



SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
COLLEGE OF COMPUTER SCIENCE AND INFORMATION
TECHNOLOGY
COMPUTER SYSTEMS AND NETWORKS

FILE SECURITY MANAGEMENT

THESIS SUMMITTED AS A PARTIAL REQUIREMENTS OF B.Sc. (HONOR)
DEGREE IN INFORMATION TECHNOLOGY AND NETWORK

November 2017

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**SUDAN UNIVERSITY OF SCIENCE AND
TECHNOLOGY
COLLEGE OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY
COMPUTER SYSTEMS AND NETWORKS**

FILE SECURITY MANAGEMENT

Prepared by:

Mosab Hashim Hassan

Omer Mustafa Ali

Alshaikh Diya-aldeen

Supervisor:

Intisar Mohammed El-haj

Supervisor Signature:

.....

Date:

November 2017

الآية

قال تعالى:

(وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ)

صدق الله العظيم

سورة هود الآية (88)

الحمد لله

اللهم إن نعمك كثيرة علينا لا نحصي ثناءً عليك ولا نقدر وأنت سبحانك كما أثنيت
على نفسك وأنت سبحانك غني عن العالمين
اللهم لك الحمد و الشكر كما ينبغي لجلال وجهك و لعظيم سلطانك و علو مكانك
سبحانك ياربنا لك الحمد و الشكر حمداً كثيراً طيباً مباركاً فيه

DEDICATION

We thank Allah for blessing us with the chances that guided us
here to accomplish this project in time

Nothing can be said to satisfy our family's efforts for what
they put in to grow us up and treat us right to produce who we
are now

And we would like to dedicate this humble effort for our
families, teachers and most importantly our loving parents for
being there the whole time to support us.

ACKNOWLEDGEMENT

First and last Praise is to Almighty Allah.

We would love to thank everyone who encouraged us to achieve this tremendous task. Especially our parents who believed in us that we could achieve such a thing.

Our families, thank you for believing in us, please do not ever doubt our dedication and love for you.

Acknowledge a special thanks to our supervisor teacher **Intisar Mohammed el-haj** for all her effort and guidance towards us.

Highly appreciate the efforts expended to everyone that helped us to finish this research.

Abstract

Information security is the protection of data against external attacks, malware and unauthorized access by detecting, preventing and responding to these threats.

In this project a windows application was developed that allows the user to control the critical data to be encrypted/decrypted using a specified key, that holds a unique identifier which is a serial number of the USB or address of the Device's Bluetooth, By registering necessary information from the user, Any data encrypted data using this application can't be decrypted by another user or application. TDES algorithm is used to encrypt and decrypt process. This application allows the user to edit his personal information and keys and also recover the keys using a verification E-mail on his registered E-mail.

This application is developed using Microsoft visual studio with the help of .NET Framework. And C# as a programming language that provides ManagementObjectSearcher, BluetoothDeviceInfo classes and 32FEET.NET package.

The output of this project is an executable windows application that allows the users to secure their files.

In the future work it's proposed that this software is implemented across web platform to support cross-platform operation and provide more availability to the user.

المستخلص

أمن المعلومات هو حماية البيانات من الهجمات الخارجية، والبرمجيات الخبيثة والوصول غير المصرح به عن طريق الكشف و منع والرد على هذه التهديدات.

في هذا المشروع تطوير تطبيق ويندوز الذي يسمح للمستخدم بالتحكم في بياناته الهامة ليتم تشفيرها و فك تشفيرها باستخدام مفاتيح محددة، وهي عبارة عن معرف فريد للناقل العالمي التسلسلي او عنوان جهاز البلوتوث ومن خلال تسجيل المعلومات الضرورية من المستخدم، لا يمكن فك تشفير بيانات شفرة بهذا البرنامج من قبل مستخدم آخر أو تطبيق آخر وتستخدم خوارزمية التشفير TDES في عملية التشفير وفك التشفير و يسمح هذا التطبيق للمستخدم بتحرير معلوماته الشخصية ومفاتيحه، أيضا يمكنه من استعادة مفاتيحه باستخدام البريد الإلكتروني المسجل مسبقاً.

تم تطوير هذا التطبيق باستخدام مايكروسوفت فيجوال استديو بمساعدة إطار العمل NET. Framework و C# كلغة برمجة توفر ManagementObjectSearcher، BluetoothDeviceInfo classes و حزمة 32FEET.NET.

مخرج هذا المشروع هو تطبيق ويندوز القابل للتنفيذ يسمح للمستخدمين بتأمين الملفات الخاصة بهم. لتطوير هذا النظام يقترح تطويره عبر الويب ليستطيع المستخدم الوصول لبياناته المحمية عبر جميع اجهزته و في كل الاوقات لزياده إتاحة البيانات للمستخدم بصورة عامه

List of Terms

Term	Description
2TDEA	2-key Triple Des Encryption Algorithm
3TDEA	3-key Triple Des Encryption Algorithm
AES	Advanced Encryption Standard
API	Application Programming Interface
CIA	Central Intelligence Agency
CPU	Central Process Unit
DES	Data Encryption Standard
E-mail	Electronic Mail
EFS	Encrypting file system
FIPS	Federal Information Processing Standard
FUSE	File Systems in User Space
IBM	International Business Machines
ID	Identifier
IDE	Integrated Development Environment
IOS	iPhone Operating System
IrDA	Infrared Data Association
JFSS	Java File Security System
LSB	Least Significant Bit
NBS	National Bureau of Standards
NSA	National Security Agency
OS	Operation System
PC	Personal Computer
UI	User Interface
UML	Unified Modeling Language
USB	Universal Serial Bus
XML	Extensible Markup Language

List of Contents

Introduction.....	1
1.1. Review.....	2
1.2. Research Problem.....	3
1.3. Proposed Solution	3
1.4. Research Objectives	3
1.5. Scope	4
1.6. Importance of the Research.....	4
1.7. Project Structure.....	4
Literature Review	5
2.1. Introduction	6
2.1.1. DES (Data Encryption Standard) and TRIPLE DES	6
2.2. Previous Studies	9
2.2.1. Performance Evaluation of Java File Security System (JFSS)	9
2.2.2. Security and Privacy in Computer Systems	10
2.2.3. [REDACTED]	10
2.2.3. Developing File Security for Windows Operation System	12
2.2.4. Data Security System Using Encryption Key in Digital Images for Secret Communication	13
2.3. Comparisons between the studies	16
Research Methodology	18
3.1. Introduction	19
3.2. System Skeleton	19
3.2.1. System analyses.....	20
3.2.2. Extract USB device Id	20
3.2.3. Extract device Bluetooth's ID.....	20
3.2.4. Encryption/Decryption	20
3.2.5. Secure file editor.....	20
3.3. Tools and Techniques	21
3.3.1. Enterprise Architect.....	21

3.3.2.	Visual Studio	21
3.3.3.	32FEET.NET	22
3.3.4.	Management Object Searcher class:	22
3.4.	Specifications of Used Hardware	23
3.5.	System UML	23
3.5.1.	Registration.....	23
3.5.2.	View Information.....	23
3.5.3.	Encrypt/Decrypt	24
3.5.4.	Edit Information.....	24
3.5.5.	Secure File editor	24
3.6.	System Database	30
3.6.1.	Users Table	30
3.6.2.	Files Table	30
3.6.3.	Verification-Code Table	31
	Implementation	32
4.1.	Introduction	33
4.1.1.	User Registration	33
4.1.2.	Add devices.....	33
4.1.3.	Import files to be secured.....	34
4.1.4.	Check connectivity of registered devices	34
4.2.	User Interfaces	35
4.2.1.	Loading Screen.....	35
4.2.2.	Login Screen.....	36
4.2.3.	Registration Screen.....	37
4.2.4.	Choosing devices Screen	38
4.2.5.	Encryption / Decryption Screen.....	39
4.2.6.	Import files Screen.....	40
4.2.7.	Secure file Screen	41
4.2.8.	Secure file Screen	42
4.2.9.	Help Screen.....	43
4.2.10.	Profile Screen.....	44
4.2.11.	Profile updates Screen.....	45
4.2.12.	Password updates Screen.....	46
4.2.13.	Password update Screen	47

4.2.14.	Plain text Screen	48
4.2.15.	Encrypted text Screen.....	49
4.2.16.	Decrypted Image Screen.....	50
4.2.17.	Encrypted Image Screen.....	51
4.2.18.	Account Check Screen	52
4.2.19.	Email Verification Screen.....	53
4.2.20.	Verification Code Message:.....	54
4.2.21.	Account Check Screen	55
	Results, conclusion and Recommendations	56
5.1.	Introduction	57
5.2.	Results	57
5.3.	Conclusion.....	57
5.4.	Recommendations	58
	References	59
	Appendix	60

List of Figures

Figure 2-1 triple DES algorithm.....	8
Figure 2-2: Input Image of Color Component.....	14
Figure 2-3: Plane Separation Process (R&G&B).....	14
Figure 2-4: Data Hiding Image.....	15
Figure 2-5: Reconstructed All Planes in Color Image with Secret data.....	15
Figure 3-1: phase's diagram.....	19
Figure 3-2: System Use case diagram.....	25
Figure 3-3: Registration use case diagram.....	26
Figure 3-4: View Information use case diagram.....	27
Figure 3-5: Edit information use case diagram.....	28
Figure 3-6: System activity diagram.....	29
Figure 4-1: loading screen.....	35
Figure 4-2: login screen.....	36
Figure 4-3: registration screen.....	37
Figure 4-4: select devices.....	38
Figure 4-5: encryption/decryption screen.....	39
Figure 4-6: importing files.....	40
Figure 4-7: secure file.....	41
Figure 4-8: save secured file.....	42
Figure 4-9: help screen.....	43
Figure 4-10: user profile.....	44
Figure 4-11: profile update screen.....	45
Figure 4-12: password update.....	46
Figure 4-13: confirm password.....	47
Figure 4-14: file before encryption.....	48
Figure 4-15: file after encryption.....	49
Figure 4-16: Image file before encryption.....	50
Figure 4-17: Image file after encryption.....	51
Figure 4-18: check account.....	52
Figure 4-19: email verification.....	53
Figure 4-20: verification code message.....	54
Figure 4-21: verification code.....	55

List of Tables

Table 2-1: comparisons between studies	17
Table 3-1: specifications of used devices	23
Table 3-2: user's database table	30
Table 3-3: files table in database	30
Table 3-4: verification code table in database	31

Chapter 1

Introduction

1.1. Review

Information security is the processes and methodologies which are designed to protect and ensure the correctness of information with every type including physical data files against any kind of threads.

Information security is a viral responsibility beard by the individual responsible with protecting the information. The confidentiality, availability and integrity (CIA) of information are more important for the long-term success of securing method than traditional, physical approaches [1].

From the moment the PC is switched on, the system faces countless threads, including spyware attacks, viruses and hackers trying to weasel their way into the system.

The Computer is inevitable thing in our life, it is very important to keep critical files safe. File security has become important technology as for the increasing use of computer systems. This project designs a file security application in Windows O.S using hard authentication with various mechanisms to secure user's local files. As it satisfies the main three information security measures: the confidentiality where it only grants access to authorized personal to their files, the integrity where it doesn't allow any other user or third party to access or change information that belongs to other user and the availability of information whenever an authorized user requests it.

It provides the users with multiple ways to secure their files using a key of their own choice and also guarantees the availability of the secured data as long as the user is the actual personal that his information can be retrieved using e-mail verification code.

1.2. Research Problem

When people share resources, their data can be lost or accessed by authorized or unauthorized users, and using the Internet the data can be hacked and important information can be compromised.

Using existing file security methods force the user to use the data only in the computer used to place a lock on it, and on other approach requires the user a password to limit the access for the authorized people holding the password but it saves the passwords in the system which means any other user have access to the system and the knowledge of the stored password on the system files can access the data.

1.3. Proposed Solution

User's data can be secured by placing passwords in all of his important data. the proposed encrypting algorithm can provide more certainty that the user's data remain secured, even if the password is revealed no other user can access the data because the physical keys (USB, Bluetooth device) for the data are held only by the user.

1.4. Research Objectives

This project must satisfy the following objectives:

- To enforce security on user's critical data by encryption and decryption.
- To reduce the risk on storing data in a public computers.
- To act as second defense line when a security breach occurs through the network or malicious software.

1.5. Scope

In this project, the user must register to the system providing his necessary information, backup password and add his portable devices (USB Stick, Bluetooth device) as physical keys to use their id's as encryption keys and then allow the user to select files to be encrypted using one of the specified keys or the backup password in case of lost keys. Information retrieval is available through an e-mail verification code.

1.6. Importance of the Research

This research adds another level of security to the user and helps in offering secured environment to the user's critical data.

Also provides versus hard authentication security mechanisms in case of the lack of some equipment's (keys).

