Project Report

on

Two Factor Authentication System

In partial fulfilment of requirements for the degree

of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

Submitted by:

AAYUSH MODI [17100BTSCE01198]

ADITYA CHOUHAN [17100BTCSE01203]

ADITYA MALVIYA [17100BTCSE01205]

Under the guidance of

MRS. RUPALI BHARTIYA

SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE

SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

JULY-DEC 2019

SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE

SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DECLARATION

We here declare that work which is being presented in the project entitled "**Two Factor Authentication**" in partial fulfillment of degree of **Bachelor of Technology in Computer Science & Engineering** is an authentic record of our work carried out under the supervision and guidance of **Mrs. Rupali Bhartiya** Asst. Professor of Computer Science & Engineering. The matter embodied in this project has not been submitted for the award of any other degree.

Student 1 Signature

Student 2 Signature

Student 3 Signature

Date:

SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE

SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

PROJECT APPROVAL SHEEET

Following team has done the appropriate work related to the "**Two Factor Authentication**" in partial fulfillment for the award of **Bachelor of Technology in Computer Science & Engineering** of "SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY" and is being submitted to SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE.

Team:

1. Aditya Chouhan

2. Aditya Malviya

3. Aayush Modi

Internal Examiner **External Examiner**

Date

SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE

SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that **Mr. Aditya Chouhan**, **Mr. Aditya Malviya** and **Mr. Aayush Modi** working in a team have satisfactorily completed the project entitled "**PROJECT TITLE**" under the guidance of MRS. Rupali Bhartiya in the partial fulfillment of the degree of **Bachelor of Technology in Computer Science & Engineering** awarded by SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY affiliated to SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE during the academic year **July2019-Dec 2019**.

Project Guide

Mrs. Rupali Bhartiya

Project Coordinator

Prof. Anand Singh Rajawat

Prof. Chetan Chauhan

Dr. Anand Rajavat

Director & Head,

Department of Computer Science & Engineering

ACKNOWLEDGEMENT

We are grateful to a number of persons for their advice and support during the time of complete our project work. First and foremost our thanks goes to **Dr. Anand Rajavat** Head of the Department of Computer Science & Engineering and **Mrs. Rupali Bhartiya** the mentor of our project for providing us valuable support and necessary help whenever required and also helping us explore new technologies by the help of their technical expertise. His direction, supervision and constructive criticism were indeed the source of inspiration for us.

We would also like to express our sincere gratitude towards our Director **Dr. Anand Rajavat** for providing us valuable support.

We are really indebted to **Prof. Anand Singh Rajawat and Prof. Chetan Chauhan,** project coordinator for helping us in each aspect of our academics activities. We also owe our sincere thanks to all the **faculty members** of Computer Science & Engineering Department who have always been helpful.

We forward our sincere thanks to all **teaching and non-teaching staff** of Information Technology department, SVVV Indore for providing necessary information and there kind co-operation.

We would like to thanks our parents and family members, our classmates and our friends for their motivation and there valuable suggestion during the project. Last, but not the least, we thank all those people, who have helped us directly or indirectly in accomplishing this work. It has been a privilege to study at SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE.

ABSTRACT

Two Factor Authentication has been done in order to heighten Authentication Systems. The overall access to a System is not defined by a single factor, like password, but the combination of multiple factors. In order to potentiate the security of access control systems, two factor authentication (TFA) comes in very handy mainly because it focusses on combination of both factors. Two factor authentication has already been doing tremendous jobs in client server web application. There are a huge number of devices and solutions for 2FA, from tokens to RFID cards to smartphone apps.

The project is going to be developed out as a background service that makes sure that the protected data is not accessible to the unauthorized user. This can be done by making data encrypted over malicious access or in absence of the authorized person. To achieve this, Bluetooth tokens will be used by our system to ensure the authorized persons availability nearby the computer in which the data is being accessed.

LIST OF FIGURES

FIG NO.	FIGURE NAME	PAGE NO
4.1.1	Use Case Diagram	
4.3.1	Data Flow Diagram (Level 0)	
4.3.2	Data Flow Diagram (Level 1)	
4.3.3	Data Flow Diagram (Level 2)	
5.1	Detailed Class Diagram	
5.2.1	Sequence Diagram	
5.2.2	Collaboration Diagram	
5.3	State Diagram	
5.4	Activity Diagram	
7.3	Snapshot	

TABLE OF CONTENT

Declaration I

Project Approval Sheet II

Certificate III

Acknowledgement IV

Abstract V

List of Figures VI

CHAPTER 1 - INTRODUCTION.....1-3

1.1 Introduction 1

1.2Problem Statement…….....1

1.3 Need for the proper system.……....1

1.4 Objective.....1

1.5 Modules of the System.….....2

1.6 Scope….....3

CHAPTER 2 - LITERATURE SURVEY.....4-5

2.1 Existing System 4

2.2 Proposed Solution….....4

2.3 Feasibility Study……....4

2.3.1 Technical Feasibility……....4

2.3.2 Economical Feasibility……....5

2.3.3 Operational Feasibility……....5

CHAPTER 3 - REQUIREMENT ANALYSIS.....6-8

3.1 Methods used for requirement.....6

3.2 System Specification……..6
3.2.1 Software Requirement……..6
3.2.2 Hardware Requirement……..7
3.3 Functional Requirements.....7
3.4 Non Functional Requirements …….....7
3.5 Benefits…….....8

CHAPTER 4 - DESIGN…….....9-11
4.1 Software Requirement Specification.....9
4.1.1 Document Conventions.....9
4.1.2 Use Case Diagrams.....……..……..9
4.1.3 User Interface.....9
4.2 Conceptual Level Activity Diagram.....10
4.3 Data Flow Diagram..…….....11
4.4 E-R Diagram…….....11

CHAPTER 5 - SYSTEM MODELING…….....12-15
5.1 Detailed Class Diagram…….....12
5.2 Interaction Diagram……..…….....12
5.3 State Diagram……..……..…….....14
5.4 Component Diagram……..……..…….....14
5.5 Deployment Diagram…...……..…….....15
5.6 Testing……...……..……..…….....15

CHAPTER 6 - CONCLUSION & FUTURE WORK..... 16-16
6.1 Limitation of Project… …….....16
6.2 Future Enhancement……..……..…….....16

CHAPTER 7 - BIBLIOGRAPHY & REFERENCES.....17-20
7.1 Reference Books..…….……..…….....17
7.2 Other Documentations & Resources 17
7.3 Snapshots…….. 17

CHAPTER -1
INTRODUCTION

1.1 Background

The introduction of the Two Factor Authentication has been done in order to heighten the Authentication Systems. The overall access to a System is not defined by a single factor, like password, but the combination of multiple factors. In order to potentiate the security of access control systems, two factor authentication (TFA) comes in very handy mainly because it focusses on combination of both factors. Two factor authentication has already been doing tremendous jobs in client server web application. There are a huge number of devices and solutions for 2FA, from tokens to RFID cards to smartphone apps. For e.g.

a. Google Authenticator is a 2FA app that works with any supporting site or service.
b. Microsoft Phonefactor offers 2FA for a reasonable cost and is free to small organizations of 25 members or less.
c. Apple's iOS, iTunes store and cloud services all support 2FA to protect user accounts and content.

But besides web, its application for isolated machines i.e. desktops, is equally important as normal user have their confidential and private files on their PC hard drives, so TFA can be realised using Bluetooth and Rijndael Algorithm for them.

Bluetooth, a wireless technology for the transmission of data among two devices & operates on Personal Area Network(PAN).The major advantage that Bluetooth offers for TFA is its range of network which is just 100 meters and is enough to personify an authenticated user's presence. Bluetooth can conduce in the T-FA System in the following manner:

Authentication: Connect to a particular device only if the device is known to the system, otherwise abort connection. The familiarity of Bluetooth device is ascertained by the MAC address of the device.

Authorization: Only authorized Bluetooth devices should have the access to the protected data.

Confidentiality: Since Bluetooth devices have a range of only 100 meters, there won't be any spoofing since as soon as the device is out of range, the protected personal files and folder would be encrypted. Rijndael Cipher is an Advanced Encryption Standard (AES) based on design principle grounded as substitution permutation network and is quick in both software and hardware. Avoidance of the Fiestal network in the AES is its important characteristic.

1.2 Problem Statement

In present day, the increasing reliance on computer systems has led to the dependence on confidential security measures. Various methods used to identify a user are Digital signature, Challenge-Response, Biometrics, IPsec (Internet Protocol Security), Single Sign On and Password. Password has become one of the most ubiquitous modern day security tool and is very commonly used for authentication. These passwords are string of characters used for authentication or user access. Unfortunately users set passwords that can be easily memorized, in turn increasing threats. Password meters indicating password strength are used to increase effectiveness of passwords and make them less predictable. Users possessing administrator privileges can create, modify and delete accounts. In order to judge the strength of passwords, password policies came into existence yet passwords face several flaws corresponding to bookmarklet, authorization, web and user interfaces. Although biometrics and security tokens are some of the alternatives to passwords, they increase the overall risk theft, privacy threat and rise in infrastructural costs. The length of passwords plays an important role in determining its strength. Success on brute force attack mainly depends on the length of passwords. Generally, brute force attack fails in case of long passwords. Passwords containing alphanumeric characters are another type of strong passwords. Password disclosure should be avoided in order to prevent social engineering attacks. So, to conclude problem domain, it can be said as the existing one factor authentication system lags in some or other way may be due to non-encryption of data to be protected.

1.3 Need for the proper System

Virtually everyone has been prompted to answer a security message or input an SMS messaging code to log in to some kind of account. This extra step beyond username and password is two-factor authentication (2FA). These authentication methods of secondary verification, designed to ensure that a person is who they say they are, are examples of multi-factor authentication.2FA is a commonly used method of authentication used for situations in which someone may misspell a password, forget their password, log in from a new device, or perform any other potentially suspicious behaviour. More than two requirements may be added to the authentication process. That's why we need a proper System which provide the surety of secure the important data ,Two-factor authentication is a supplement to a digital password that, when used properly, makes it harder for a cybercriminal and unauthorized person to access the others important data and any other information's. Desksure provide all the aspects .

1.4 Objective

Two factor authentication system's objectives in real world are - adding a second layer of protective shield over the access mechanism, ensuring that the data is made available to the right person only. The project is going to be developed out as a background service that makes sure that the protected data is not accessible to the unauthorized user. This can be done by making data encrypted over malicious access or in absence of the authorized person. To achieve this, Bluetooth tokens will be used by our system to ensure the authorized persons availability nearby the computer in which the data is being accessed.

1.5 Modules of the system

We have divided two factor authentication system into two basic modules depending upon which type of user is trying to login i.e. whether as an Admin or as a Naive user.

Admin Module:

Registration Process:

The user first have to get registered as an Admin for that all the nearby Bluetooth devices will be searched by the software then user will select the name of its bluetooth device the pairing operation will be then performed .Once the pairing is done successfully the name of the Bluetooth device and Mac address will get registered into the software and then that particular bluetooth device will be recognized as an Admin.

Login Process:

When a user tries to login into the software as an Admin then first the Admin Login window will have to be opened by the user and then the user have to enter the name of Bluetooth device with which the particular user is registered as an Admin. Then to verify , the user have to clicks on verify button then the software system will try to fetch the resource user files which contains the name of the user along with the mac address. If the name of the user bluetooth device is found then using the mac address of the device our software system will try to open a connection with the remote device and then connection object will be saved statically into the static member of resources class , if the connection is not successful a user log will be maintained and if the connection is successful then pairing mechanism will be performed and on successful pairing the user log will be maintained in the log file and the Admin Dashboard will appear where the user will get all the Admin privileges.

The Functionalities of Admin are:-

- **Manage User:** The admin can add or remove the users.
- **Manage Files:** The admin can add or remove the files and can select a
- **View User Logs:** Admin can see user logs based upon chosen date.
- **Manage Protection:** The admin has a right to manage the control of the bluetooth protection. Admin can ON/ OFF the bluetooth protection as per

need. When admin turns off the bluetooth protection then all the encrypted files and will become visible to everyone and accessible by everyone.

Naive User Module:

Registration Process:

Admin has the right to add or remove any naïve user. Software System searches for available Bluetooth, devices through search devices module and then admin chooses the particular user by the name of Bluetooth device and then add it as a naive user.

