time synchronization, and security of the application. Firebase Authentication ensures that user data remains confidential, and Firestore ensures data consistency across devices and platforms.

User-Friendly Design: The application's user interface has been thoughtfully designed to be intuitive and aesthetically pleasing. Users can quickly adapt to the application, and its design promotes efficient interaction.

Enhanced Security: Security is of paramount importance, especially when dealing with sensitive information. With Firebase Authentication and robust encryption mechanisms, we have ensured that user data is safeguarded from unauthorized access.

Feedback and Continuous Improvement: We have actively sought and incorporated user feedback throughout the development process, and we remain committed to ongoing improvements and updates to meet evolving user needs.

Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

[1] Yasasw. Kumarakalva, Vidya Shankar. G. S, Shreekara. K. K, ridhar. P. H, Asha. G. R, "A SECURE PASSWORD MANAGER", JETIR,2017

[2] Samruddhi Patil , Kumud Wasnik ," A Survey on Existing Password Storage Methods and their Security" ,IJSR , 2017

[3] Shivam K. Shinde , Mohit V. Deshpande ," A Study for an Ideal Password Management System" IJRASET ,2022

[4] Abdulaziz Alrushaid, Reem Algarawi ," Security Analysis on Password Managers Applications" ,RPJ ,2020

[5] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor , "Why people (don't) use password managers effectively",USENIX,2019

[6] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan and Ross Buck "An investigation into users' considerations towards using password managers ",HCCIS,2017

[7] Carlos Luevanos, John Elizarraras, Khai Hirschi, Jyh-haw Yeh," Analysis on the Security and Use of Password Managers",PDCAT,2017

[8] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song," The Emperor's New Password Manager",USENIX,2014

[9] Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch," Cloud Password Manager Using Privacy-Preserved Biometrics",IEEE,2014

[10] Joshua Gray, Virginia N. L. Franqueira ,Yijun Yu ," Forensically-Sound Analysis of Security Risks of using Local Password Managers",IEEE,2016

[11] Masanobu Numazawa, Keisuke Ai," Education and Learning Support System Using Proposed Note-Taking Application " IEEE,2014

[12] Minoru Nakayama, Kouichi Mutsuura, Hiroh Yamamoto," Effectiveness of Note-taking Content Features on Test Scores in Online Courses",IEEE,2019

[13] Dave Towey, David Foster, Filippo Gilardi, Paul Martin, Andrew White, Yiru Jiang, Yichen Pan, Yu Qu," Students as Partners in a Multi-media Note-taking App Development",IEEE,2019

[14] Soham Dixit, Rutuja Haladkar, Aryan Tele, Shruti Kataria, Shubhangi Chintawar," ANDROID NOTES APPLICATION",IRJETS,2022

[15] Ms. Shraddha G. Muley, Ms. Jyoti C. Brahama, Ms. Pallavi S. Ugale,Ms. Sushama G. Sananse, Prof. P. S. Kharche,Prof. S. M. Dandge," Evernote – A Web Based Application on Notes Making App",IJARSCT,2021

[16] Myungseo Park, Soram Kim, and Jongsung Kim," Research on Note-Taking Apps with Security Features",IEEE,2020

[17] R. Asritha, R. Arpitha," A Survey Paper on Introduction to Android and Development Process",IRJET,2020

[18] Vijay Deshmane , Sarita Sawale , Krishna Bharambe , Pratik Lahudkar," Application Devolopment With Android",TROI,2020

[19] Mr. Vinayak Pujari, Dr. Rajendra Patil, Mr. Shailesh Sutar," A Review on Best Practices in Mobile Application Development"ISSN2349,2014

[20] Mrs. Prachi Sasankar1. Mrs. Usha Kosarkar," Research on Development of Android Applications",IOSR,2016