1.7. Project Structure

Chapter1 gives an introduction about the project operations, scope, and overall design. Chapter2 reviews previous studies and, techniques of every study and comparisons between the studies. Chapter3 reviews the tools that used in the project, a framework, a background of the encryption algorithms, Packages that used in the project, a table review the specifications of used devices and the system UML. Chapter4 reviews stages of the system in (System Skeleton), figure, a description of every stage, also reviews the user interfaces in the real implementation of the project. Chapter5 gives results that achieved from the project, a conclusion reviews the project in a simplified manner, also reviews the recommendations for future studies, development and improvement.

Chapter 2

Literature Review

2.1. Introduction

This chapter presents a background about the used algorithm, previous researches and different papers about securing the data on computers.

2.1.1. DES (Data Encryption Standard) and TRIPLE DES

The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. Although now considered insecure, it was highly influential in the advancement of modern cryptography.[2]

Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977.[2]

- Brute-force attacks:

In cryptography, a brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly.

A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data and because of these flaws and more we used the triple DES algorithm.

- TRIPLE DES:

It's basically built on the core of the DES algorithm but regarding its biggest flaw the TDES majorly enhanced the efficiency of the algorithm's key. TDES provided a relatively simple method of increasing the key size of DES to protect against brute force attacks, without the need to design a completely new block cipher algorithm.

Triple DES uses three keys, K1, K2 and K3, each of 56 bits (excluding parity bits).

The encryption algorithm is:

Cipher text = EK3 (DK2 (EK1 (plaintext)))

I.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

Plaintext = DK1 (EK2 (DK3 (Ciphertext)))

I.e., decrypt with K3, encrypt with K2, and then decrypt with K1. as shown in figure (2-1)

Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

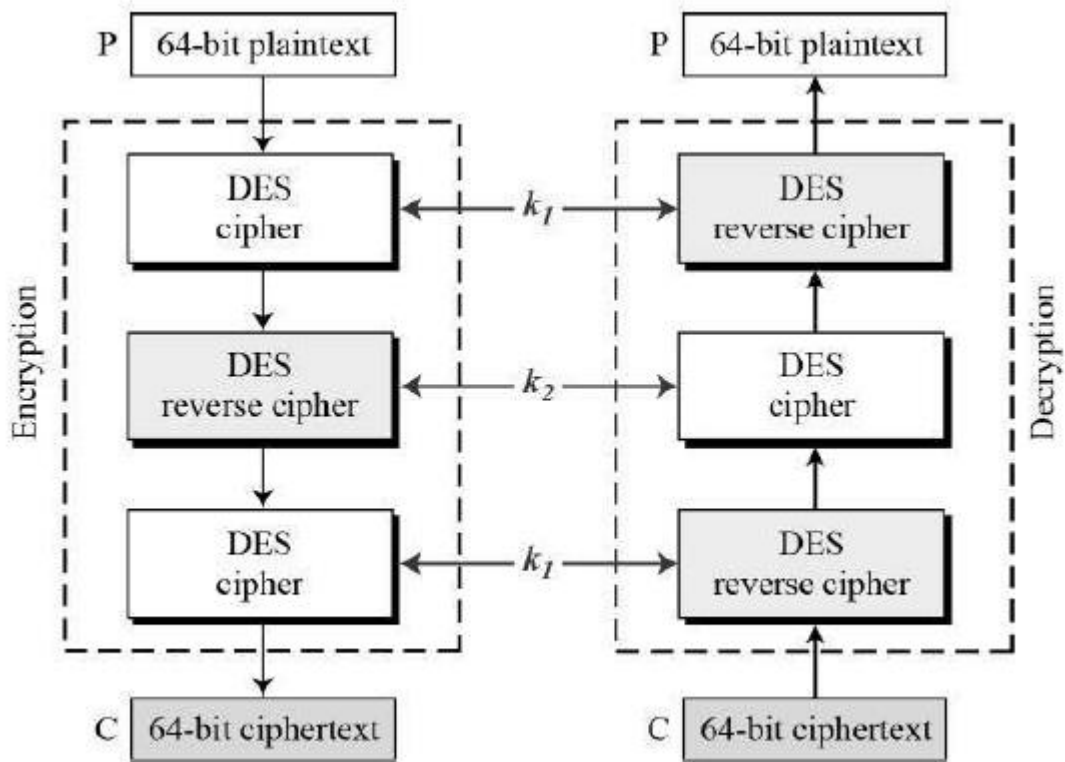


Figure 2-1 triple DES algorithm

Keying options

Keying option 1

All three keys are independent. Sometimes known as 3TDEA or triple-length keys.

Keying option 2

K_1 and K_2 are independent, and $K_3 = K_1$. Sometimes known as 2TDEA or double-length keys.

Keying option 3

All three keys are identical, i.e. $K_1 = K_2 = K_3$ [2].

2.2. Previous Studies

This part presents previous and similar studies in data security and protection field.

2.2.1. Performance Evaluation of Java File Security System (JFSS)

JFSS is integrated once with the operating system, it enhances the file security on demand of the user. The file system is the primary focus of access control in an operating system. The flat file systems make poor secure file systems because there is no way to hide the existence of a file from a user.

This approach is very convenient, and user friendly. It is developed in the user space and on the Java technology. The technology is well known for high portability, high CPU utilization by its multithreading feature, rich Application Programming Interface (API), and huge developer community.

There are three types of cryptography in the file cryptographic systems:

- 1) At file level.
- 2) At file system level.
- 3) At partition level.

JFSS System that has some properties of the file level cryptography and which is implemented in the file systems in user space (FUSE). It encrypts or decrypts the data files on the demand of the user and it can be mounted at any place on the disk. It also maintains the encryption key for encrypting or decrypting the file and that key is stored on the smart cards by the users. The encrypted file and the key are stored in the concern of the security of the data separately [4].

- The points that rise in the paper:
 - 1) Portability.
 - 2) Enforce some performance limitations.
 - 3) Developed in FUSE.

2.2.2. Security and Privacy in Computer Systems

The main portion of the paper then compares the security and privacy situations, considerations for protecting private information handled by computer systems. The privacy problem is really a spectrum of problems which ultimately must be assessed as engineering.

The points that rise in the paper are:

- Controlling user access to the resource sharing computer system, it has been suggested One-time password are necessary to satisfactorily identify and authenticate the user , in Time sharing systems permanently assigned passwords are considered acceptable for user identification.
- Private information will always have some value to an outside party; the penetrations will be attempted against computer systems handling such information.
- The computer hardware requirements appear to be the privacy and security situations. Such features as memory read-write protection, bounds registers, privileged instructions and privileged mode of operation are required to protect information.
- Not all users of a shared computer-private system will be authorized access to all files in the system. Just as not all users of a secure computer system will be authorized access to all files.

- In the classified defense environment users are indoctrinated in security measures and their personal responsibility can be considered as parts of the system design.
- Monitor programs governing the internal scheduling and operation of multi-programmed time-sharing or batch-operated machines are likely to be extensive and complex; and if security or privacy is to be guaranteed, some authority must certify that the monitor is properly programmed and checked out.
- In a security situation, a security officer is responsible for the control of classified information.
- Privacy and security situations are certainly similar in that deliberate penetrations must be anticipated, if not expected; but industrial espionage against computers may be less serious.
- For the most part, methods for assuring the communication channels have been the exclusive domain of the military and government.
- The different between the two situations are only of degree, there are a few aspects in which the two situations genuinely differ in kind.

The essential differences between the two situations appear in the paper:

- Legal foundations for protecting classified information are well established whereas in the privacy situation.
- The worth of the material at risk in the two situations can be quite different, not only to the owner but the other parties.
- The magnitudes of the resources available for protection and for penetration are markedly smaller in the privacy situation [5].

2.2.3. Developing File Security for Windows Operation System

This paper designs file security function on Windows O.S. whenever you use Windows O.S, you need to protect some file data. This paper designs these security protection functions. This paper proposes two security functions on Windows O.S. One is file security, The other is directory access protection.

- Technique.

The program execution is composed of the login form, a member subscription form, a directory approach control form, and file security form, these forms collect user data description to the files to be encrypted including the username password and the encryption algorithm.

- Results

This paper designed the access control, directory and file security features in the Windows operating system, the features offered in this paper are to set the security function on a particular file in the Windows Operating System and to control the access to a specific directory.

- Provided advantage

This research provided advanced level of protection by protecting the access to even the encrypted files after encryption where only users with permission to access them can read the encrypted data to decrypt it.

- Disadvantage

The complexity to the casual users where they will not know what encryption algorithm to use and the difference between them and also the operation overhead produced by encryption first and access control applied on every encrypted file [6].

2.2.4. Data Security System Using Encryption Key in Digital Images for Secret Communication

To enhance the system for secret data communication over unsecure channel supported Color Image and Encrypted info concealment victimization AES and Least important bit replacement methodology.

The project proposes the development of security system for secret data communication through encrypted info embedding in Color footage.

Technique

A given input image shown in (Figure 2-2) is born-again to anyone plane technique. Once plane separation process shown in (Figure 2-3), the encrypted info hider will conceal the key info into the image pixels as shown in (Figure 2-4). The information concealment technique uses the LSB replacement formula for concealing the key message bits into the input image. Inside the knowledge extraction module, the key info square measure getting to be extracted by victimization relevant key for choosing the image pixels to extract the information by victimization the secret writing key, the information square measure getting to be extracted from Input image to induce the information regarding the information.

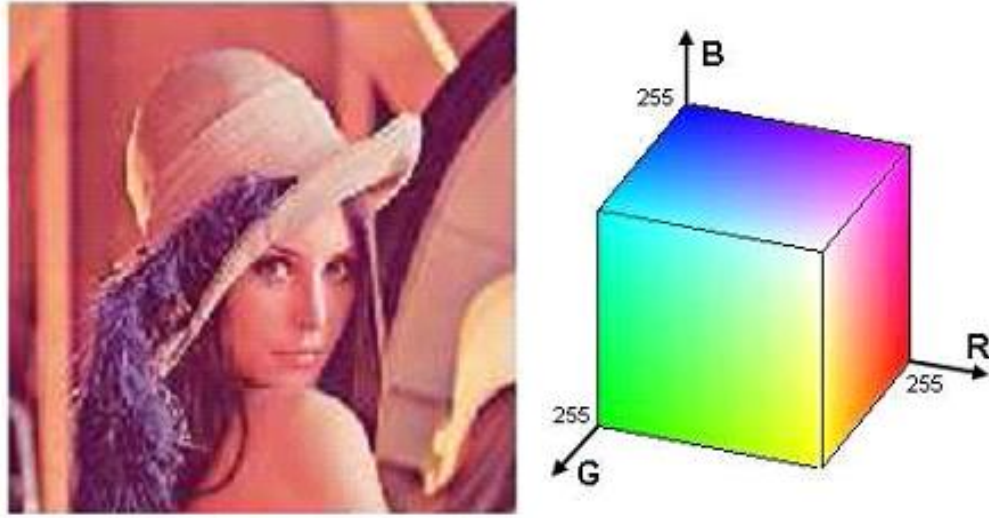


Figure 2-5: Input Image of Color Component



Figure 2-6: Plane Separation Process (R&G&B)

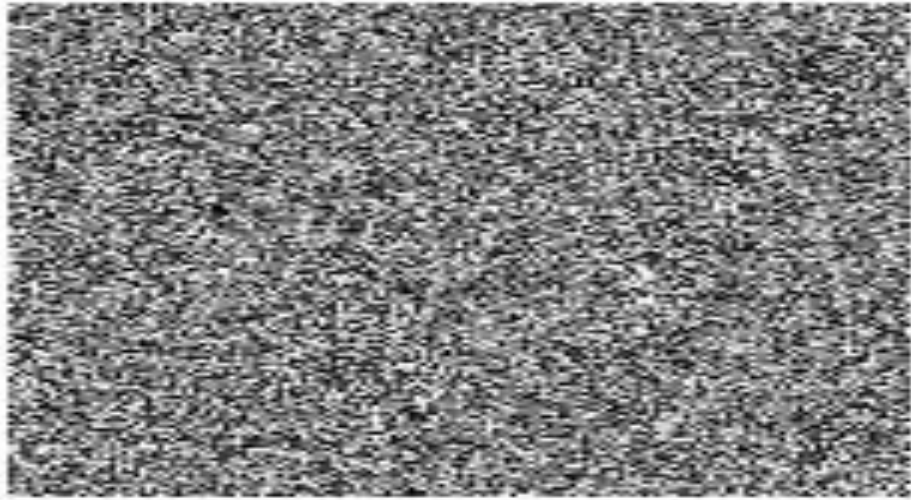


Figure 2-7: Data Hiding Image

Figure 2-8 shows the reconstructed image after the process of hiding data.as shown below there is no different between the original image (Figure 2-2) and the other image with secret data (Figure 2-5).