Login Process:

When a user tries to login into the software as an Naïve then first the Naïve User Login window will have to be opened by the user and then the user have to enter the name of Bluetooth device with which the particular user is registered as an Naive. Then to verify , the user have to clicks on verify button then the software system will try to fetch the resource user files which contains the name of the user along with the mac address. If the name of the user bluetooth device is found then using the mac address of the device our software system will try to open a connection with the remote device and then connection object will be saved statically into the static member of resources class , if the connection is not successful a user log will be maintained and if the connection is successful then pairing mechanism will be performed and on successful pairing the user log will be maintained in the log file and the window named “MyFiles” will appear where the user will get all the Naïve privileges.

The Functionalities of Naïve User:

- **Add/Remove Files**: Naïve user can add or remove files from the MyFiles window of its user account. Naïve can be able to remove the previously encrypted file from the window.
- **Encrypt/Decrypt Files**: User can be able to select the particular file and can Perform the operation of encryption or decryption.

1.6 Scope

The use of WI-FI as a wireless communication medium could be integrated replacing Bluetooth. The number of authentication factors could be increased, for example, including biometric authentication (face recognition and fingerprint scanner) or location based encryption decryption.

This design could be as well turn into a mobile application that would allow the original file to be encrypted without requiring saving the original file in the same memory.

CHAPTER 2
LITERATURE SURVEY

2.1 Existing System

Rijndael is another name of what is technically known as Advanced Encryption Standard (AES). Although it is the predecessor of AES Working upon a project that deals with security concerns of data using AES and for 2nd step authentication using Bluetooth gives intuitiveness to the developers about the vast scopeof development in the proposed system. “Authy” is an IOS app that also implements TFA for desktop. Two factor authentication system relies more on the personalised token to authenticate. Google, Microsoft, Salesforce, all big IT giants have implemented TFA in some form or other.

Coming to the development side of TFA using Rijndael and Bluetooth, on programmatic level, implementing AES is not an easy task as it is one of the rare standards whose black hole is not yet discovered. Many Programming technologies has implemented this vary algorithm in their core libraries which are like ready to use. For e.g. C# has built in core namespace that presents a public abstract class “Rijndael” which is all set to get used for such a system that wants to take benefit of AES.

The below is the snapshot of the existing Rijndael implementation in C#,

Namespace: System.Security.Cryptography

Assembly: mscorlib (in mscorlib.dll)

Inheritance Hierarchy

System.Object

System.Security.Cryptography.SymmetricAlgorithm

System.Security.Cryptography.Rijndael

System.Security.Cryptography.RijndaelManaged

2.2 Proposed System

However, Rijndael is necessary for working out on a TFA software, but is alone not sufficient, Bluetooth is the second major need for developing the proposed system. It is worth noting that, however Microsoft has provided the Rijndael in very well defined form, but has not yet implemented Bluetooth interface which is ready to use for Bluetooth integration. There are no built in .NET APIs for Bluetooth integration into development project. Writing Bluetooth interface is no big deal, but the technology should offer security and robustness which can never be expected from C# as it is originally a product of Microsoft

However Java can play a vital role for this need. Java has also a built in API for Bluetooth integration recognized as "JSR-82.

2.3 Feasibility Study

Java is a light weight simple to use and platform independent technology to program applications. Being of independent, it provides cross platform usage of the utility. Java is Secure and Robust, this feature describes the most for choosing java for making a security application as a security application need to be secure itself and also should be able to handle application malfunctions to be caused by security intruders. Also Java 4 gives great support for cryptography so it comes out to be a choice for developing a security extension for replacing old password style for securing computer files. Java has a built in class known as Cipher and also a third party library is also very popular for the same known as "BouncyCastle".

2.3.1 Technical Feasibility

Choosing C# for development for our project would have been greedy decision. As it provides Ready-made Rijndael for use in any project like ours. On the other hand, choosing Java for development of our project presents us with new challenges and future scope of core java API development of AES. One of our stiff reasons to choose this project is to get exposure in field of encryption more precisely in AES. Java being "The Secure language" and it also offers future scope of API development for AES so these two reasons mainly gives us the urge to work towards the development of such project in it.

2.3.2 Economical Feasibility

The project is economically feasible, Two-factor authentication methods are typically prompted in two forms. Some businesses or organizations may require every user to successfully fulfil two-factor authentication methods before granting access.it is an additional layer of security that can make it significantly more difficult for hackers and unauthorized person to gain access to sensitive information.

2.3.3 Operational Feasibility

The project is operationally very feasible as it is user-friendly, the project is also really helpful as the user can use it to encrypt the crucial file of the user at any moment of time using the Bluetooth of their device. It is a Desktop Application so It is necessary for the user to have the independent software on their machine to perform encryption as well as decryption. Multi-factor authentication should be used whenever possible because it immediately neutralizes the risks associated with compromised passwords by adding an additional layer of security to protect highly sensitive personal information. If a password is hacked, guessed, or phished, a bad actor would still need the required second factor on the important data, making the stolen password alone useless.

CHAPTER 3
REQUIREMENTS ANALYSIS

3.1 Method used for Requirement analysis

In present day, the increasing reliance on computer systems has led to the dependence on confidential security measures. Various methods used to identify a user are Digital signature, Challenge-Response, Biometrics, IPsec (Internet Protocol Security), Single Sign On and Password. Password has become one of the most ubiquitous modern day security tool and is very commonly used for authentication. These passwords are string of characters used for authentication or user access. Unfortunately users set passwords that can be easily memorized, in turn increasing threats. Password meters indicating password strength are used to increase effectiveness of passwords and make them less predictable. Users possessing administrator privileges can create, modify and delete accounts. In order to judge the strength of passwords, password policies came into existence yet passwords face several flaws corresponding to bookmarklet, authorization, web and user interfaces. Although biometrics and security tokens are some of the alternatives to passwords, they increase the overall risk theft, privacy threat and rise in infrastructural costs. The length of passwords plays an important role in determining its strength. Success on brute force attack mainly depends on the length of passwords. Generally, brute force attack fails in case of long passwords. Passwords containing alphanumeric characters are another type of strong passwords. Password disclosure should be avoided in order to prevent social engineering attacks. So, to conclude problem domain, it can be said as the existing one factor authentication system lags in some or other way may be due to no encryption of data to be protected.

3.2 Data Requirements

The problem domain gives birth to numerous requirements. Specifically, user's perspective of the system defines two major needs that are to be addressed namely,

a. Real time untameable protection of data.
b. Personal prompt for data access.

3.3 Functional Requirements

Functional requirements are the requirements that define specific behaviour or function of the system

- Login process : System Tray , it contains three options
  1) Open
     Admin
     Panel
  2) My Files
  3) Exit.

  Initially for first login it requires to Open Admin Panel. For this User's Bluetooth Should be open and discoverable, type the name of your Bluetooth and the System will verify your Bluetooth Device. After verifying the Bluetooth device it will successfully login as Admin.
- Admin Dashboard : In admin Dashboard admin has following privilege It can Manage protection
  1) Add Users
  2) Manage users
  3) Add File
  4) Manage File
  5) View User logs
- After login as Admin or naive user you can encrypt any kind of file. For this you have to click on the Add file icon, then select the root of the file which you want to encrypt, after this you will get the message that "Do you really want to secure the file using Desksure?" After this your file will be encrypt and fully Secure.

3.4 Non-Functional Requirements Safety Requirements

Sender and Receiver: Admin and Naive User should make sure that only they are having the same device to encrypt and decrypt the file inside the DeskSure. Both should take care of it.

- **Security Requirements:** We develop a software in which user's file will be secure by encryption using Bluetooth. Only, admin and naive user should be aware of their encrypted file. User should be ware about that his/her device should not be in the hand of others otherwise, that prig will read your important data that resides in the file.
- **Software Quality Attributes:** The Quality of the software is maintained in such a way that only Admin can see and manage his own file as well as admin has privilege to see the other's file and can see the logs about the users. There is no probability of knowing the users encrypted file.

3.5 System Specification

- Operating System (Windows) • Minimum CPU or processor speed.
- Minimum GPU or video memory.
- Minimum system memory (RAM).
- Minimum free storage space.

3.5.1 Hardware specification

- 512 MB or more RAM.
- 50 MB or freer disk space.
- A Bluetooth card on the PC and a Bluetooth enabled mobile device

3.5.2 Software specification

- JDK 1.4 OR ABOVE & OS (Windows/Unix/Mac/Solaris).
- Bluetooth Card driver.

CHAPTER 4
DESIGN

4.1.1 Software Requirements Specification

The problem domain gives birth to numerous requirements. Specifically, user's perspective of the system defines two major needs that are to be addressed namely a real time untameable protection of data.

Personal prompt for data access.

Planning:

The development of the project revolves around implementing the core Rijndael i.e. the raw Rijndael algorithm in java hence, the development would start from researching about the Rijndael and all of its aspects to carry out its core functions in java as a full-fledged java class. Furthermore, after carrying out the development of core Rijndael, the process moves to the phase in which the

Bluetooth integration's interface can be written after which the application programming can be initiated as both the core pillars of the applications are ready and available to be integrated.

Scheduling:

While the development of the project doesn't significantly have requirement gathering phase, but it have lot of research and learning phase that makes it bit more complicated to be partitioned between a team. However we three have decided to not separately work in the initial phase as the initial phases are teaching us the basics of the discipline we are working upon. But, after requirement and analysis, we would work in our parts only. Like one will be dealing with Bluetooth integration, other would be building up the core functions of the algorithm, the other would be documenting the things and the would be keeping everyone on same page yet managing all the components and making the abstracts of the system so that finally it can be built up in such a way that each of us will have same share of knowledge i.e. Each of us will be known to the system fully

Purpose:

The purpose of this document is to build a Desktop system to secure the users crucial file, with the help of two factor Authentication.

Document Conventions:

Throughout the document (formatted in Google Docs) font used for:

1. Topics are Times New Roman formatted in 'Heading 3' style. Font size for headings is 16
2. Sub topics are Times New Roman formatted in 'Heading 3' style. Font size for sub-topics is also 14
3. Text is Times New Roman formatted in 'Normal' style. Font size for text is 12
4. Italics have been used for laying special emphasis on certain information.

All references to the websites used are hyperlinked in Times New Roman, Normal + Times style and size 12

Objective:

Two factor authentication system's objectives in real world are - adding a second layer of protective shield over the access mechanism, ensuring that the data is made available to the right person only **Scope:**

This design could be as well turn into a mobile application that would allow the original file to be encrypted without requiring saving the original file in the same memory

- ## Software and Hardware Requirements:

Following are the hardware and the software requirements for the this project

Hardware Requirement:

i. 512 MB or more RAM.
ii. 50 MB or freer disk space.
iii. A Bluetooth card on the PC and a Bluetooth enabled mobile device.

Software Requirement:

i. JDK 1.4 OR ABOVE & OS (Windows/Unix/Mac/Solaris).
ii. Bluetooth Card driver.

- ## Applicability:

Two factor authentication system has its applicability in the areas where user cannot rely on the general password protection and wants to ensure a personal prompt ensuring data access using a wireless token

4.1.2 Supplementary Specifications

The two factor authentication system is the best approach to meet the desktop based protection tool using Bluetooth device. The system would ensure that only a valid user has access to the data or can be thought as, data is accessible onto its very own user. The system would start as a background service as soon as any user logs in to the PC and would then try to make a handshake with an already registered Bluetooth device upon user login and maintains handshake with it, data is accessed only when the system authenticates the Bluetooth token received from the mobile device. If the handshake is interrupted or the token cannot be verified, then the system blocks the user access to the data by encrypting the data and logs off the software system.

The main functions of the proposed system are:

1. Encrypts specific data using AES for user.
2. Maintains and ensures handshake with the registered Bluetooth device.
3. Authenticates user upon Bluetooth token.