Figure 2-9: Reconstructed All Planes in Color Image with Secret data

Advantages

- This formula use random size of key.
- Attributable to this random size the center person can't predict the scale of key and knowledge.
- The amount of times execution of loop isn't mounted in order that safer formula.
- This can be safer and straightforward to implement [7].

2.3. Comparisons between the studies

Table 2-1 shows the comparisons between studies and also shows features that provided by every study. The first study (Security and privacy in computer System) focus on controlling user access and uses the encryption technique, but its complex. The second study (JFSS) also controls user access, provide encryption with external key, in addition it provides the portability. The (developing file security for windows operation system) control the user access, using encryption but its complex. The study (data security system using encryption key in digital image for secret communication) uses the concealing techniques to conceal the data in digital image, it uses a random size of key and that make it complex.

Table 2-1: comparisons between studies

study name feature	Security and Privacy in Computer Systems (paper)	Performance Evaluation of Java File Security System (JFSS)	Developing File Security for Windows Operation System (paper)	Data Security System Using encryption Key in Digital Image for Secret Communication
Control User access	✓	✓	✓	—
complexity	✓	—	✓	✓
portability	—	✓	—	—
Concealing	—	—	—	✓
Encryption	✓	✓	✓	—
Random size of key	—	—	—	✓
Use External Key	—	✓	—	—

Chapter 3

Research Methodology

3.1. Introduction

This chapter reviews system structure in this paradigm, it also explains the techniques and software products that are used during this project.

3.2. System Skeleton

Figure 3-1 shows phases that the system passes through.

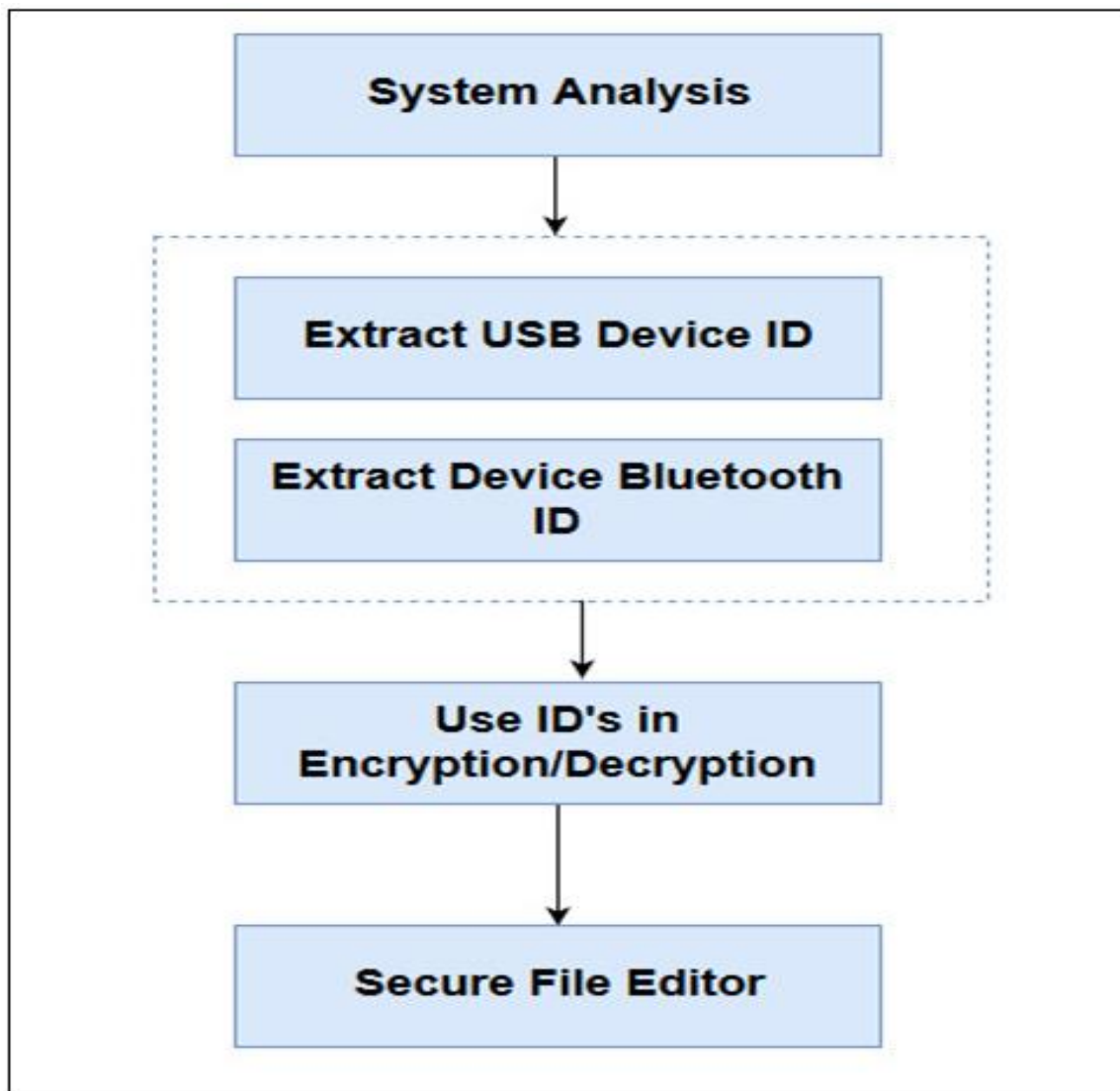


Figure 3-2: phase's diagram

3.2.1. System analyses

In this phase we do the analysis for the system and extract the UML diagrams that illustrate system processes.

3.2.2. Extract USB device Id

In this phase we extract the USB serial using Management Object Searcher class that get all connected devices id's as an array.

3.2.3. Extract device Bluetooth's ID

In this phase we use 32Feet.NET package that provides us with BluetoothClient class that contains the function discover devices that returns an array of BluetoothDeviceInfo that contains information of each device then we get the device name and device address using the function GetDrives from DriveInfo class.

3.2.4. Encryption/Decryption

In this phase we used TDES as an encryption algorithm and the USB serial or Bluetooth id that the user enters in the registration as a key for encryption and decryption operations.

3.2.5. Secure file editor

In this part an empty form is used and covered it with a text box and added a menu to easy the use of the editor and also implemented the encryption algorithm to save the file securely when the user requests it.

3.3. Tools and Techniques

This section of research reviews tools, techniques, packages, algorithms and every mechanism that used in project.

3.3.1. Enterprise Architect

UML (Unified Modeling Language) is a standard notation for the modeling of real-world objects as a first step in developing an object-oriented design methodology [8].

3.3.2. Visual Studio

Visual Studio is a complete set of development tools for building ASP.NET Web applications, XML Web Services, Desktop applications and Mobile applications.

Visual Basic, Visual C# and Visual C++ all use the same integrated development environment (IDE). That enables tool sharing and eases the creation of mixed-language solutions.

In addition, these languages use the functionality of the .NET Framework, which provides access to key technologies that simplify the development of ASP Web applications and XML Web Services.

- Integrated Development Environment (IDE):

Visual Studio is a suite of tools for creating software, from the planning phase through UI design, coding, testing, debugging, analyzing code quality and performance, deploying to customers, and gathering telemetry on usage. These tools are designed to work together as seamlessly as possible, and are all exposed through the Visual Studio Integrated Development Environment (IDE).

You can use Visual Studio to create many kinds of applications and games that run not only on Windows, but also Android and iOS. Websites and web services based on ASP.NET, JQuery, AngularJS, and other popular frameworks applications for platforms and devices as diverse as Azure, Office, SharePoint, Hololens, Kinect, and Internet of Things, to name just a few examples: Games and graphics-intensive applications for a variety of Windows devices, including Xbox, using DirectX [9].

3.3.3. 32FEET.NET

32feet.NET is a shared-source project to make personal area networking technologies such as Bluetooth, Infrared (IrDA) and more, easily accessible from .NET code. Support desktop, mobile or embedded systems. 32feet.NET is free for commercial or non-commercial use. The project currently consists of the following libraries:

- Bluetooth
- IrDA
- Object Exchange

Bluetooth support requires a device with either the Microsoft, Widcomm, BlueSoleil, or Stonestreet One Bluetopia Bluetooth stack. Requires .NET Compact Framework v3.5 or above and Windows CE.NET 4.2 or above, or .NET Framework v3.5 for desktop Windows XP, Vista, 7, 8 and 10. A subset of functionality is available for Windows Phone 8 and Windows Embedded Handheld 8 in the InTheHand.Phone.Bluetooth.dll library.

3.3.4. Management Object Searcher class:

Management Object Searcher class provides the base functionality of a device. It is the primary control class for a device and is the container and manager of hosted services provided by a device. This class exposes static methods and properties used to

manage device information, start, and stop internal services and to manage hosted services and drivers used in this project to detect connected flash drive (USB Stick)[10].

3.4. Specifications of Used Hardware

Table 3-1: specifications of used devices

Device	Feature
Computer(desktop/laptop)	Provide Bluetooth
Phone(mobile)	Provide Bluetooth
USB flash drive (USB Stick)	Provide Serial connection

3.5. System UML

The user in this system can do the following:

3.5.1. Registration

The user must provide the system with necessary information that will be used in main functions (login, encrypt/decrypt, etc...).

3.5.2. View Information

The user can view the information (full name, Devices used, E-mail, encrypted files).

3.5.3. Encrypt/Decrypt

The user chooses the key to be used in encryption or decryption and the system check if the chosen devices are available or not if the devices are available the system can do the chosen operation (encrypt/decrypt), if the devices are not available the system will alert the user to connect the device.

3.5.4. Edit Information

The user can edit full name, E-mail, password, USB device or Bluetooth device that saved in registration.

3.5.5. Secure File editor

In this part an empty form is used and covered it with a text box and added a menu to help the user to use of the editor and also implemented the encryption algorithm to save the file securely when the user requests it.

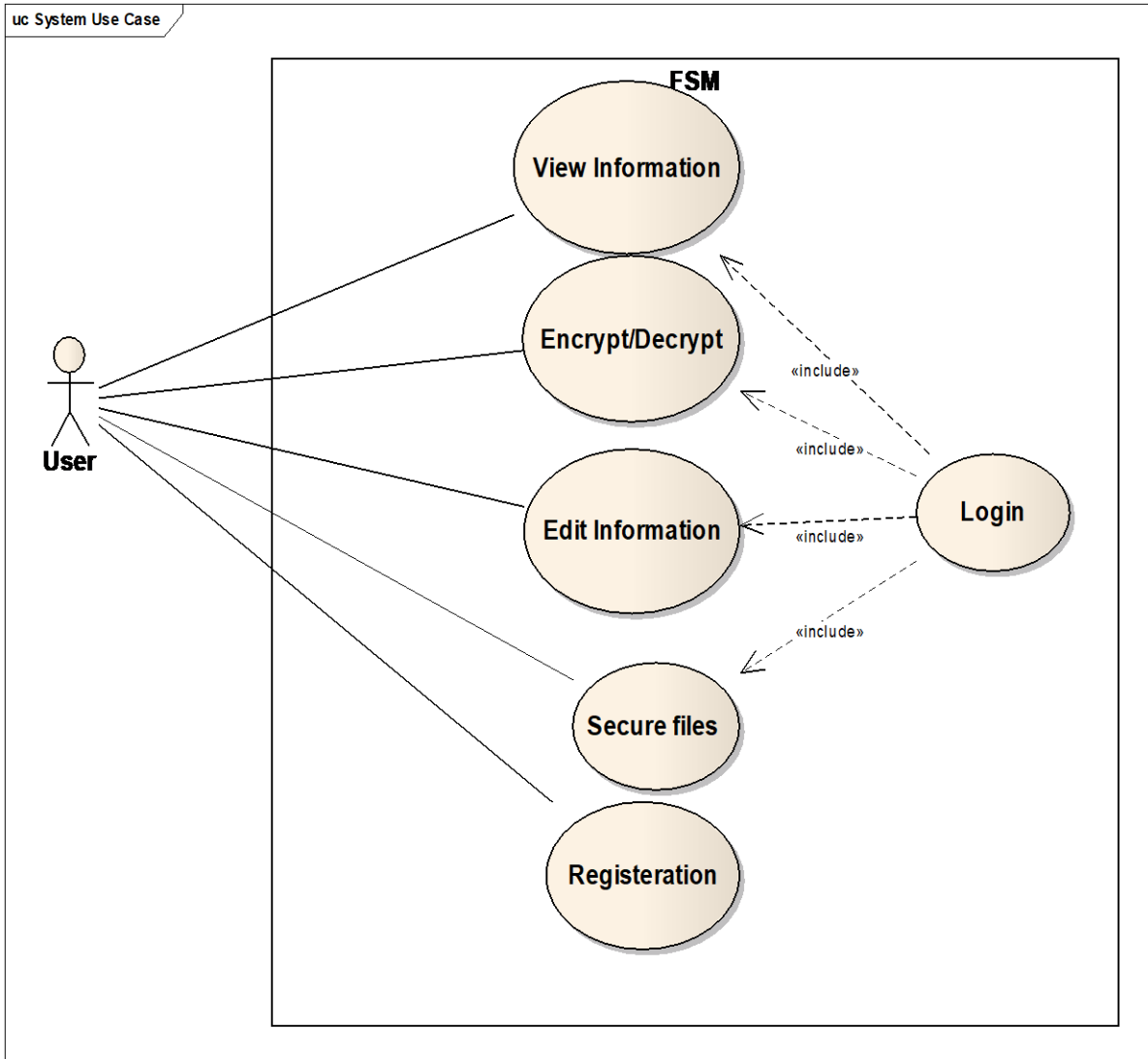


Figure 3-3: System Use case diagram

The user must provide the system with user name and password to access the system, USB serial or Bluetooth number to be used as a key for login, encryption/decryption operations, backup password to be used if the user lost the keys (USB serial, Bluetooth) used in encryption/decryption shows in Figure 3-3.