4.1.3 Use Case Model

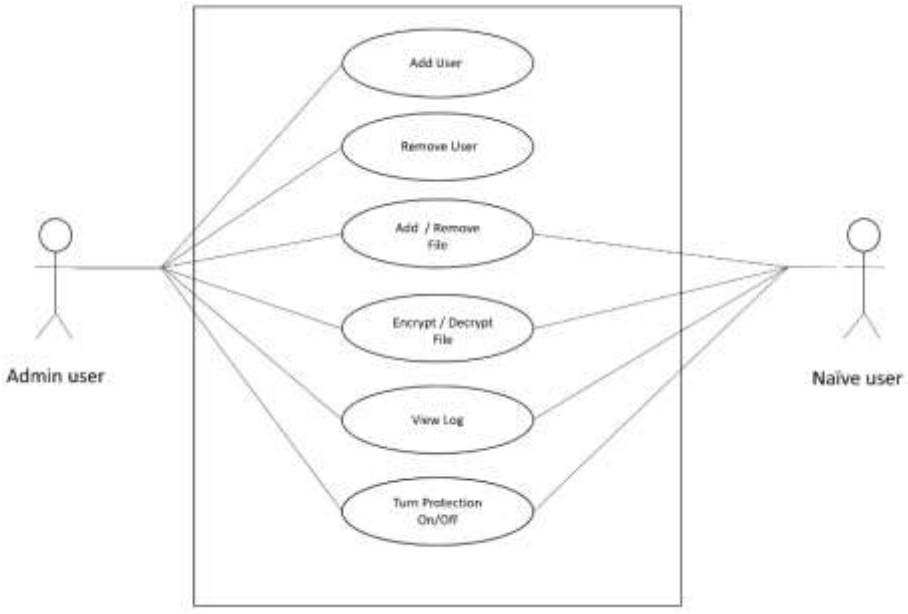


Fig 4.1.1 Use case diagram

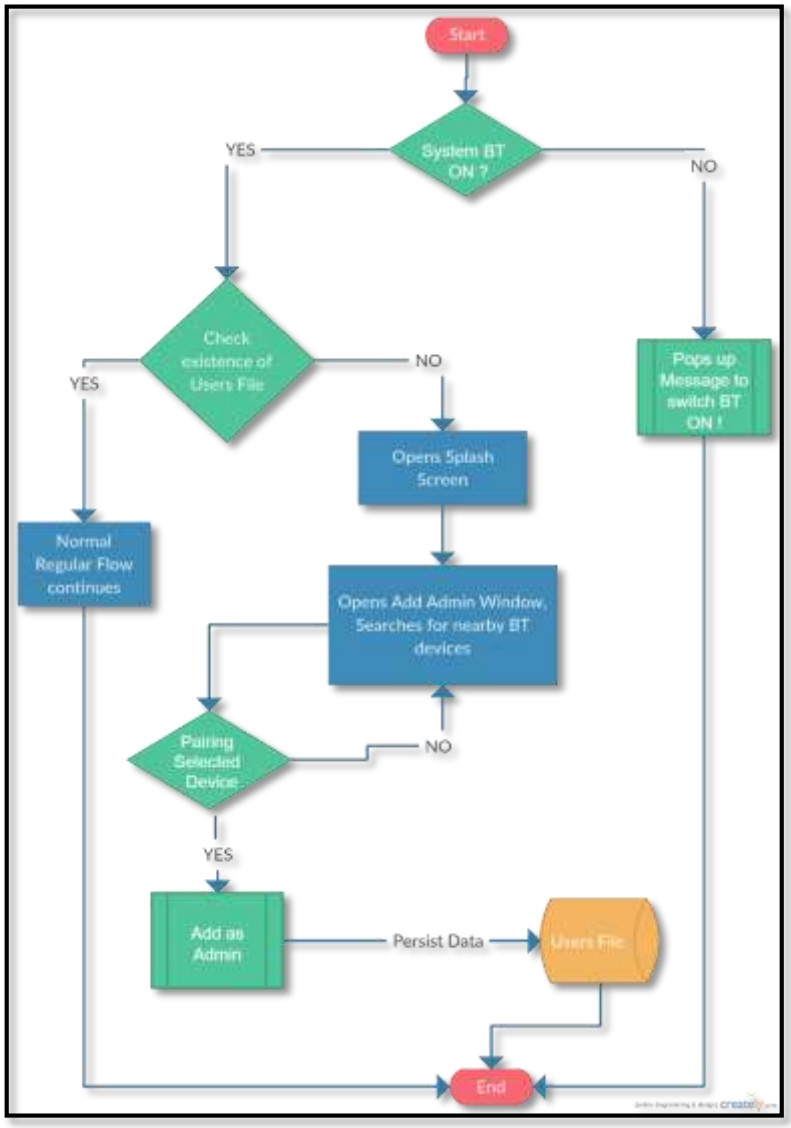
4.2 Conceptual level activity diagram

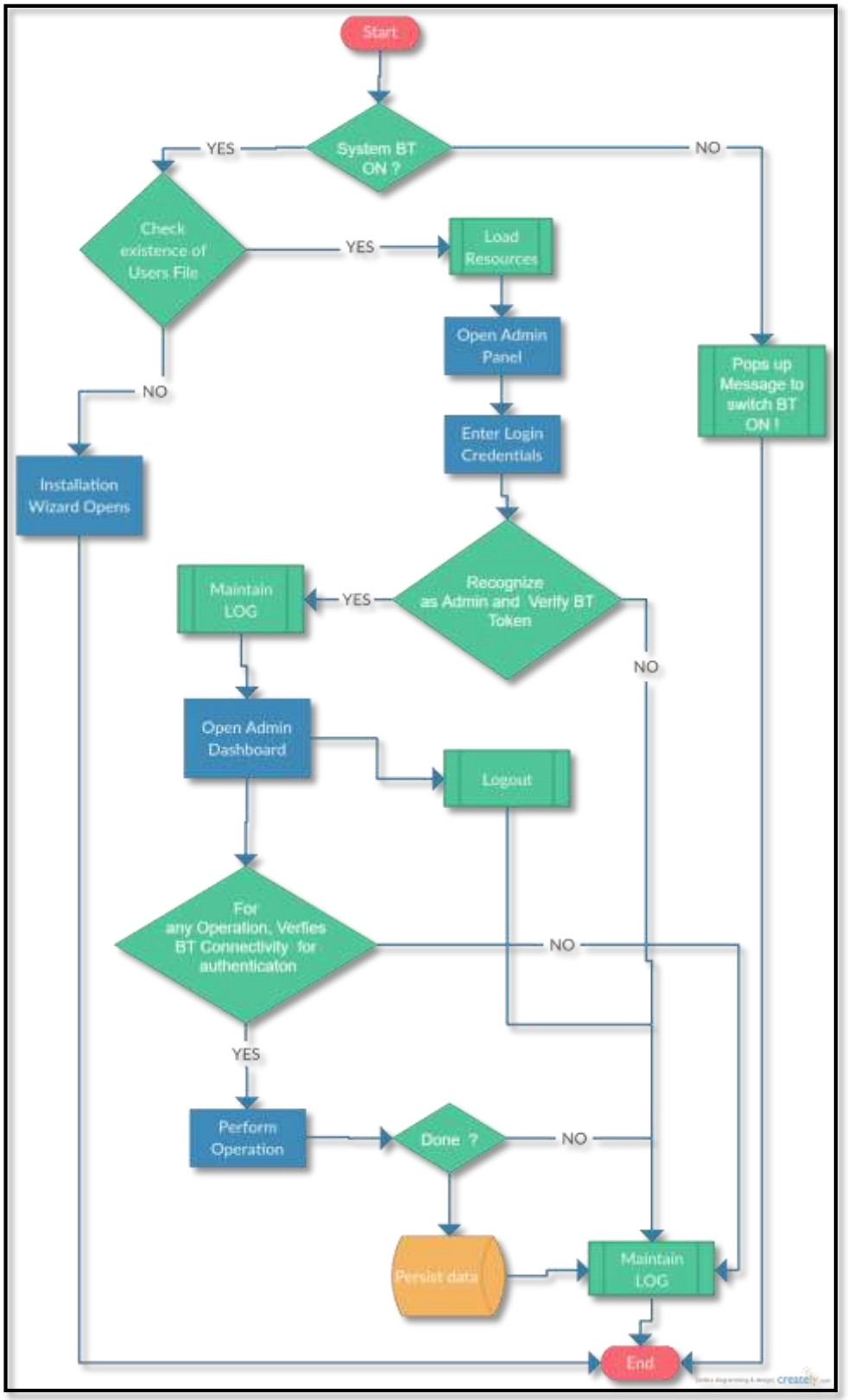
Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams are intended to model both computational and organizational processes (i.e. workflows). Activity diagrams show the overall flow of control. As discussed above, the below is the brief information about the activities happening in our project.

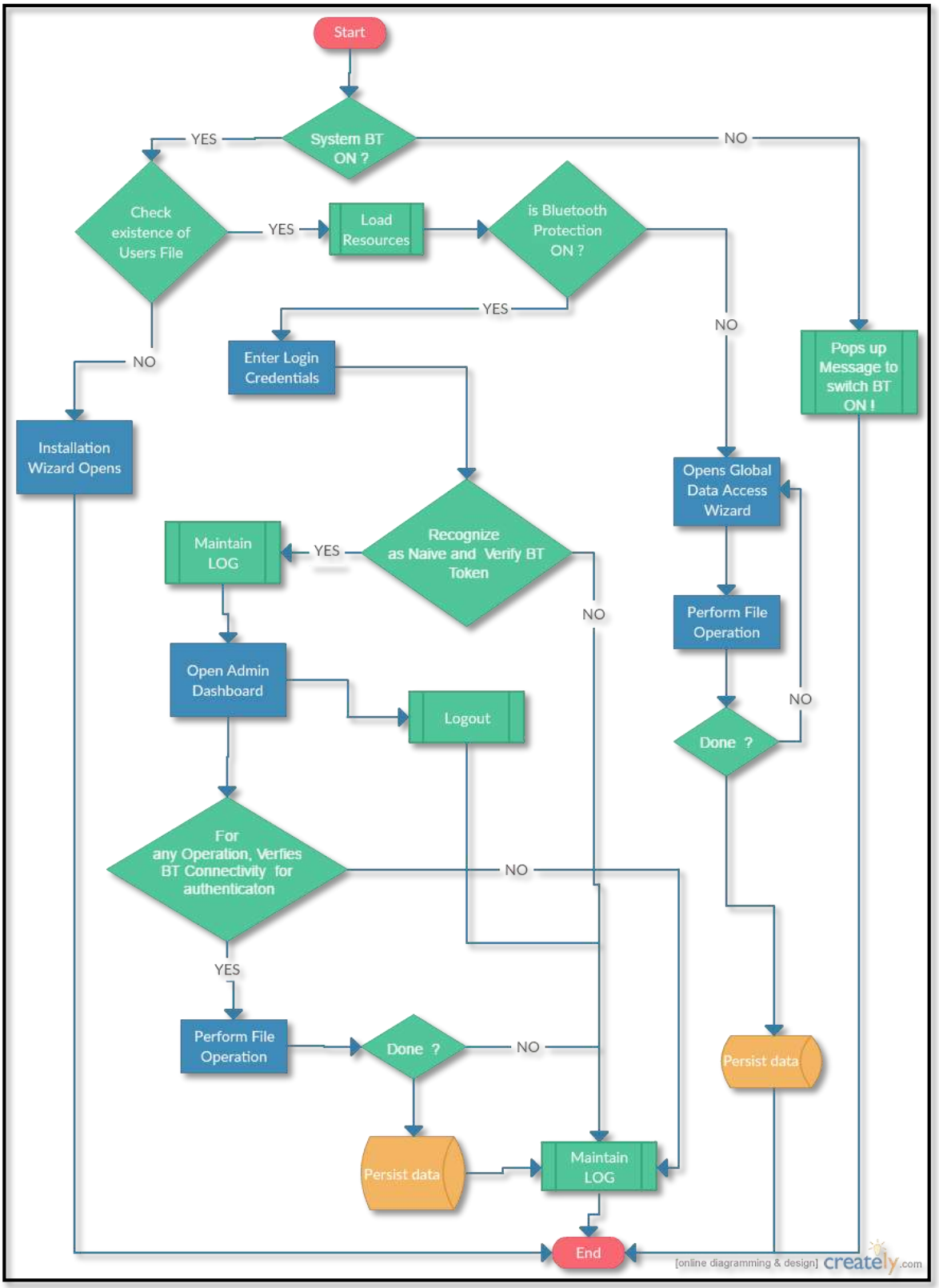
1. The software system starts as a background service as soon as the PC is logged in.
2. As soon as it gets started, when user tries to log in for the registered Bluetooth device against the registered MAC addresses for users using bluetooth friendly name as user ID.
3. If the device is in the range and is found, then the system tries to maintain a handshake with the device, in case the device is not found then nothing happens if someone requests to access it and access log is maintained keeping the data encrypted.
4. The system ensures the handshake just before every operation to be performed, if the handshake gets interrupted in any case, the system makes the data unavailable
5. by simple switching off the utility and again nothing happens and if someone tries to access it then a log stating the timestamp and username of the PC is made in the file inside of the system.
6. If the handshake is maintained and a data request is made then the Bluetooth device is prompted for connectivity token, the token is sent to the system in the PC and if it is yes then the data is accessed with user logs being maintained in the background with the actions being done, if it's a NO or something goes wrong and token cannot be verified to be YES, then the user logs are maintained and data gets encrypted and the utility is switched off.

4.3 Data flow Diagram(Level 0,1,2)

DeskSure has typically three flows in which control can be driven namely, the Admin flow, Naïve flow and Global Access flow, the Flow chart diagrams are shown below from which the programmatic decisions can be easily inferred.




Start
System BT ON ?
YES
NO
Check existence of Users File
YES
Load Resources
Open Admin Panel
Enter Login Credentials
Recognize as Admin and Verify BT Token
YES
Maintain LOG
Open Admin Dashboard
Logout
NO
Pops up Message to switch BT ON !
NO
Installation Wizard Opens
For any Operation, Verfies BT Connectivity for authenticaton
NO
YES
Perform Operation
Done ?
NO
Persist data
Maintain LOG
End


Start
System BT ON ?
YES
NO
Check existence of Users File
YES
Load Resources
is Bluetooth Protection ON ?
YES
NO
NO
Enter Login Credentials
Pops up Message to switch BT ON !
Installation Wizard Opens
Opens Global Data Access Wizard
Maintain LOG
YES
Recognize as Naive and Verify BT Token
NO
Perform File Operation
Open Admin Dashboard
Logout
NO
Done ?
For any Operation, Verfies BT Connectivity for authenticaton
NO
YES
Perform File Operation
Done ?
NO
Persist data
Persist data
Maintain LOG
End
[online diagramming & design] creately.com

CHAPTER 5
SYSTEM MODELING

5.1 Detailed Class Diagram

Class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing, and documenting different aspects of a system but also for constructing executable code of the software application. Class diagram describes the attributes and operations of a class and also the constraints imposed on the system. Class diagram shows a collection of classes, interfaces, associations, collaborations, and constraints DeskSure has a rigid and well architected Class structure, constituting various supporting classes like Resources, Bluetooth, User, Users, UserFile, UserFiles, Log, Logs, and enumerations like FileStatus. Below is the class diagram depicting major classes to be involved in development.

DeskSure comprises of mainly 8 core classes which are:

1. Bluetooth: Provides functionalities to manage the bluetooth stack of the computer system, functions like searchAvailableDevices, pairDevices, etc.

2. Resources: It is one of the most important classes as it makes basis for data manipulation by holding data in instances and also provides secondary functions like fetching file size, providing icon images, etc.

3. User: It merely represents a User entity in the system and is used as a custom data structure.

4. Log: It is also a data structure which represents a single LOG value.

5. UserFile: DeskSure needs file mapping with its users, which cs implemented as a mere data structure called UserFile.

6. Logs, Users and UserFiles are the classes which holds multiple instances of Log, User, and UserFile respectively and facilitates IO operations with data on disk like saving retrieving, manipulating, etc.