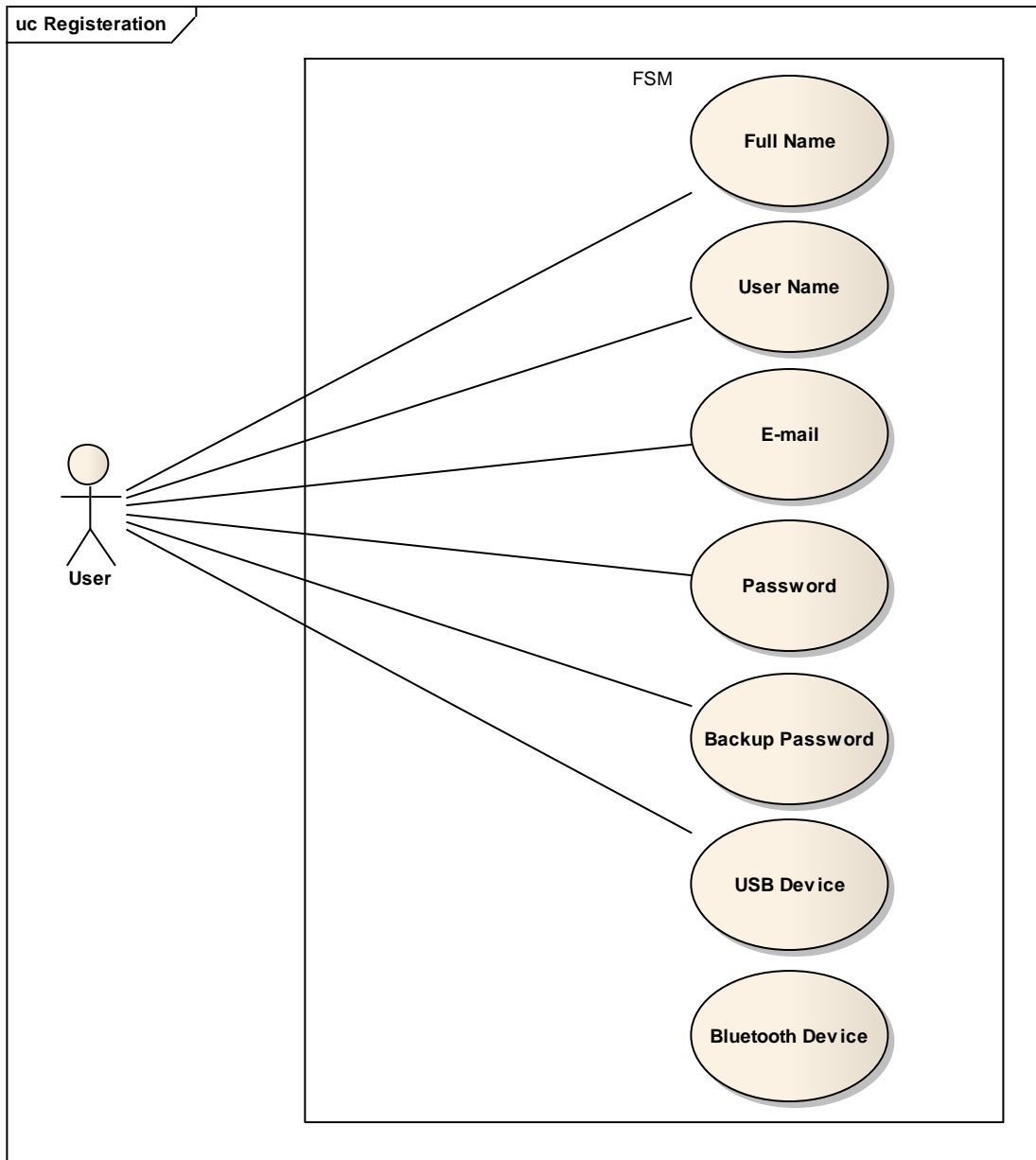


Figure 3-4: Registration use case diagram

Figure 3-5 shows view information operation that includes user's basic information (full name, Email address, registered key and all the files that have been encrypted by this user) also information about what user encrypted which files are not available to any user but the owner of the files.

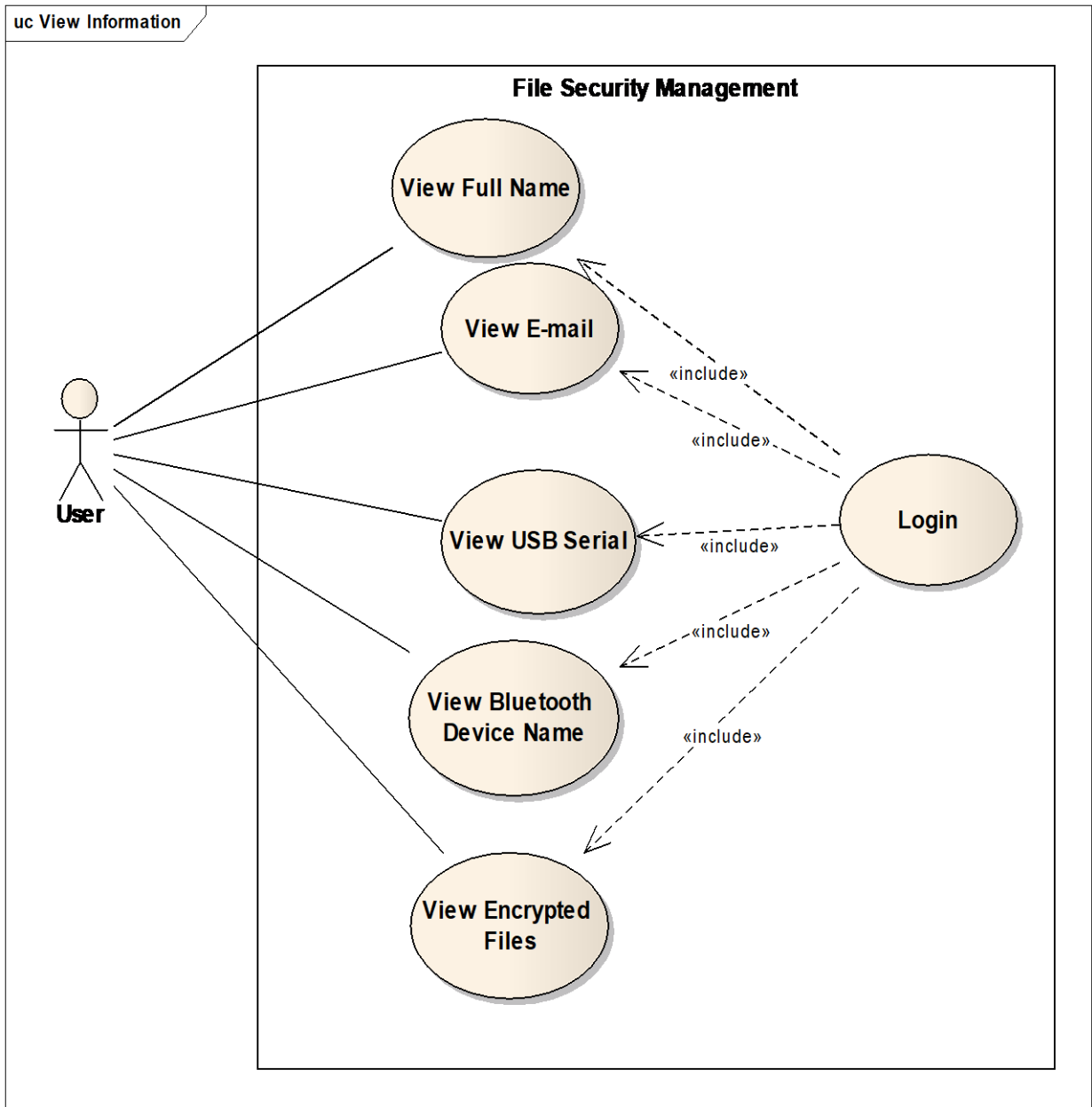


Figure 3-6: View Information use case diagram

Figure 3-7 shows the edit information operation. Which includes user's information in updating full name, Email, keys used and the password. But also user password and the keys can be edited using the email verification approach when the user loses them.

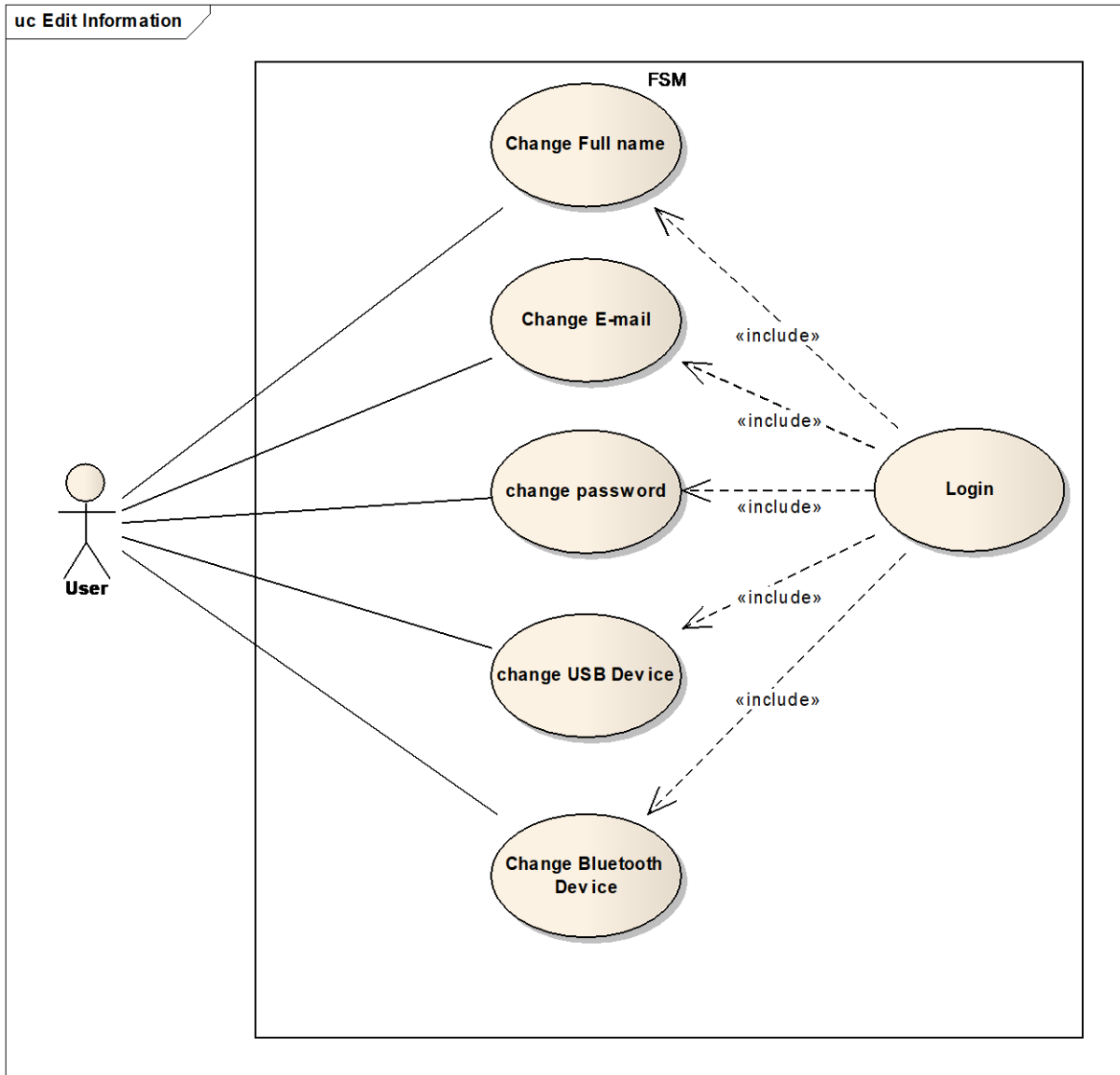


Figure 3-8: Edit information use case diagram

Figure 3-9 shows the activities that user can do in the system. This system starts with the login screen where the user chooses one of the options shown in the diagram, in the registration process the user that successfully completes the registration sent back to the login screen where can login to the system. In this option the user can access the main page where can directly interact with the system's main operation which it encrypting the required data and decrypting data back to access it. Profile view option where the user can monitor the encrypted files as well as editing the personal information, and also a logout button to exit the account back to the login page. Users stuck and the login page can't access their accounts can use the password reset approach as well as the devices reset to generate a verification code sent to their register email addresses and after verification access is granted to their accounts so none of their important data is lost.