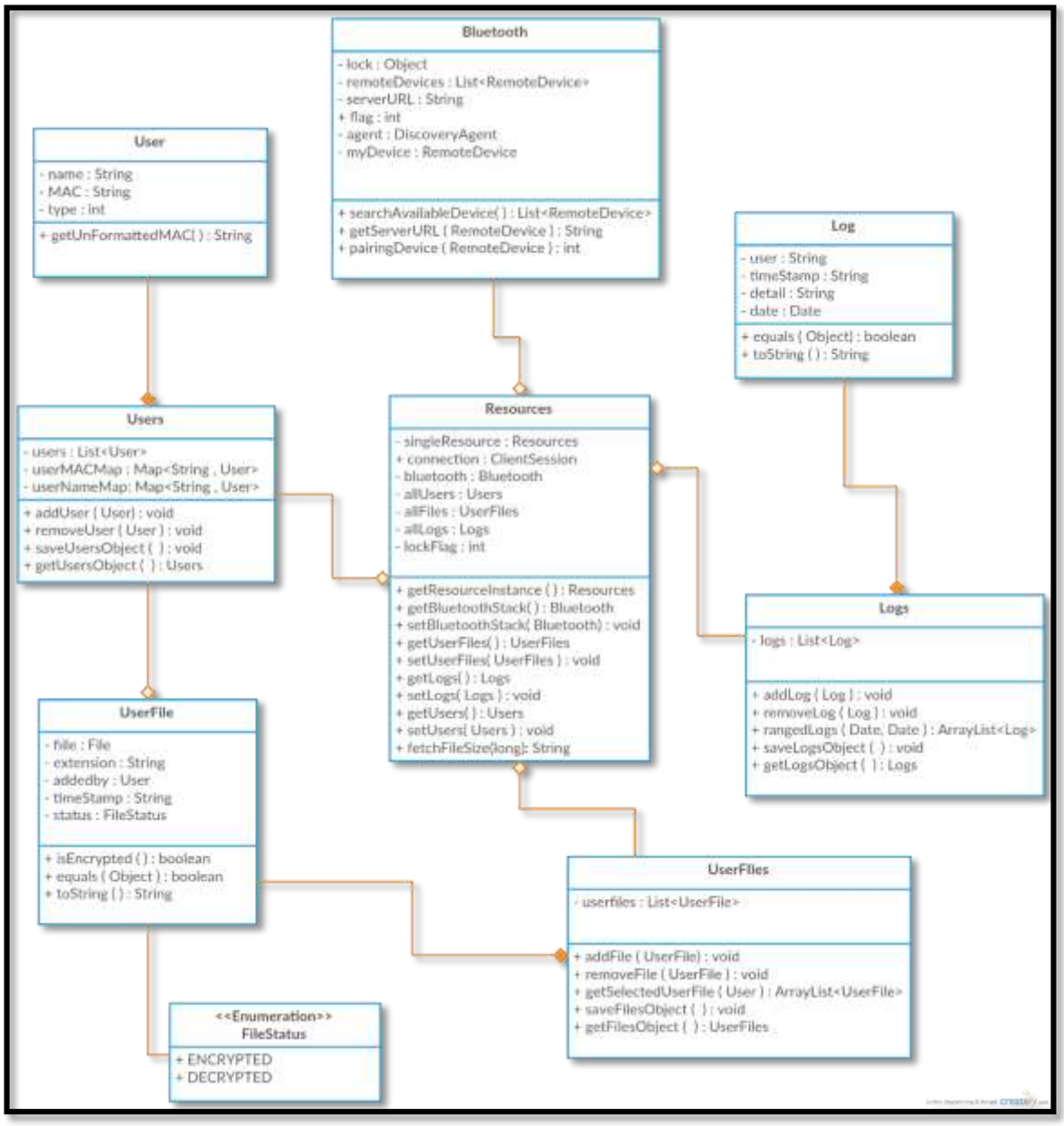


Fig 5.1 - CLASS DIAGRAM OF DESKSURE

5.2 Interaction Diagram

5.2.1 Sequence Diagram

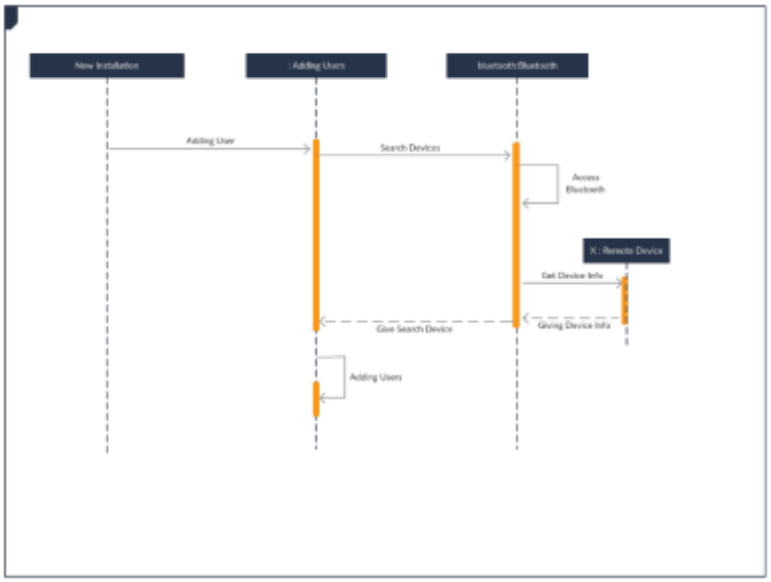


Fig 5.2.1 Adding user on new Installation

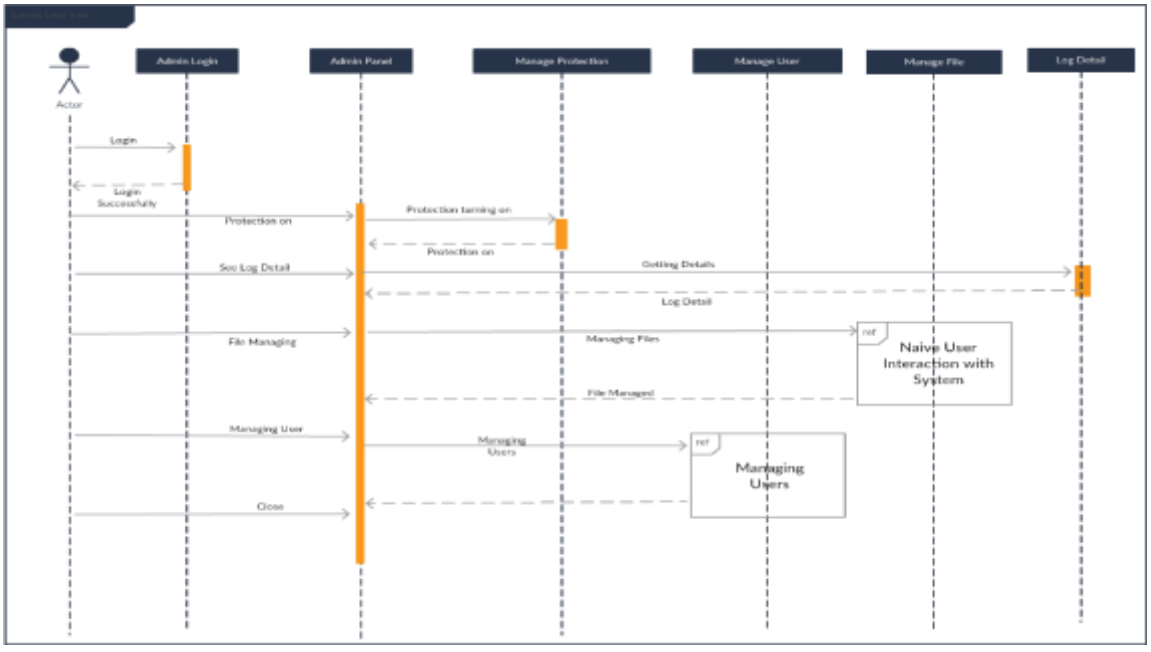


Fig 5.2.2 Admin Interaction to the System

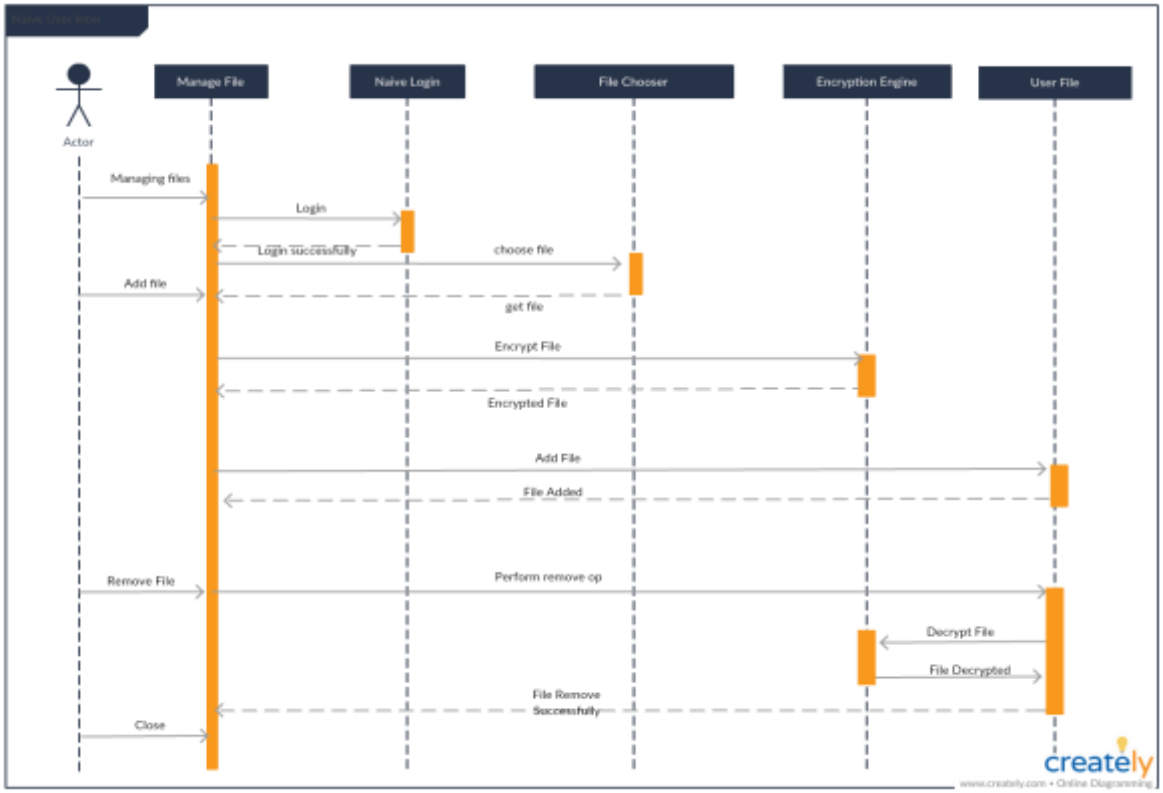


Fig 5.2.3 Naïve user Interaction to the System

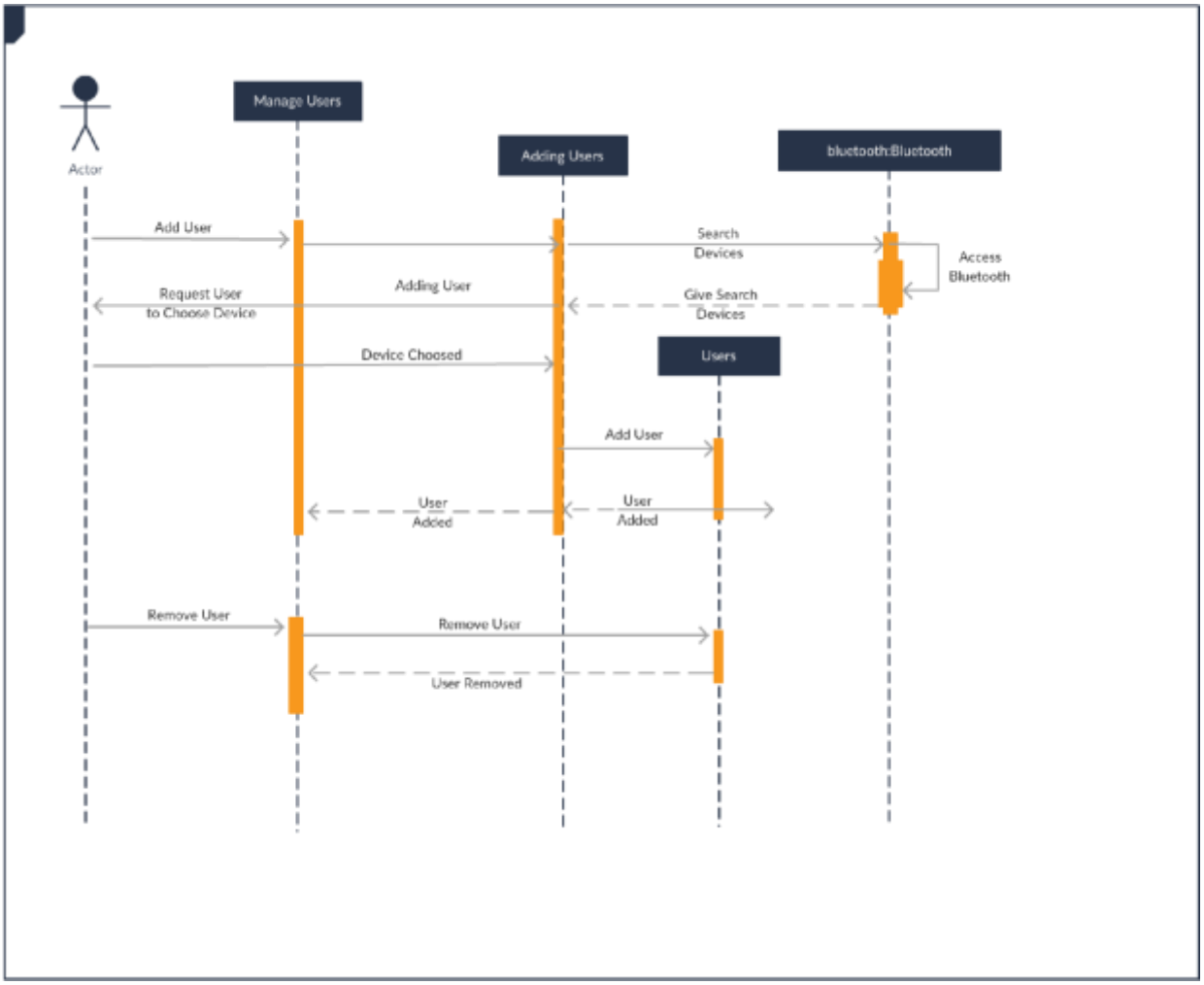


Fig 5.2.4 Manage user Interaction

5.2.2 Collaboration Diagram

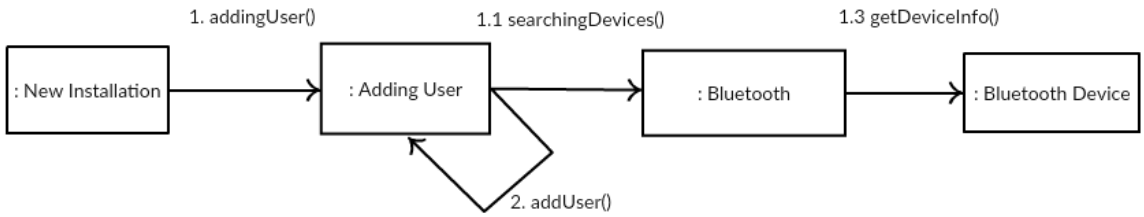


Fig 5.2.5 Add user on new Installation

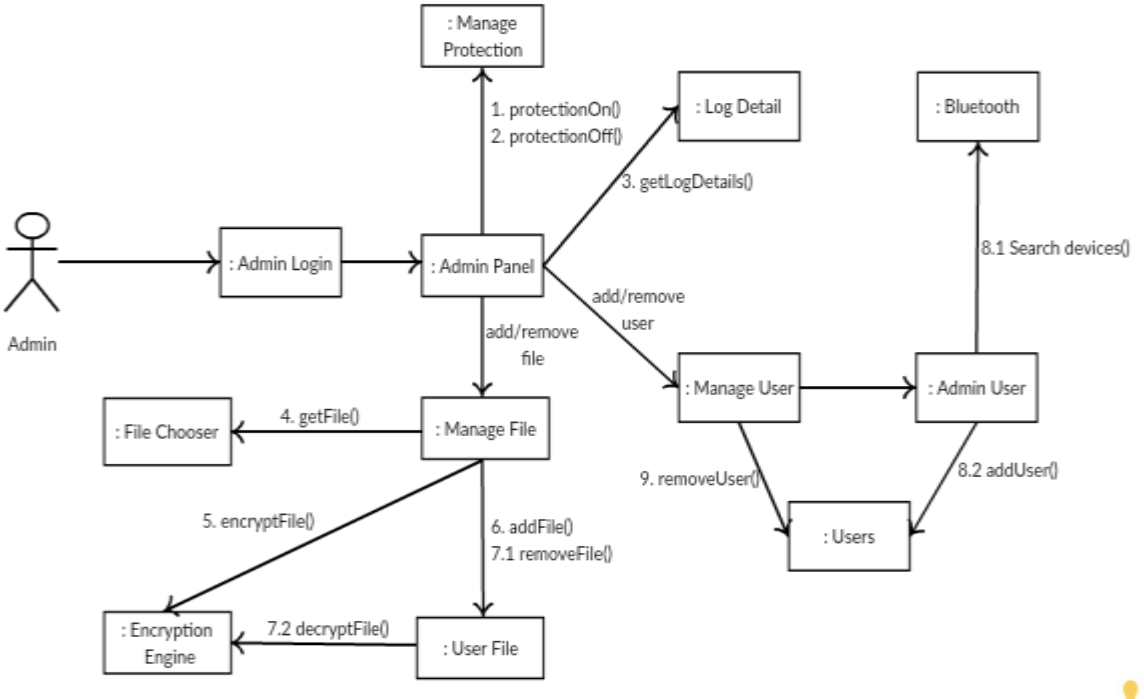


Fig 5.2.6 Admin Interaction to the System

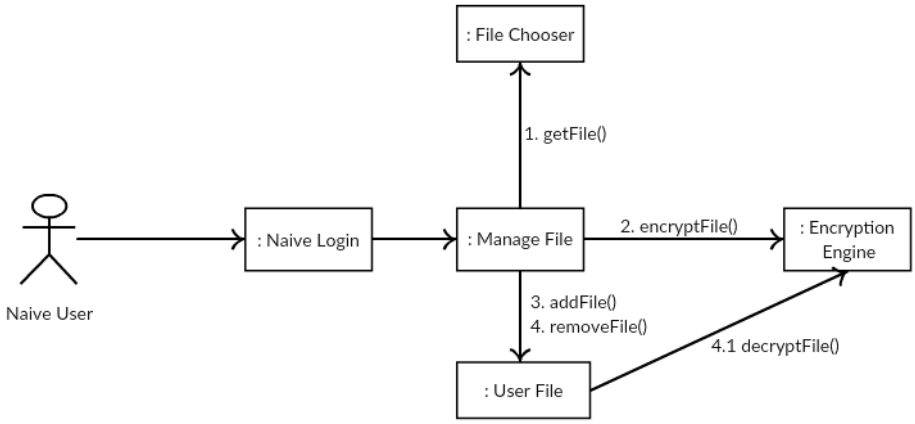


Fig 5.2.7 Naïve user Interaction to the System

5.3 State Diagram

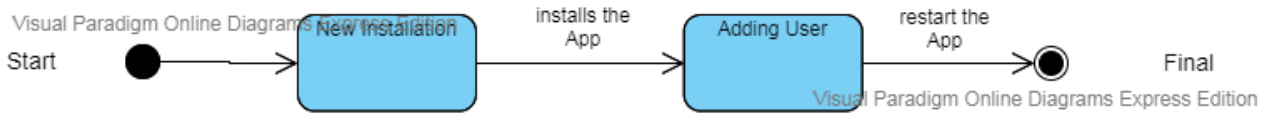


Fig 5.3.1 Installation state Diagram

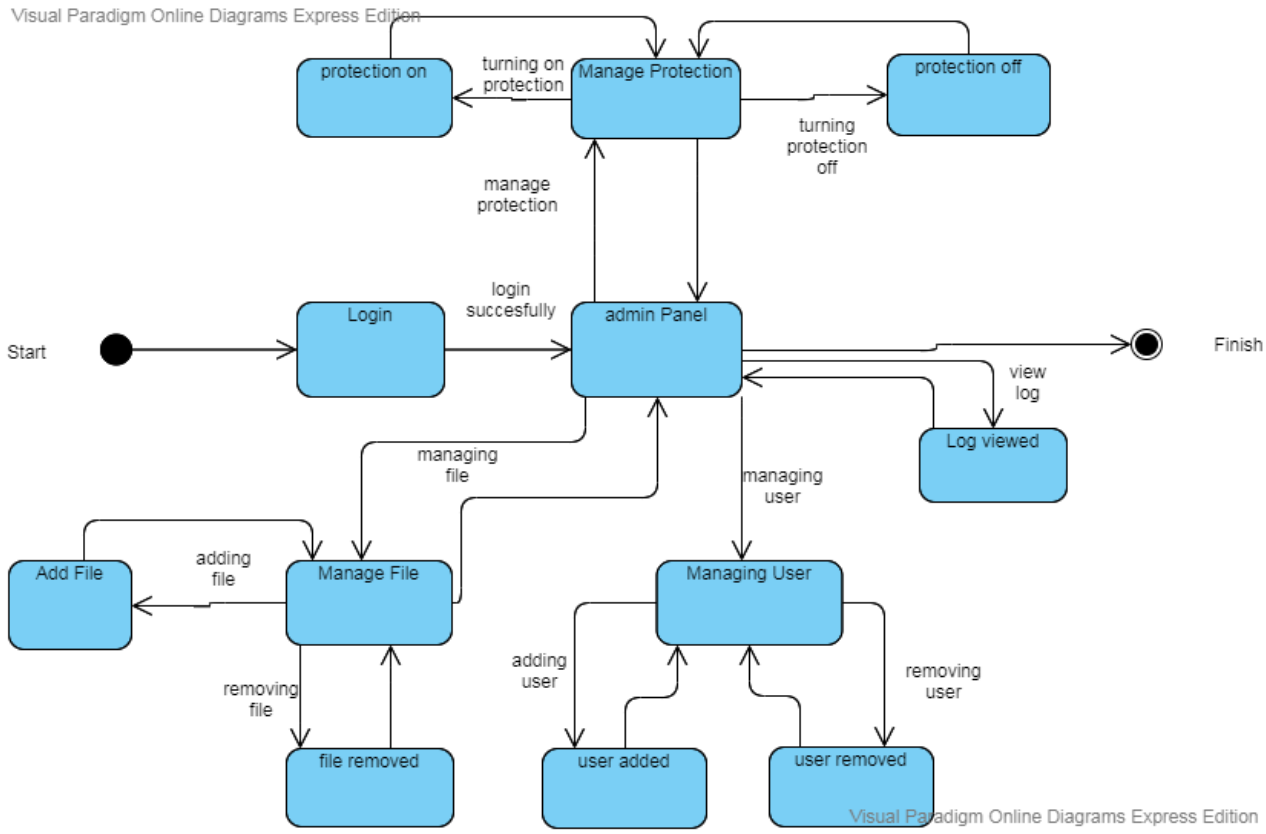


Fig 5.3.2 Admin state Diagram

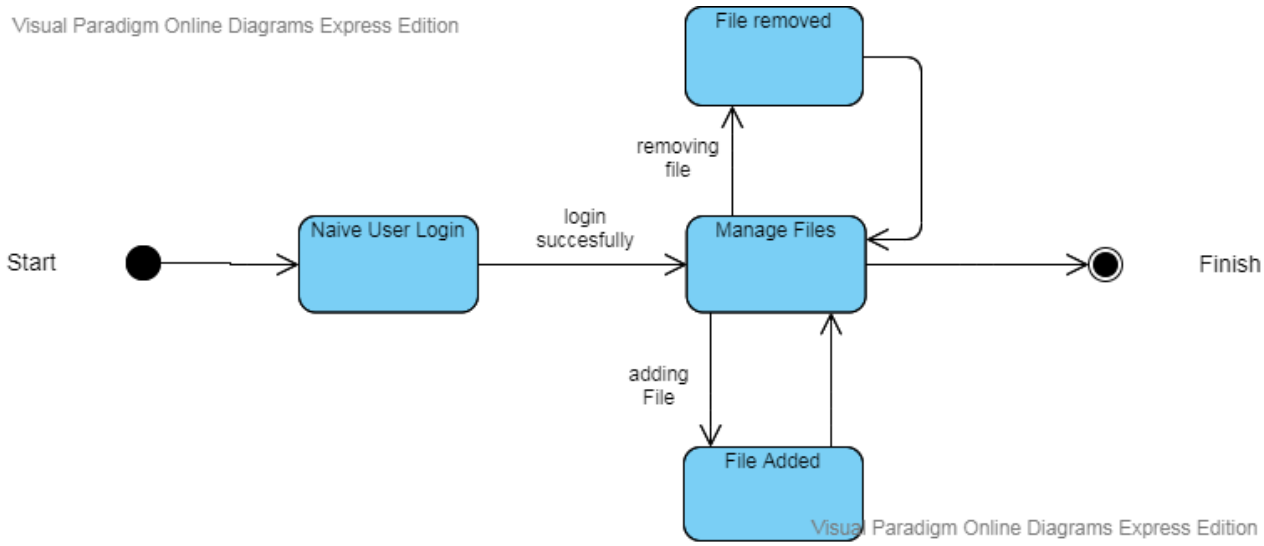


Fig 5.3.3 Naïve user state Diagram

5.4Activity Diagram

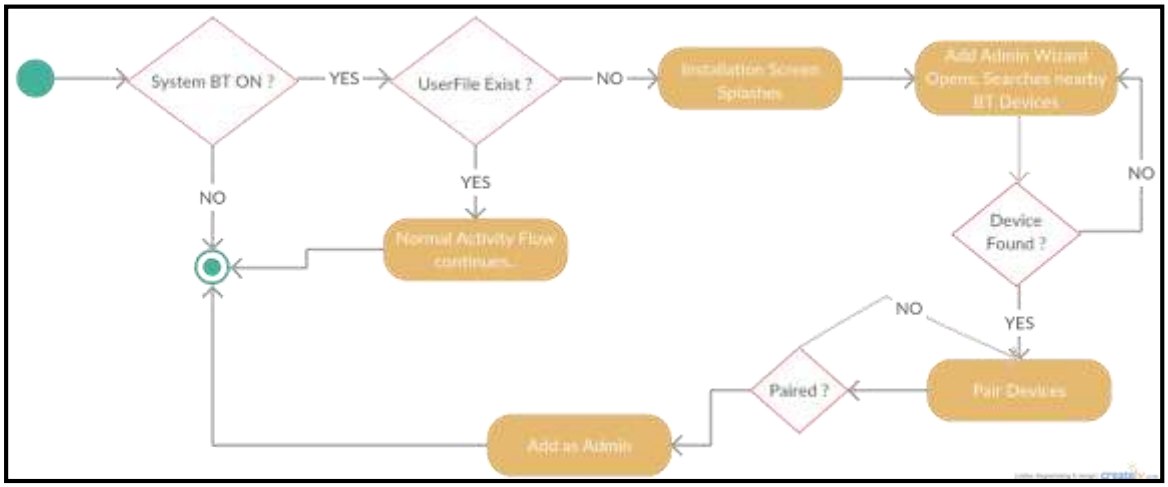


Fig 5.4.1 - ACTIVITY DIAGRAM FOR FIRST TIME ACCESS OF SOFTWARE

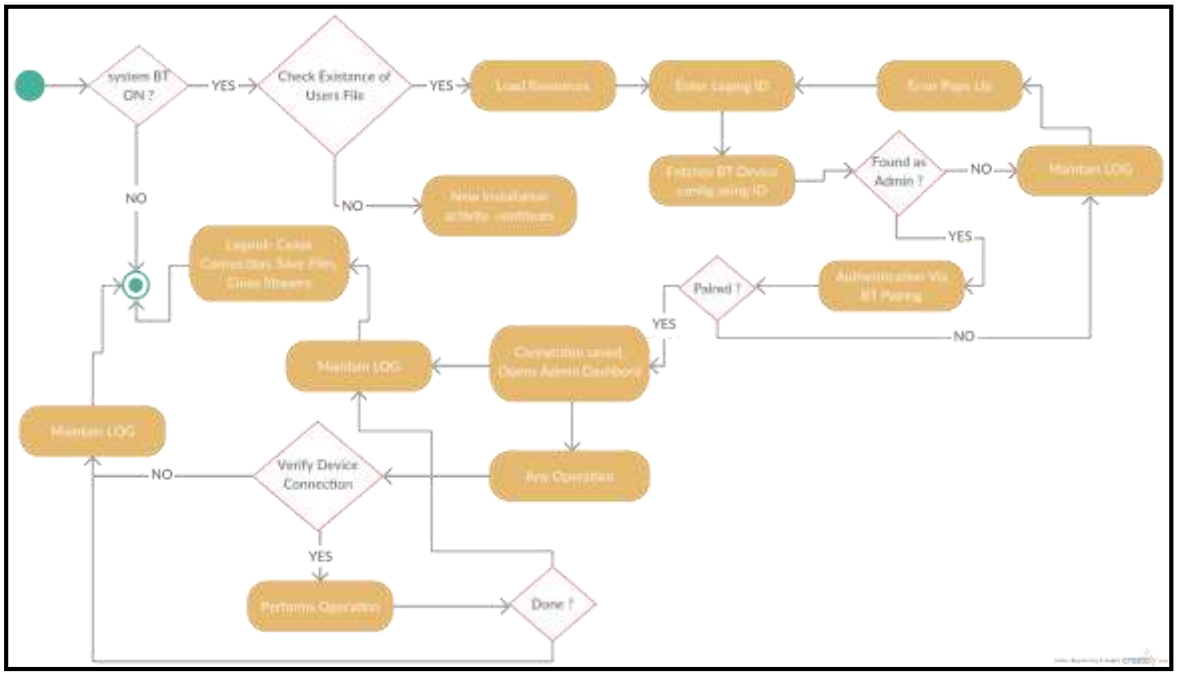


Fig 5.4.2 - ACTIVITY DIAGRAM FOR ADMIN USER ACCESS

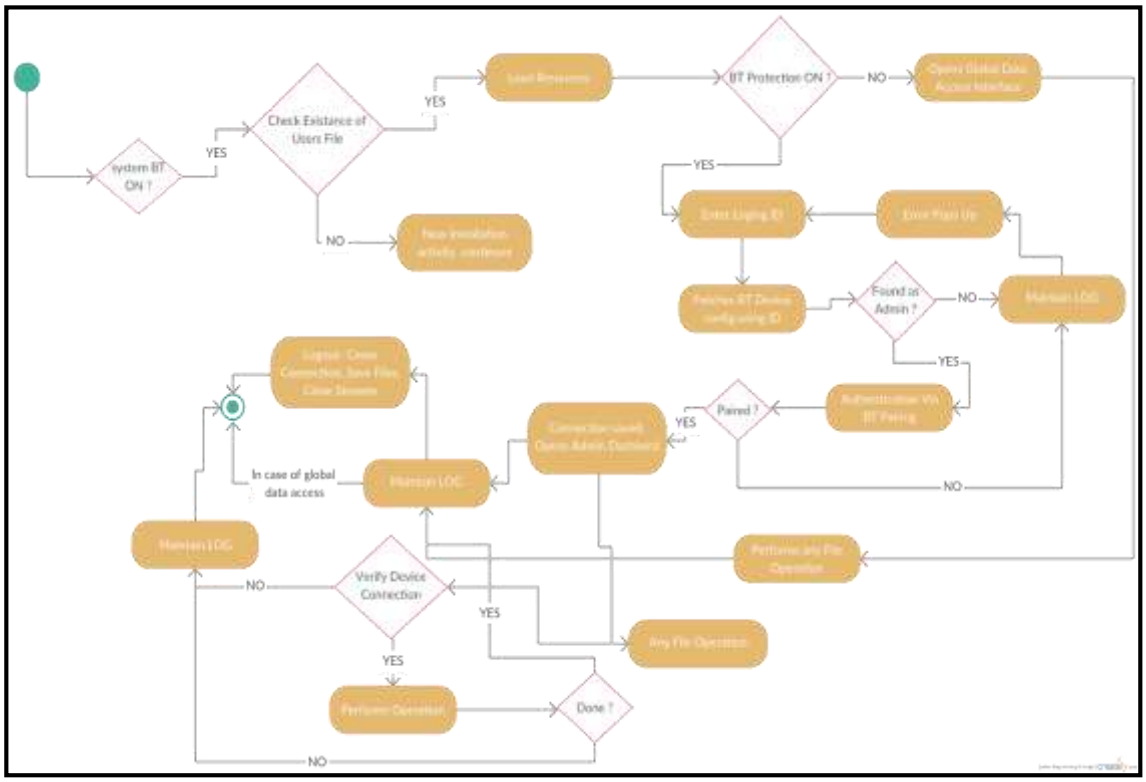


Fig 4.3 - ACTIVITY DIAGRAM FOR NAIVE USER ACCESS

5.5 Testing

Test case design of DeskSure is divided in three major categories which are naive user test cases, admin user test cases and the login or registration test cases.