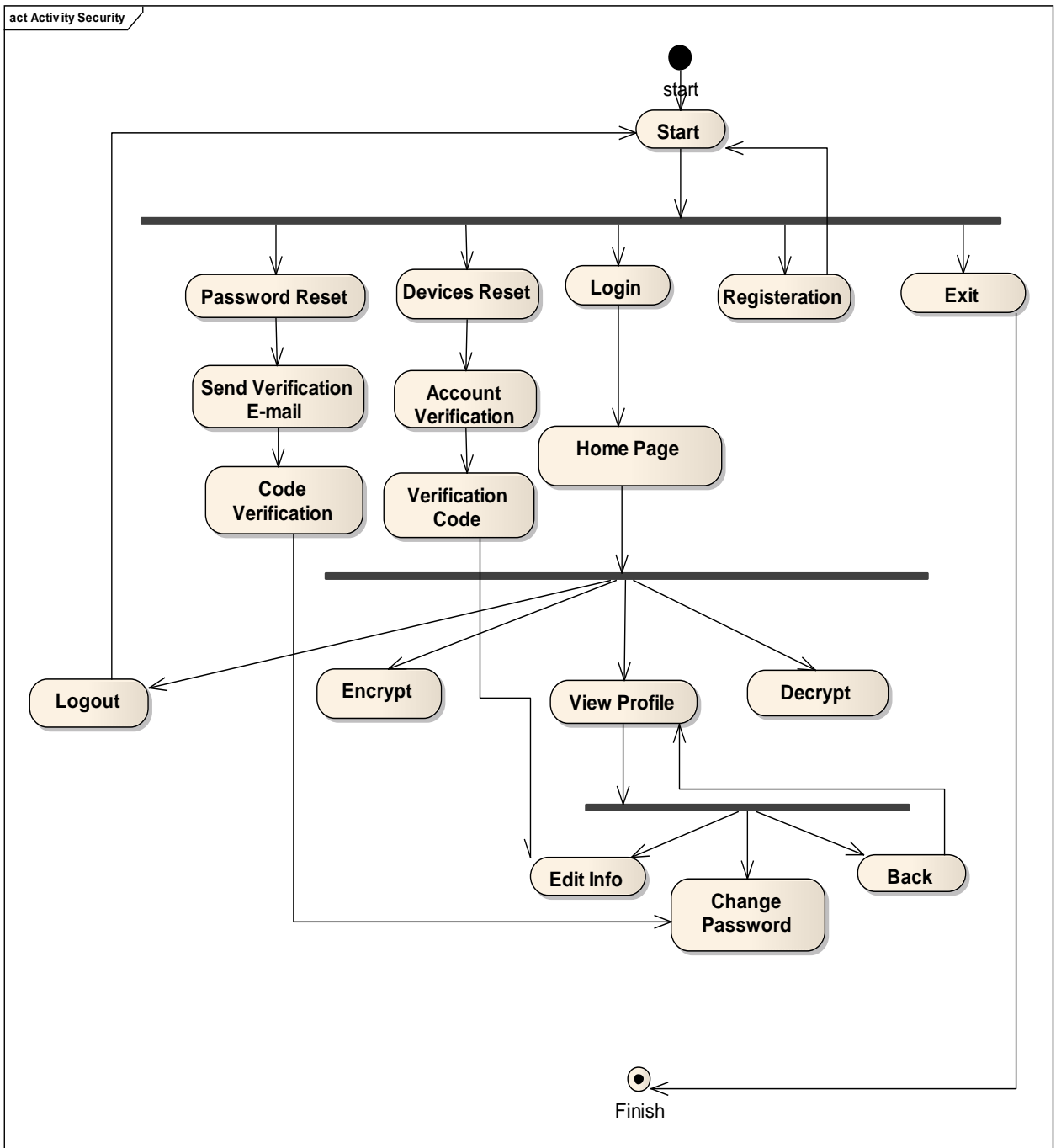


Figure 3-10: System activity diagram

3.6. System Database

This part illustrates the tables of the database that used in the system.

3.6.1. Users Table

Table 3-2 illustrates the elements of the user's database with type, size, and name on database and a note on the element.

Table 3-2: user's database table

NO.	Column name	Column name on database	Column type	Column size	Note
1	Full name	fullname	varchar	50	Not null
2	User name	username	varchar	50	Primary key
3	Password	password	varchar	50	Not null
4	Email	email	varchar	50	Not null
5	Backup password	backuppasword	varchar	50	
6	USB Name	usb	varchar	50	
7	USB Serial	usbSerial	varchar	50	
8	Bluetooth Name	bluetooth	varchar	50	
9	Bluetooth Number	bluetoothNumber	varchar	50	

3.6.2. Files Table

Table 3-3 illustrates the elements of the File's database with type, size, and name on database and a note on the element.

Table 3-3: files table in database

NO.	Column Name	Column Name on database	Column type	Column size	Note
1	User name	username	varchar	50	Not null
2	File name	filename	varchar	50	Primary key
3	Used key	usedkey	varchar	50	Not null

3.6.3. Verification-Code Table

Table 3-4 illustrates the elements of the verification code database with type, size, and name on database and a note on every element.

Table 3-4: verification code table in database

NO.	Column Name	Column Name on database	Column type	Column size	Note
1	User name	username	varchar	50	Not null
2	Code	code	varchar	50	Primary key

Chapter 4

Implementation

4.1. Introduction

In this chapter we will talk about the stages of the proposed system. The system has three main stages, will be detailed later.

First phase of the system is about user registration and adding all information including Full Name, Username, Email and the password of the account. In the second phase the user will add the devices that will use in Encryption and set the backup password. Last phase consists of two steps: in the first step the system will check the key (device) to encrypt or decrypt files. Second step is the encryption and decryption processes.

4.1.1. User Registration

The user must register to the system providing his full name, username, password, e-mail, backup password and connect his physical keys to register their id's in the system.

In the case of losing one of his login in information the user can initiate a verification code generated within the application and sent to his registered e-mail after verifying that the user can remembers the e-mail address, and by it the user can restore lost information.

4.1.2. Add devices

This process runs in the registration where the user connects his keys to the system to register their id's to be used in the system.

4.1.3. Import files to be secured

When the user login to the system he can use his keys to encrypt his files but when requesting this operation the user must connect his key to make sure that is the actual user and not an unauthorized access.

4.1.4. Check connectivity of registered devices

The system will check the user's device that is used in the encryption of files will be secured if the user's device is connected in the USB route. And active Bluetooth devices will be checked if the used key is a Bluetooth device.

4.2. User Interfaces

This part shows the interfaces of the program implementation.

4.2.1. Loading Screen

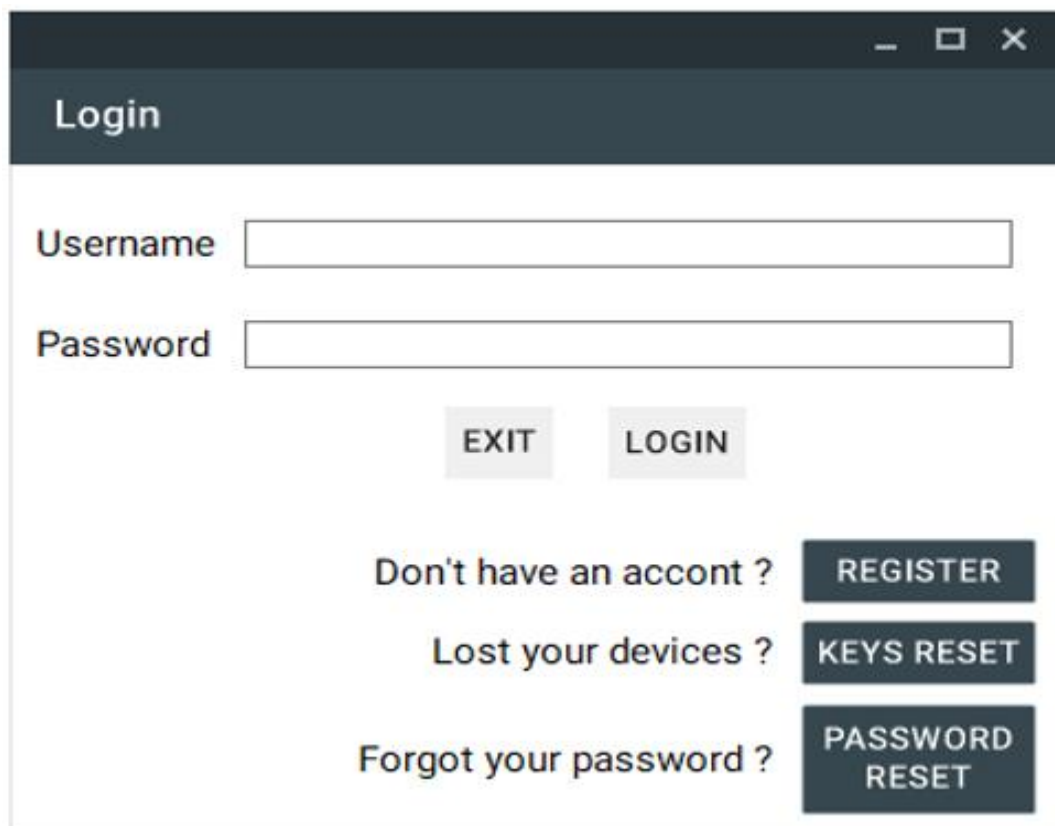
The screen that appear after running the system shown in Figure 4-1.



Figure 4-2: loading screen

4.2.2. Login Screen

In Figure 4-3 the new users can click on “REGISTER” to guide them to the registration form to start registering into the system, while already registered users can choose to login using their username and password but also a key required to authenticate this individual and can choose to reset one of his missing information or by clicking on “KEYS RESET” to reset the user’s keys by following the process of verifying the individual identity using the registered e-mail or click on “PASSWORD RESET” to reset follow the process of verifying the identity and providing the user with his lost password to update it. And the user can terminate the application by clicking on the “EXIT” button.

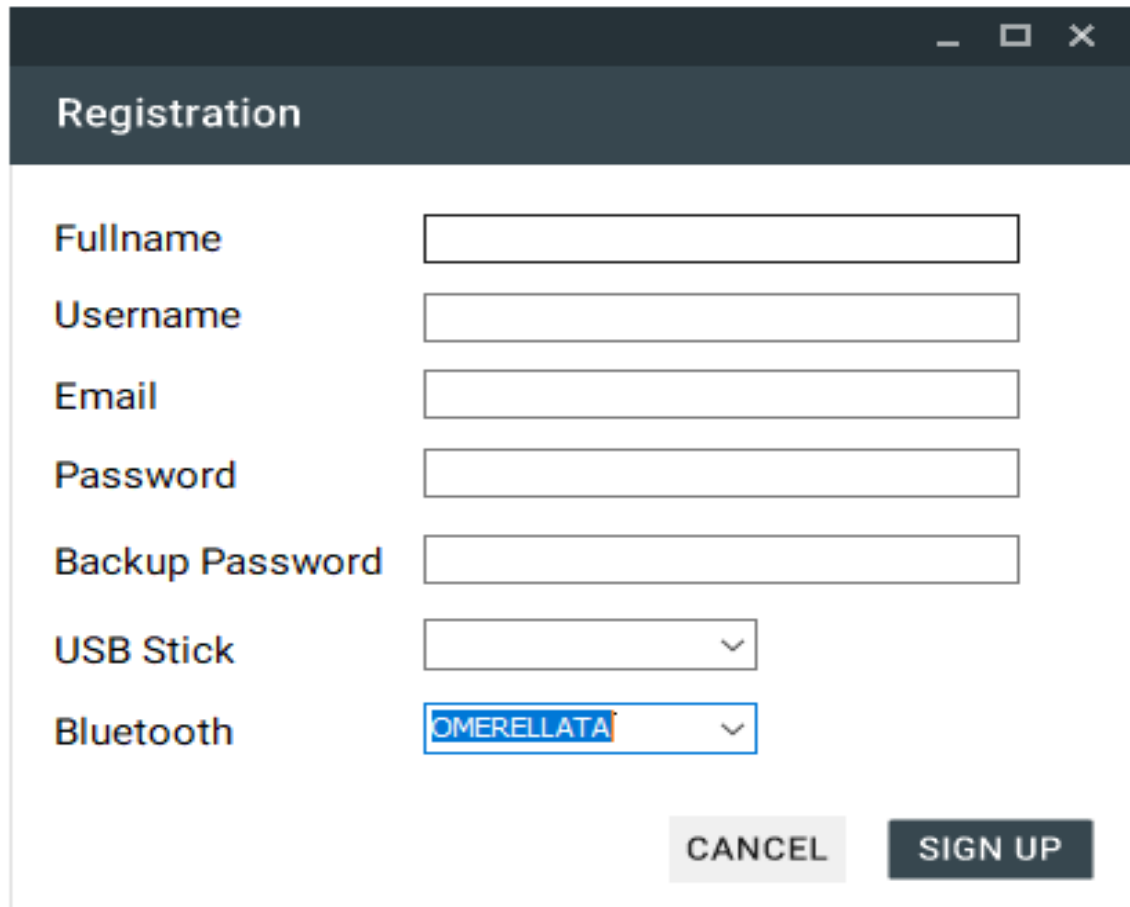


The image shows a login screen window with a dark header bar containing the title "Login" and standard window control buttons (minimize, maximize, close). Below the header, there are two input fields: "Username" and "Password". Underneath these fields are two buttons: "EXIT" and "LOGIN". At the bottom of the screen, there are three rows of text and buttons: "Don't have an account ?" with a "REGISTER" button, "Lost your devices ?" with a "KEYS RESET" button, and "Forgot your password ?" with a "PASSWORD RESET" button.

Figure 4-4: login screen

4.2.3. Registration Screen

After clicking on “REGISTER” button on the Figure 4-5 the registration screen (Figure 4-6) will appear to the user to fill his information and connect his physical keys to the application to be registered with the user’s information, And also to add backup password in case of missing key.



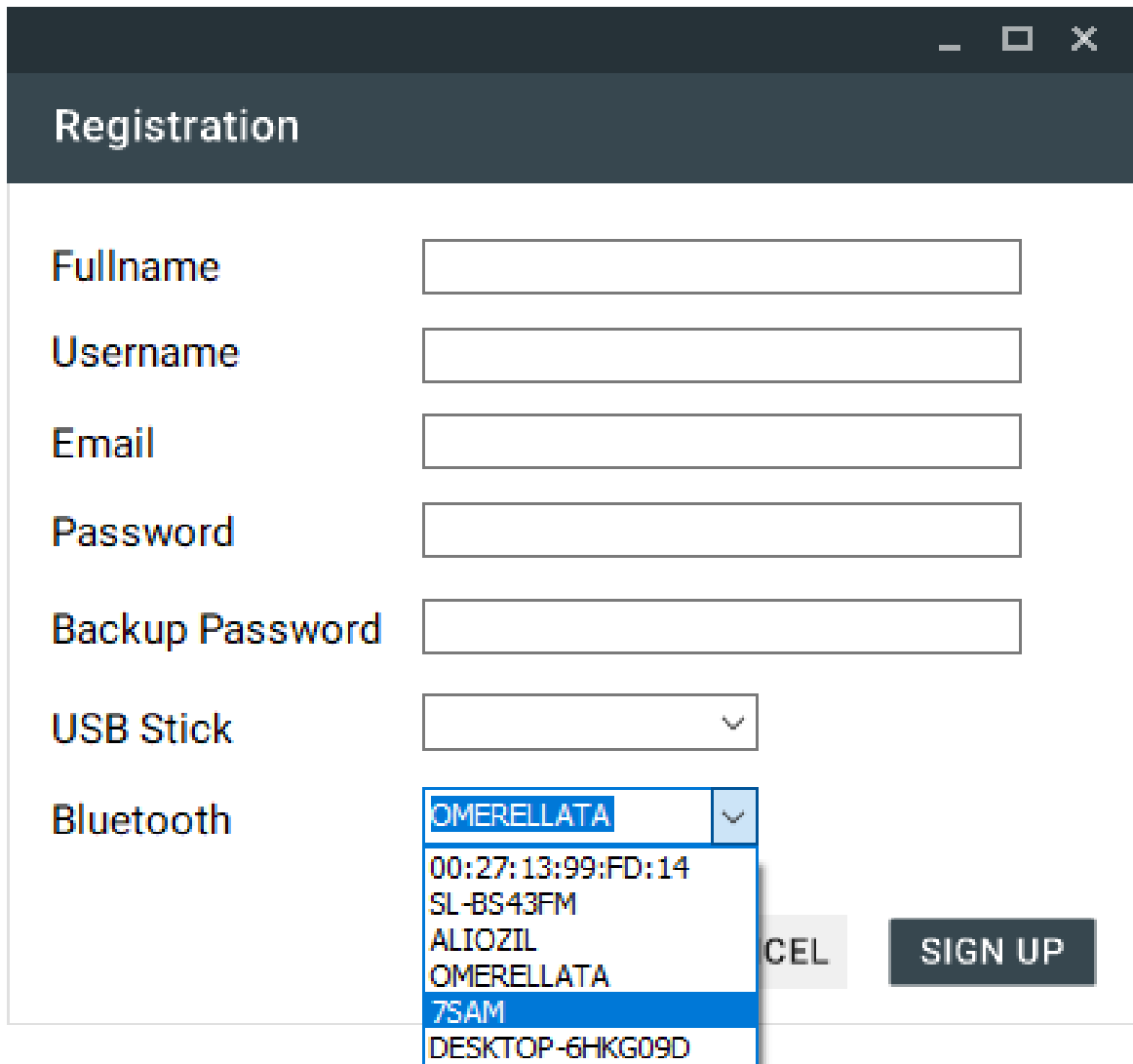
The image shows a registration window titled "Registration". It contains several input fields and two buttons. The fields are: Fullname, Username, Email, Password, Backup Password, USB Stick (a dropdown menu), and Bluetooth (a dropdown menu with "OMERELLATA" selected). The "CANCEL" button is light gray, and the "SIGN UP" button is dark gray.

Fullname	<input type="text"/>
Username	<input type="text"/>
Email	<input type="text"/>
Password	<input type="text"/>
Backup Password	<input type="text"/>
USB Stick	<input type="text" value=""/>
Bluetooth	<input type="text" value="OMERELLATA"/>

Figure 4-7: registration screen

4.2.4. Choosing devices Screen

The user will be able to choose by a combo box the Bluetooth and USB drive that will use as key in encrypt and decrypt processes.



The image shows a registration window with the following fields and options:

- Fullname:
- Username:
- Email:
- Password:
- Backup Password:
- USB Stick:
- Bluetooth: (dropdown menu open)

The Bluetooth dropdown menu contains the following items:

- OMERELLATA
- 00:27:13:99:FD:14
- SL-BS43FM
- ALIOZIL
- OMERELLATA
- 7SAM
- DESKTOP-6HKG09D

Buttons: CANCEL, SIGN UP

Figure 4-8: select devices

4.2.5. Encryption / Decryption Screen

After login Figure 4-9 appears to the user allowing him to encrypt his data or decrypt already encrypted data to access it, after choosing a device to encrypt and clicking on “ENCRYPT” button file explorer will be opened to allow the user to select the file to encrypt and by clicking on “DECRYPT” the same operation will be issued with the difference that the application will use the decrypt method using the key’s id which is selected, by clicking on “SECURED FILE” a dedicated file editor will be opened to the user to use in creating a secured file, by clicking on “USE BACKUP PASSWORD” the user will be able to decrypt any file encrypted by this account without the need for a key, by clicking on “VIEW PROFILE” the user will access a screen to edit his personal information along with his keys for future use, and on clicking “LOGOUT” the account will be logged out and the user will have to login again to access this screen

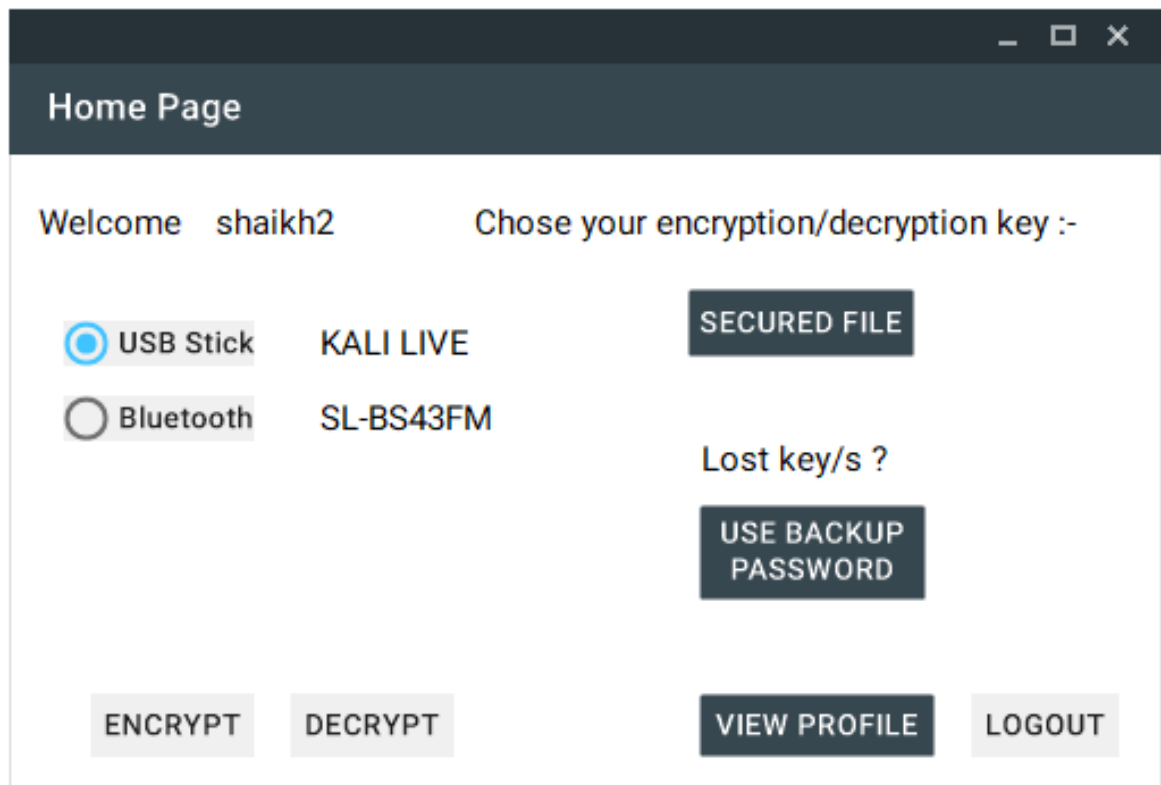


Figure 4-10: encryption/decryption screen

4.2.6. Import files Screen

By clicking on the encryption or decryption button a file explorer will show up after testing the existence of user's key allowing the user to choose a file to run the requested operation on it shown in Figure 4-11.