Login Test Cases:

Test Id	Test Case Description	Input	Expected Results	Actual Results	Status
01.	Login attempt without any user data	Username	No such user present	Not a valid user	Pass
02.	Login attempt when PC bluetooth is off	Username	Asked to Switch ON	Please switch on Bluetooth device	Pass
03.	Login attempt while mobile bluetooth device is not present	Username	No Bluetooth device found	Please switch on your BT.	Pass
04.	Login attempt with both bluetooth device on	Username	Window Dashboard	User Present	Pass
05.	Login with an invalid username	Username	No such user found	Invalid user	Pass
06.	Login with correct username and bluetooth device off	Username	Valid User Access	Please Switch on your bluetooth device	Pass

Admin Test Cases:

Test Id	Test Case Description	Input	Expected Results	Actual Results	Status
01.	Manage Protection (previously on)	Click on mange protection icon.	Bluetooth Protection OFF	Unlock	Pass
02.	Manage Protection (previously off)	Click on manage protection icon.	Bluetooth Protection On	Lock	Pass
03.	Add User	Click on add user icon of admin dashboard.	List of available user to add	New window open to add user	Pass
04.	Manage User	Click on Manage User icon.	Functionalities of add / remove user	Window open's which gives all such functionalities	Pass
05.	Add File To Encrypt	Click on Add File icon.	Admin will be able to add any file to encrypt	A browsing window will be open with such functionality.	Pass

06.	Manage files	Click on Manage Files icon	Admin will be will be able to encrypt or decrypt file	Window open's give buttons for encrypt decrypt and other facility.	Pass
07.	View User Logs	Click on the view log icon.	Admin will be able to see all the related logs of the naïve user	Log window open's providing all such functionalities	Pass
08.	When file doesn't exist in computer system.	Chooses encrypted file decrypt.	Shows a alert box.	File doesn't exist in the location.	Pass
09.	When admin remove's any user.	Chooses user to remove.	All files which are encrypted by that naïve user also be decrypted.	Performed same as expected.	Pass
10.	When admin remove's any user with some encrypted file missing.	Chooses user to remove.	Show's an Alert box with decryption.	Alert box displayed with the warning	Pass
11.	Operation performed when connection lost after login into the software.	Make connection lost.	Prevention from such access.	Message for connection lost & software shuts off	Pass (sometimes lag)

12.	Operation performed when the Bluetooth of the system is OFF	Make Bluetooth OFF	Shows error dialog.	window open that demands for Bluetooth connection	Pass

Naive Test cases:

Test Id	**Test Case Description**	**Input**	**Expected Results**	**Actual Results**	**Status**
01.	Manage files option for naïve user	Username of naïve user	Functionalities of naïve user	Naïve user dashboard open's (myfiles)	Pass
02.	Add File by Naïve user	Click on add file	File selection and then encryption of that file.	Window open's to choose and encrypt the file	Pass
03.	Remove File by Naïve User	Click on remove files	File selection and then decryption	File selected from the log of encrypted file and then remove it.	Pass
04.	Status of Encryption and decryption	Choose file to view status of the file.	Show status at bottom	Shows Status- ENCRYPTED/ DECRYPTED	Pass

05.	Show details of the chosen file	Choose file to know the details of it.	Details like size, format etc.	Sidebar shows all details	Pass
06.	When file doesn't exist in computer system.	Chooses encrypted file decrypt.	Shows a alert box,	File doesn't exist in the location.	Pass

In development of DeskSure, both, Proactive and Reactive testing approaches have been used. In proactive testing, the basic building blocks were tested against desired development and cooperation with the needs and requirements, such as bluetooth stack management, encryption decryption that needed IO to work smooth. In acceptance testing, DeskSure successfully met all the desired functionalities which were arose during SRS development. **Unit Testing**

The objective of Unit Testing is to test a unit of code (program or set of programs) using the Unit Test Specifications, after coding is completed. Since the testing will depend on the completeness and correctness of test specifications, it is important to subject these to quality and verification reviews.

Input:

- Unit Test Specifications Code to be tested. Testing Process:
- Checking for availability of Code Walk-through reports which have documented the existence of and conformance to coding standards.
- Review of Unit Test Specifications
- Verify the Unit Test Specifications conform to the program specifications.
- Verify that all boundary and null data conditions are included.

While implementation, the minimal implementations, like Encryption Engine, handling IO to save and retrieve data instances, were tested individually on

Integration Testing

After completion of our module along with testing, modular coding strategy was used. After integrating the module with the complete application, time was given

to our team to test their part of module completely and thoroughly. As the whole application is divided into several modules, there were a lot of variable names and function names, which were common to all the modules. There existed a lot of variables, which we had to incorporate into our module, but as different modules were being developed simultaneously we had to hard code things in place of the session variables in our module. So at the time of integration a lot of hard coded things had to be removed and variables were replaced.

CHAPTER 6
CONCLUSION & FUTURE WORK

6.1 Limitation of the Desksure

As similar to all the software presents in the market DeskSure also have some limitation which are problematic in some manner. Limitations are as follows:

- If someone changes the path or rename or delete the encrypted file then the software system will not be able to recognize the changes and will return 'File not Found' error in form of popup when the user of any kind tries to decrypt that particular file on which changes are made.
- One of the concerning limitation of DeskSure is that it is hardware dependent. DeskSure depends on the Bluetooth device of the system which is the hardware part and our software only used the services of those hardware. If that hardware lacks in time and working then it reflects in the working of the software. It is a concerning topic and at present there is no outcome of that limitation.
- DeskSure is a hardware dependent software means is it is dependent on the Bluetooth device, Main Memory, and processing speed of the computer system. All these things add some limitation to DeskSure. It doesn't allow it to encrypt very large data due to the need of main memory. That dependency on the memory set a range of size of file as per the system.

6.2 Future Enhancement

We are very concerning towards the future scope of the DeskSure application. We targeting many modules and to expand the range of the application. We are also concerned about the limitation of the DeskSure and try to overcome it.

- As today's world is growing towards the internet we are also targeting to make it available through internet so anyone who wants to protect its data from long range can use its facilities of encryption.

- In present DeskSure is using AES-128 bit encryption to encrypt the selected file and we targeting to make it wider and also implement it over the AES-192 and AES-256 encryption.
- DeskSure is a hardware dependent application and in future we are targeting to reduce the dependency on main memory such that file of any size can be encrypted on the DeskSure.
- One of the limitation of the DeskSure is that anyone from the outer world can delete the encrypted file of the users from the system and there is no way to retrieve them so we targeting to perform a watch over it. That watch on the encrypted file ensures that no one can edit and modify that encrypted file so once a file is encrypted it can also be protected from the external threat.
- We are also targeting to make it available from low-end devices to the high-end devices such that it can be easily available for every one with all its functionalities.

CHAPTER 7
BIBLIOGRAPHY & REFERENCES

7.1 Reference Books

Bluetooth for Java – Bruce Hopkins and Ranjith Antony.

7.2 Other Documentations & Resources

http://bluecove.org/

https://www.oracle.com/technical-resources/articles/javame/bluetooth-wirelesstechnology-part1.html

http://www.aviyehuda.com/blog/2010/01/08/connecting-to-bluetooth-devices-withjava/comment-page-1/