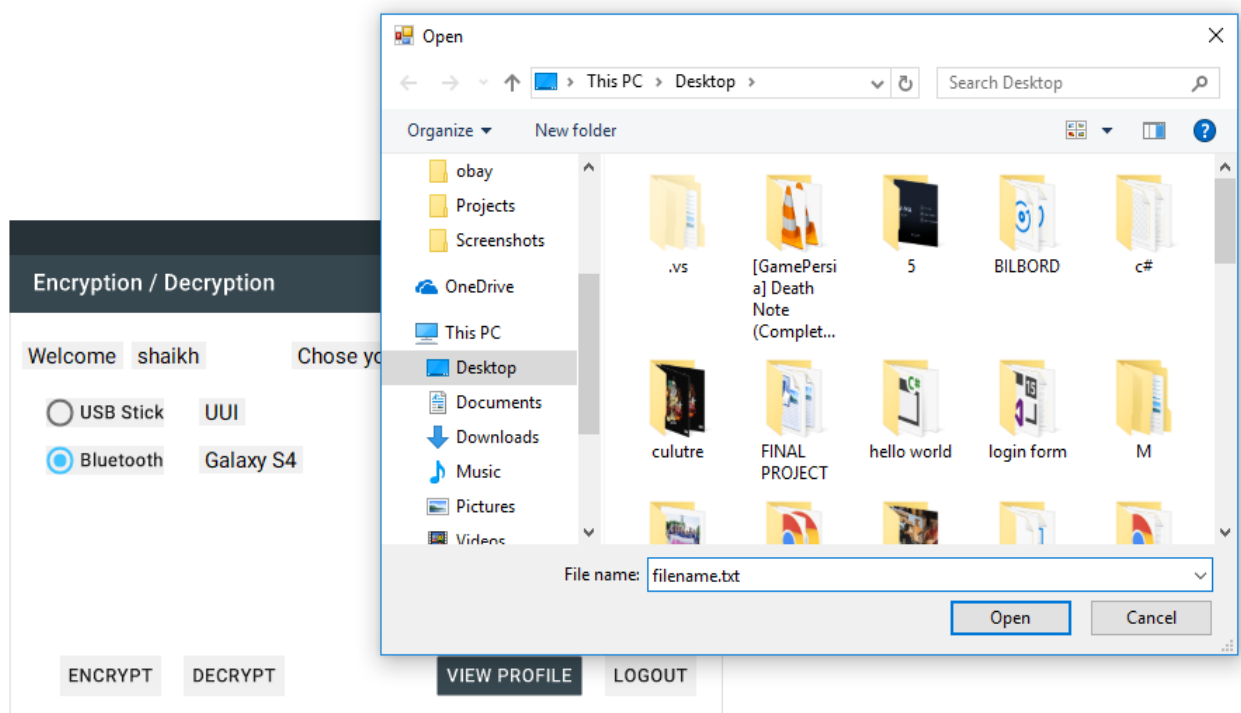


Figure 4-12: importing files

4.2.7. Secure file Screen

Figure 4-13 shows that user can create new secured file using the button “SECURED FILE” which will open a built in text editor that allows the user to manage text files providing all the basic operations Open, Save, Redo, Undo and saving the file encrypted to any location directly without the need to perform the basic encryption process.

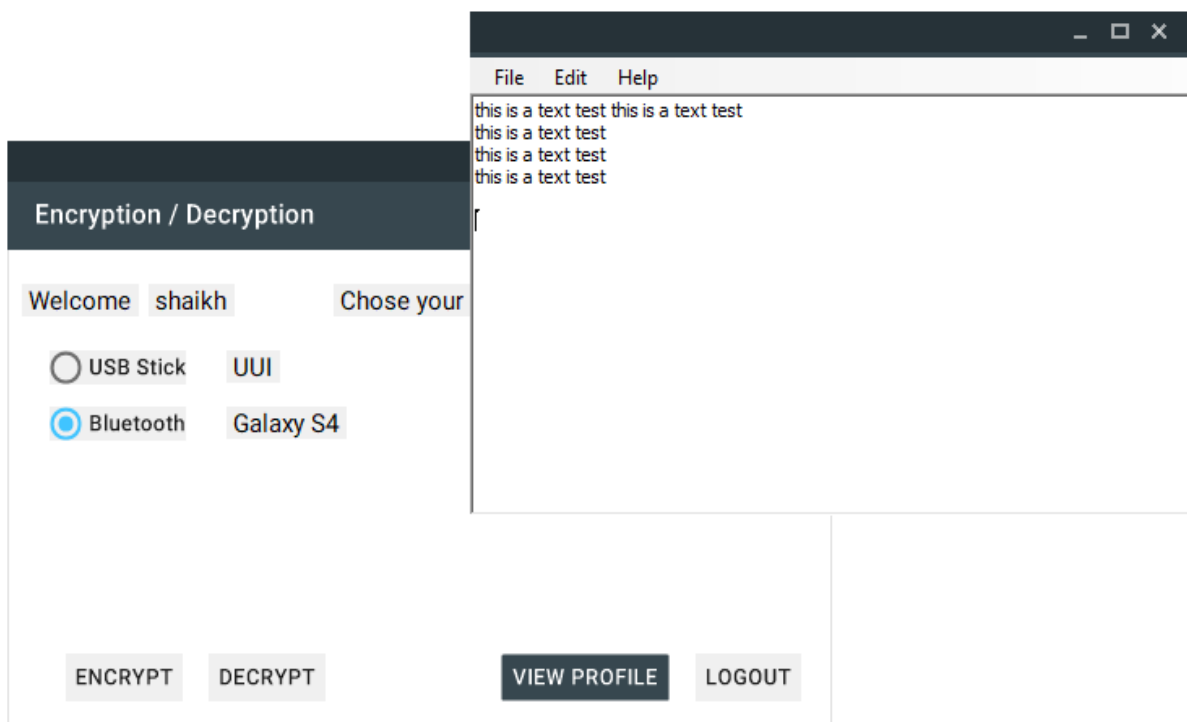


Figure 4-14: secure file

4.2.8. Secure file Screen

Options regarding to the editor are functioning as any other file editor providing the basic operations as well as a help tab that illustrates the use of the text editor.

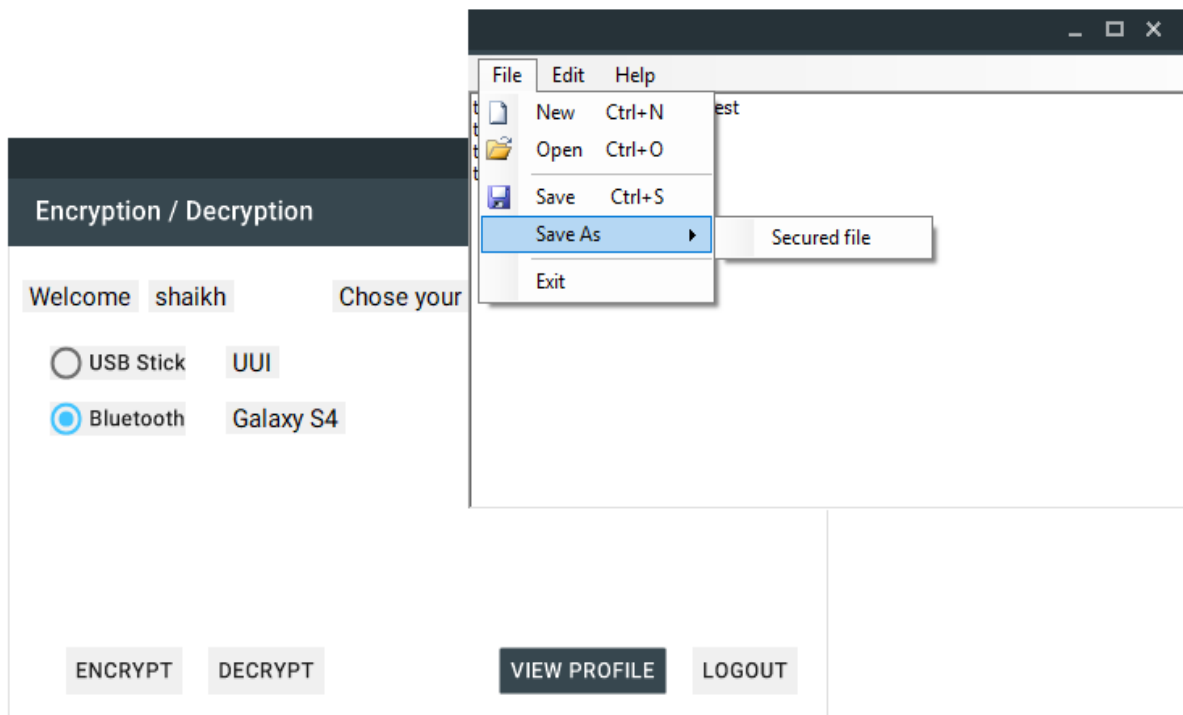


Figure 4-15: save secured file

4.2.9. Help Screen

When the user uses the secure file button and click on the help icon on the menu tab Figure 4-16 appears to describe the basic operations of this text editor which allows the user to use shortcuts, save text file to a certain location and also save the files directly encrypted from inside the editor.

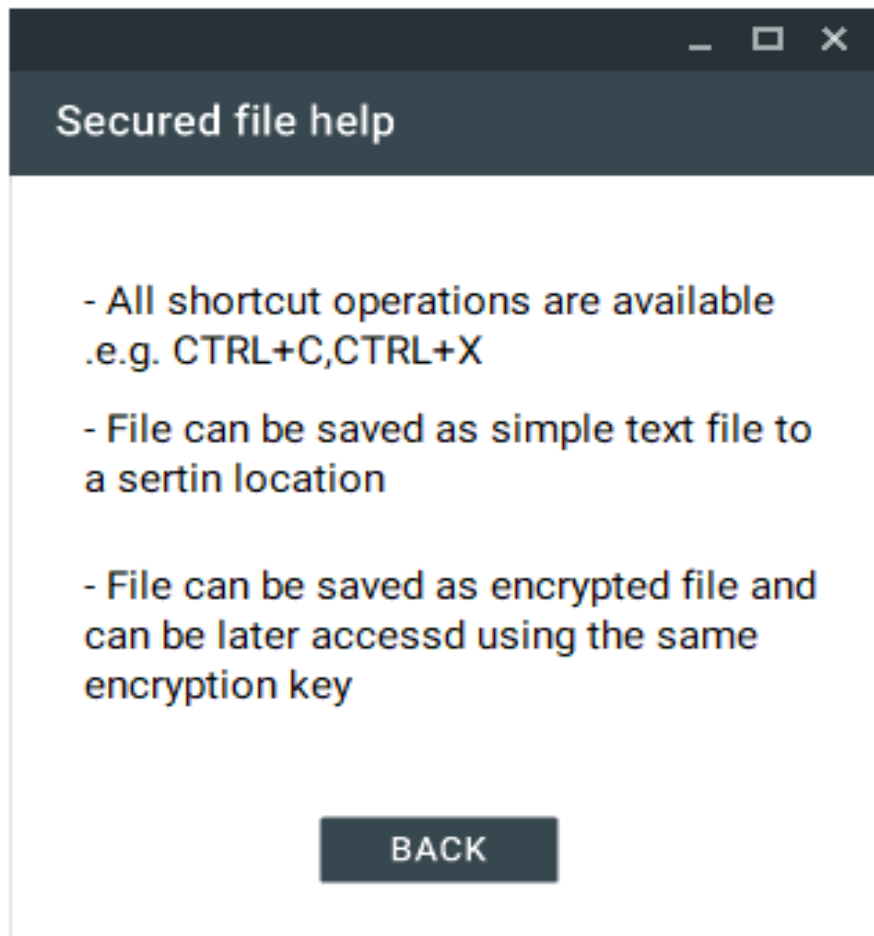
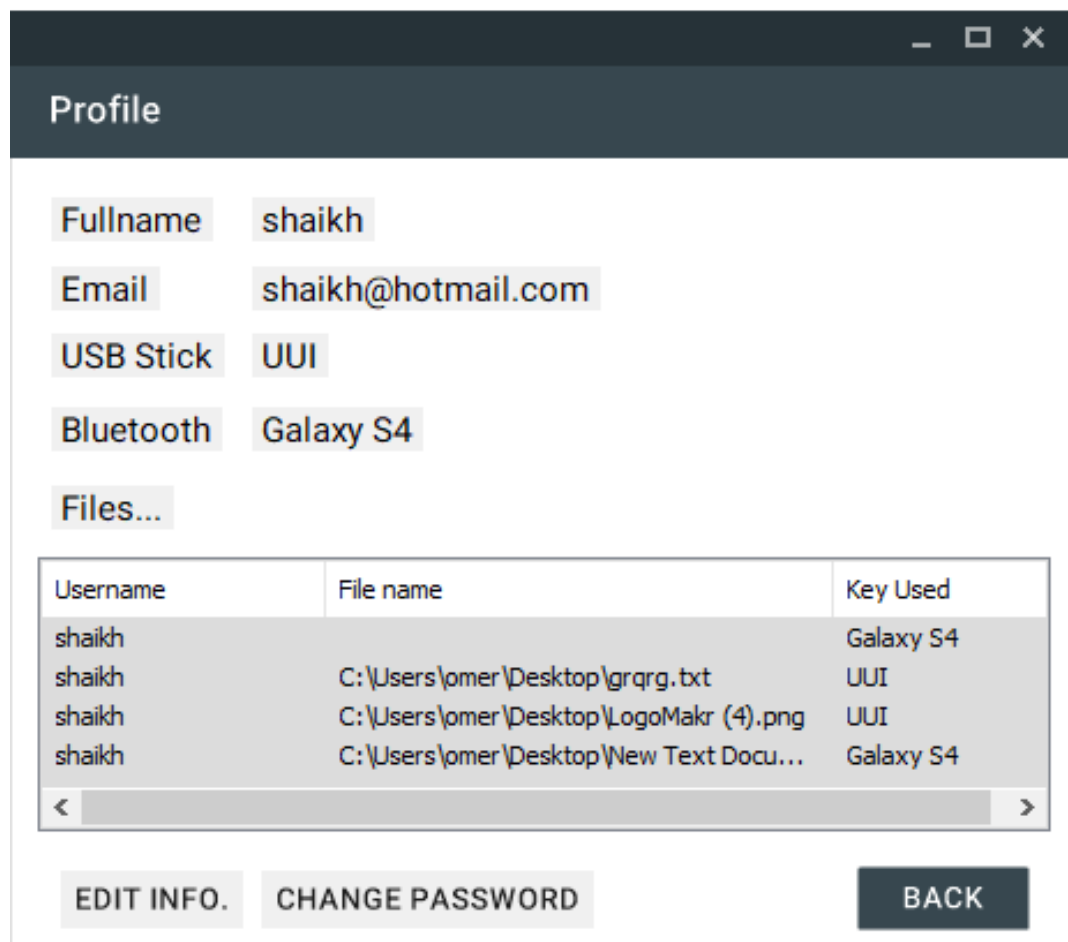


Figure 4-17: help screen

4.2.10.Profile Screen

In Figure 4-18 which is accessed through the main page the logged in user's information are illustrated and his keys also the files owned by the user are listed and when it allows the user to edit his personal information and update his keys by clicking on "EDIT INFO." And changing the account's password by clicking on the "CHANGE PASSWORD" key and going back to the main page by clicking on "BACK".