7.3 Snapshot

7.3.1 Installation Process

Fig 7.3.1 Installation Window

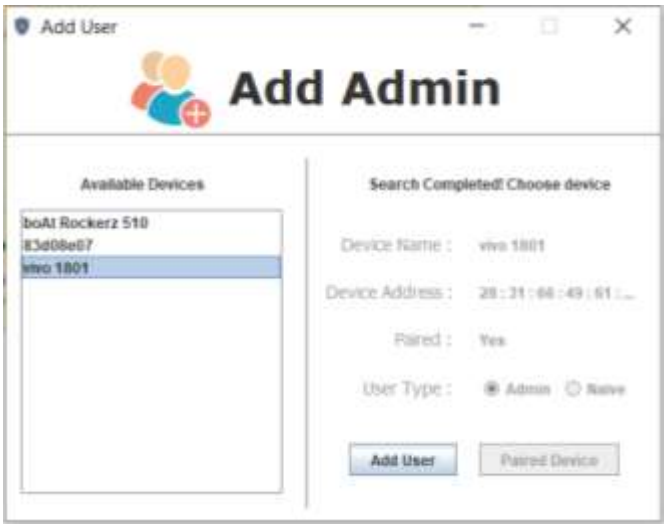


Fig 7.3.2 Adding Admin first time

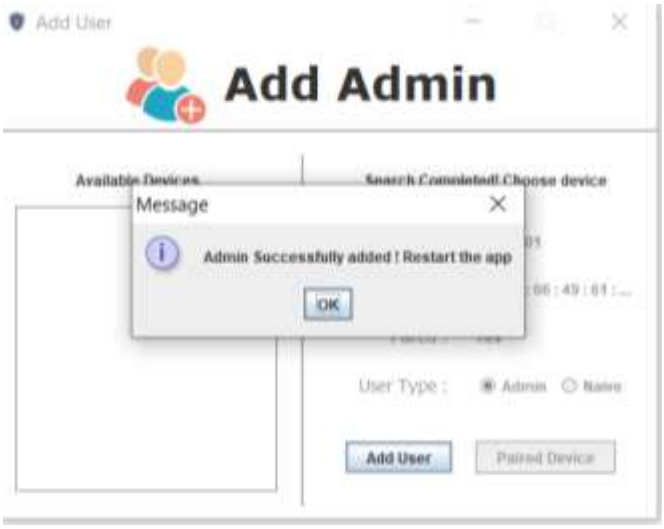


Fig 7.3.3 Admin successfully added

Fig 7.3.4 - Desksure starts on system tray

7.3.2 Admin Uses Process

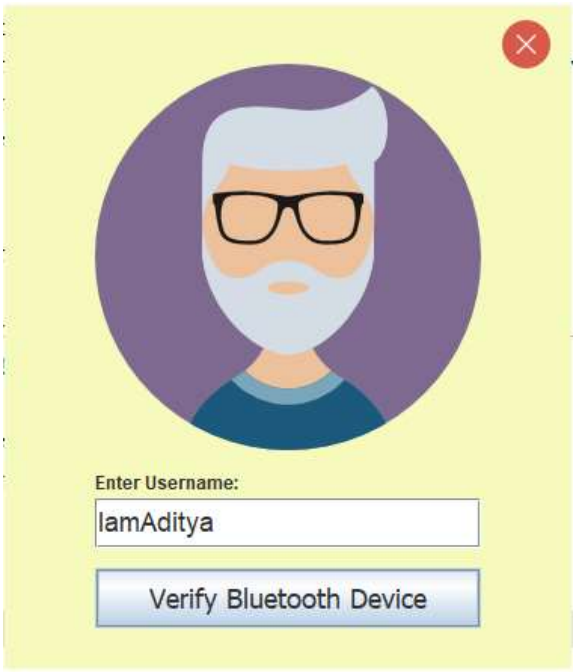


Fig 7.3.5 – Admin Login

Fig 7.3.6 – Admin Panel

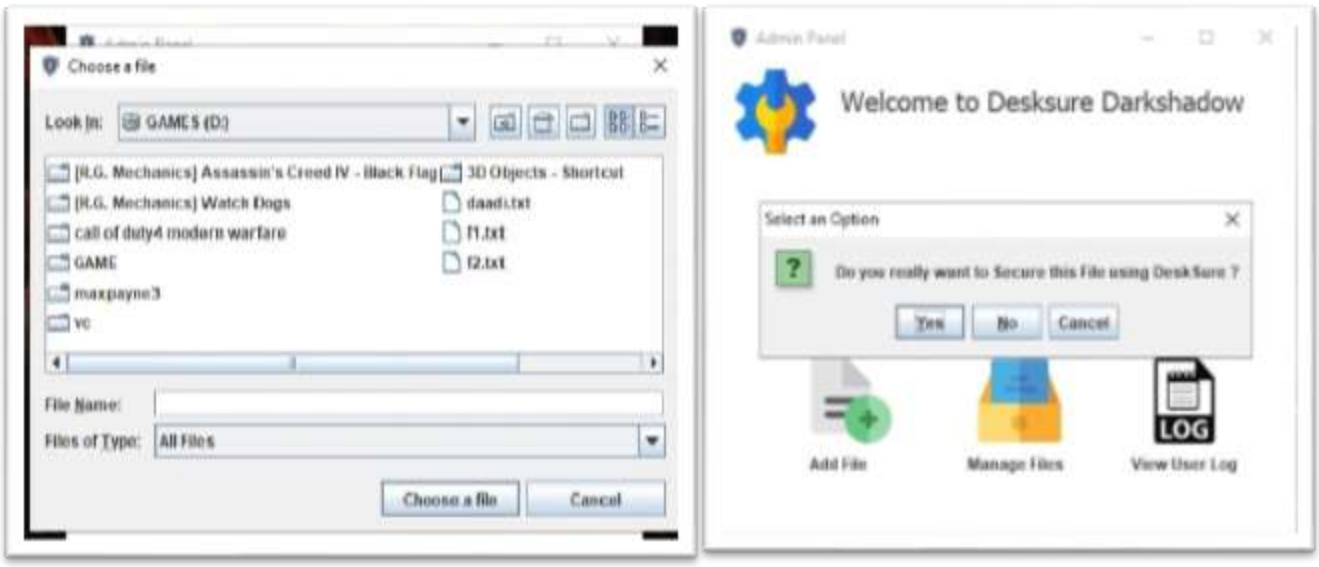
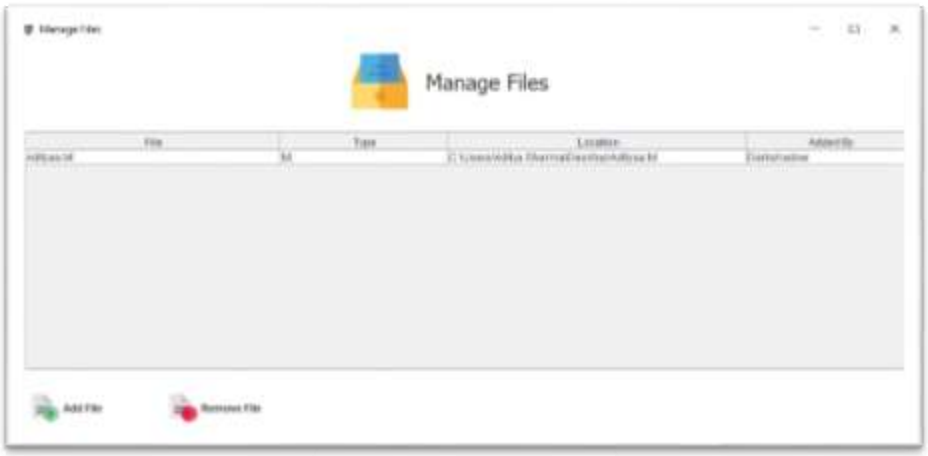


Fig 7.3.7 – Adding file



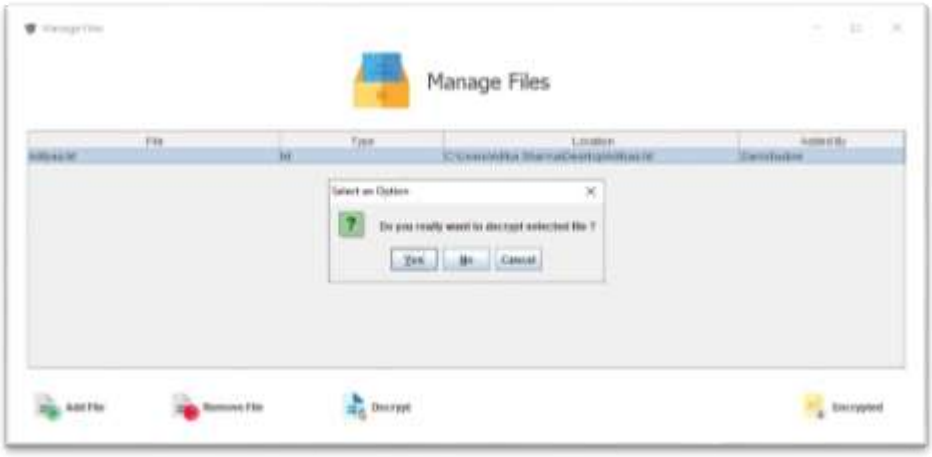


Fig 7.3.8 – Manage file window

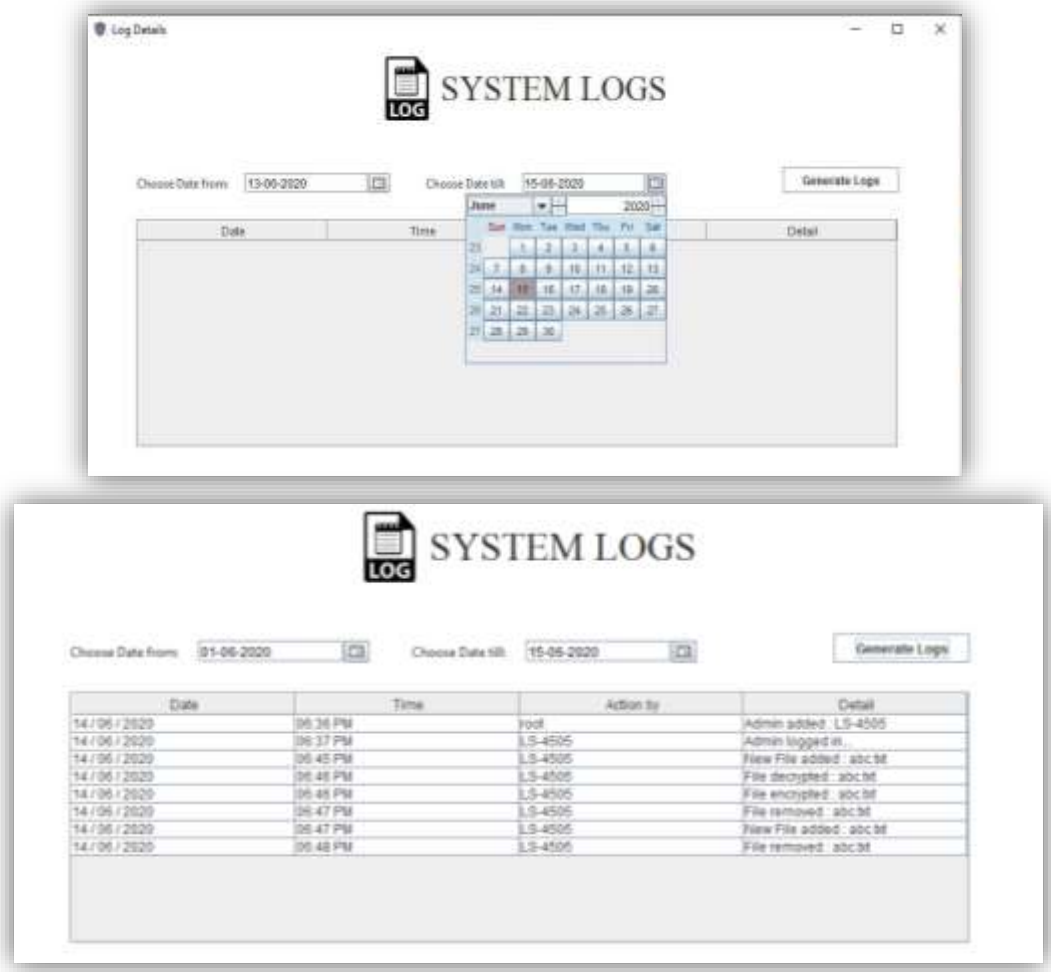
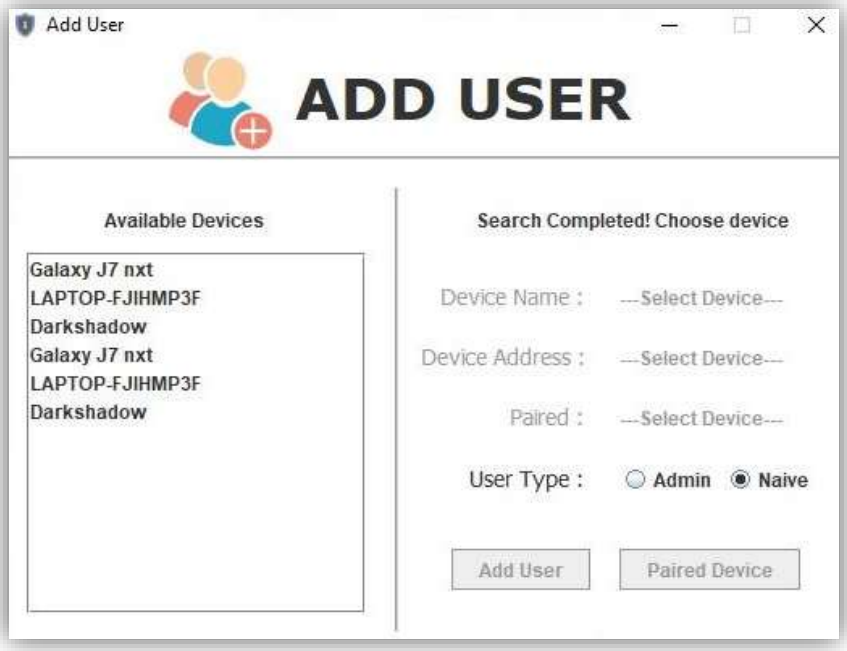


Fig 7.3.9 – Viewing log detail



7.3.3 Naïve User Uses process

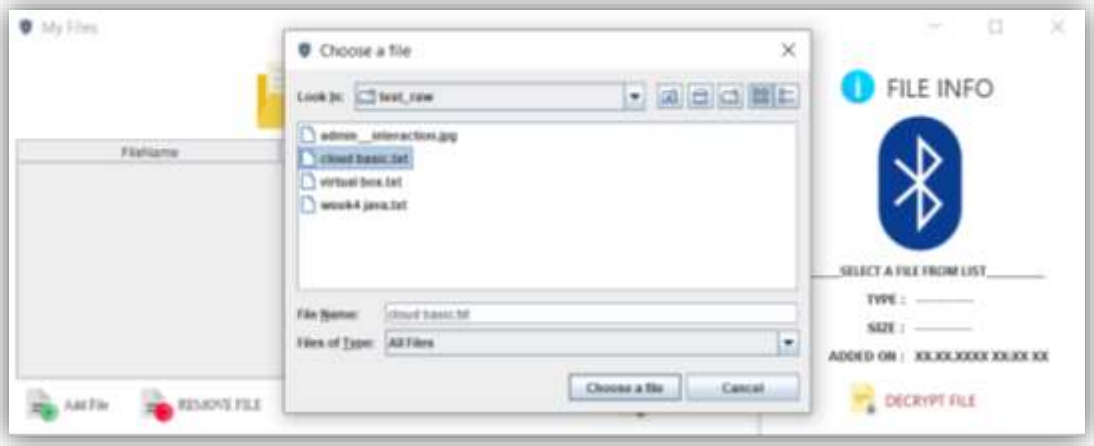


Fig 7.3.11 – Adding new user to system

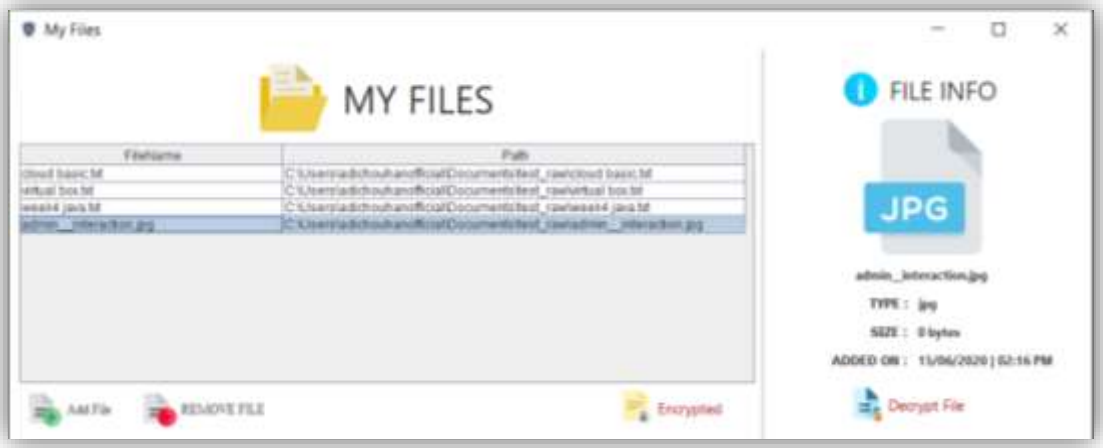


Fig 7.3.12 – Naïve user File management window