The screenshot shows a mobile application window titled "Profile". It contains the following information:

- Fullname: shaikh
- Email: shaikh@hotmail.com
- USB Stick: UUI
- Bluetooth: Galaxy S4
- Files... section containing a table:

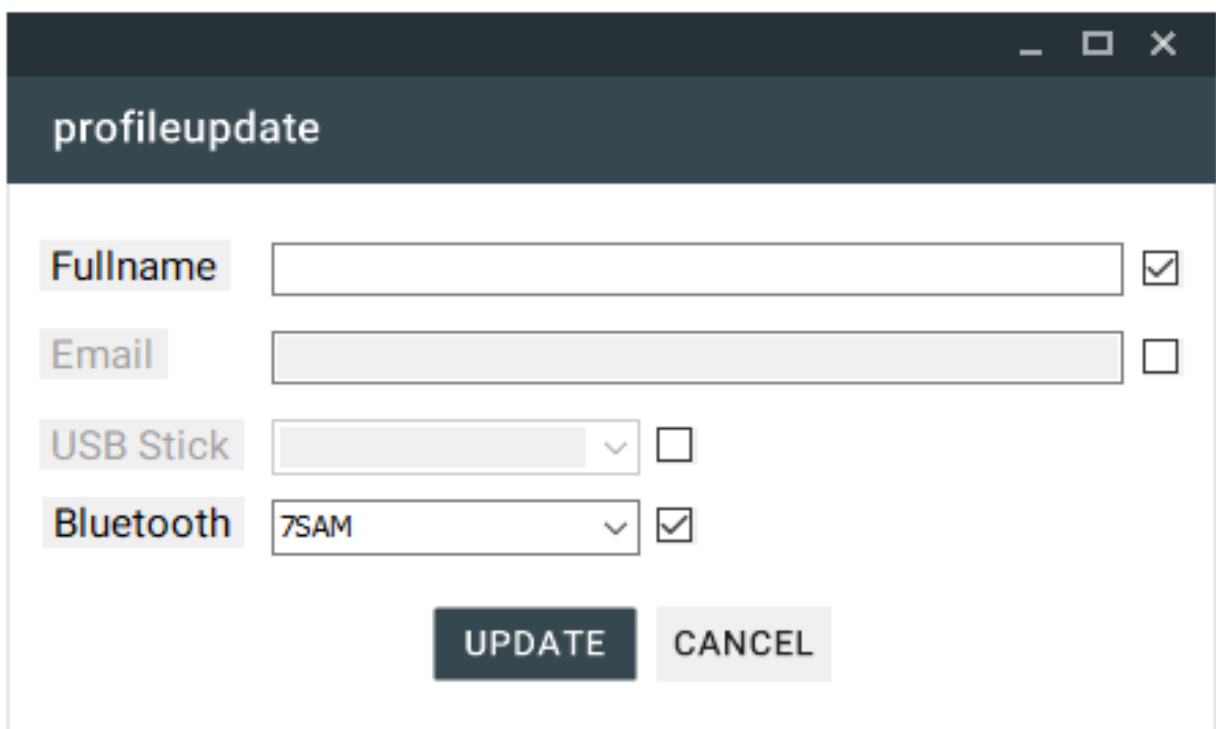
Username	File name	Key Used
shaikh		Galaxy S4
shaikh	C:\Users\omer\Desktop\grqrg.txt	UUI
shaikh	C:\Users\omer\Desktop\LogoMakr (4).png	UUI
shaikh	C:\Users\omer\Desktop\New Text Docu...	Galaxy S4

At the bottom of the screen, there are three buttons: "EDIT INFO.", "CHANGE PASSWORD", and "BACK".

Figure 4-19: user profile

4.2.11. Profile updates Screen

Figure 4-20 shows that the system allows the user to edit part or all his information and update his keys by checking the check box next to the data field the field will be activated to update with the data entered after clicking “UPDATE” and user can cancel the update operation by clicking on the “CANCEL” button.



The screenshot shows a window titled "profileupdate" with a dark header bar. Below the header, there are four rows of input fields, each with a label on the left and a checkbox on the right:

- Fullname**: A text input field with a checked checkbox.
- Email**: A text input field with an unchecked checkbox.
- USB Stick**: A dropdown menu with a checked checkbox.
- Bluetooth**: A dropdown menu showing "7SAM" with a checked checkbox.

At the bottom of the form, there are two buttons: "UPDATE" (dark grey) and "CANCEL" (light grey).

Figure 4-21: profile update screen

4.2.12.Password updates Screen

After clicking on the “CHANGE PASSWORD” button on Figure 4-22 this Figure 4-23 will be shown to the user asking for his old password to allow him to access the update password part after clicking the button “ENTER” if the entered password doesn’t match the password on the database this message will be shown to the user.

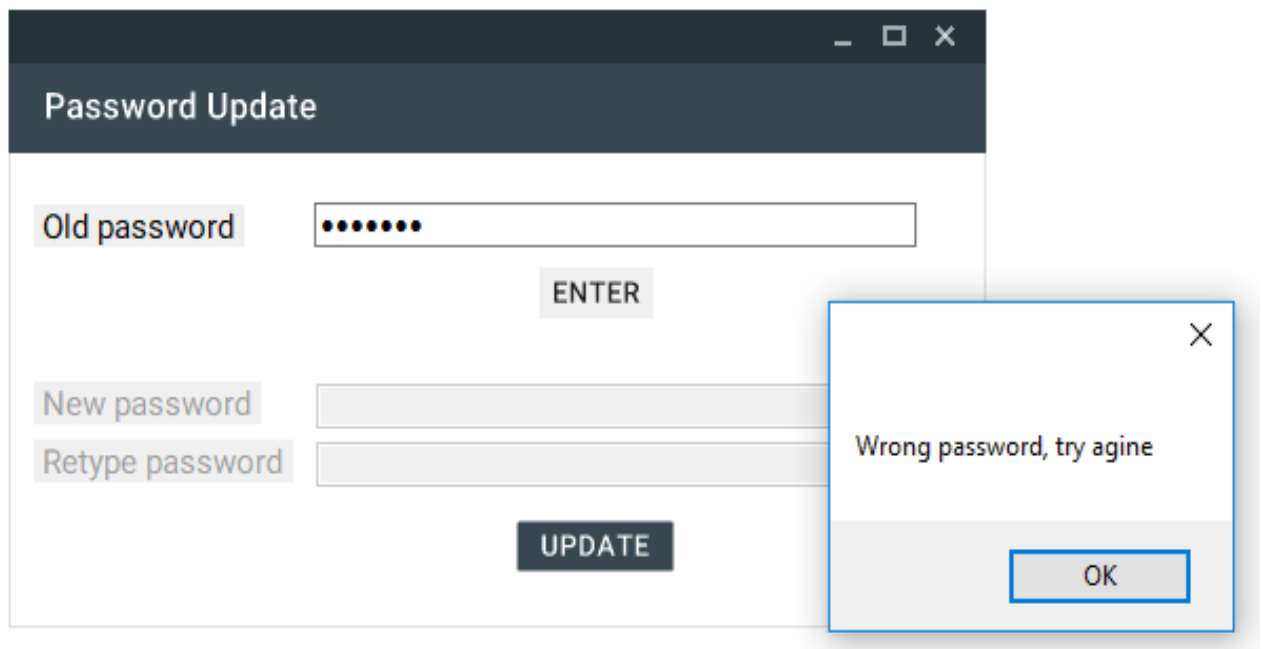
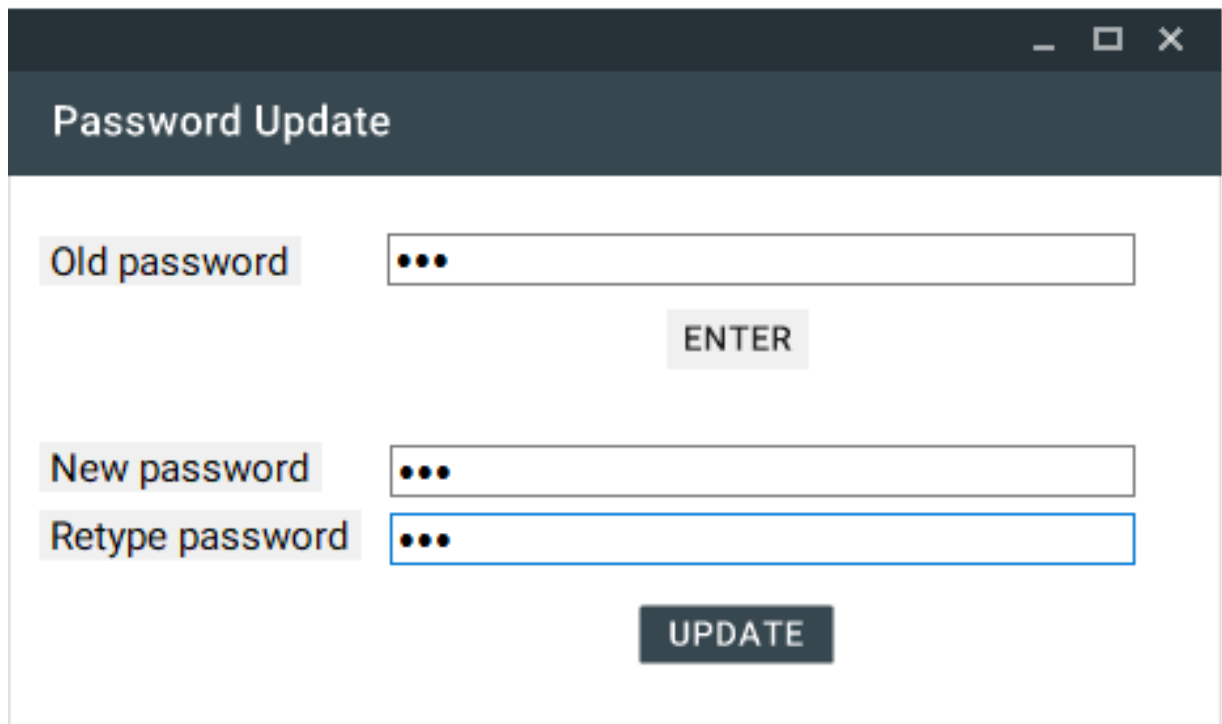


Figure 4-24: password update

4.2.13.Password update Screen

After verifying the user's password the update part is activated to the user to enter a valid password to replace the old password and after clicking the button "UPDATE" the new password is updated to the user and he can use it to access the account.



The screenshot shows a web application window titled "Password Update". The window has a dark header bar with the title "Password Update" in white text. Below the header, the main content area is white. It contains three input fields for passwords, each with a label to its left and three dots inside the field to indicate that the text is masked. The labels are "Old password", "New password", and "Retype password". Below the "Old password" field is a light gray button labeled "ENTER". Below the "New password" and "Retype password" fields is a dark gray button labeled "UPDATE".

Figure 4-25: confirm password

4.2.14.Plain text Screen

Figure 4-26 shows a plaintext accessible by every user in the system and we will perform the encryption algorithm on it.



Figure 4-27: file before encryption

4.2.15. Encrypted text Screen

Figure 4-28 shows The text after applying the encryption algorithm is unreadable by any user but only can be decrypted by the encrypting user.



Figure 4-29: file after encryption

4.2.16. Decrypted Image Screen

Figure 4-30 shows A valid image file visible by every user in the system we will run the encryption algorithm on it.

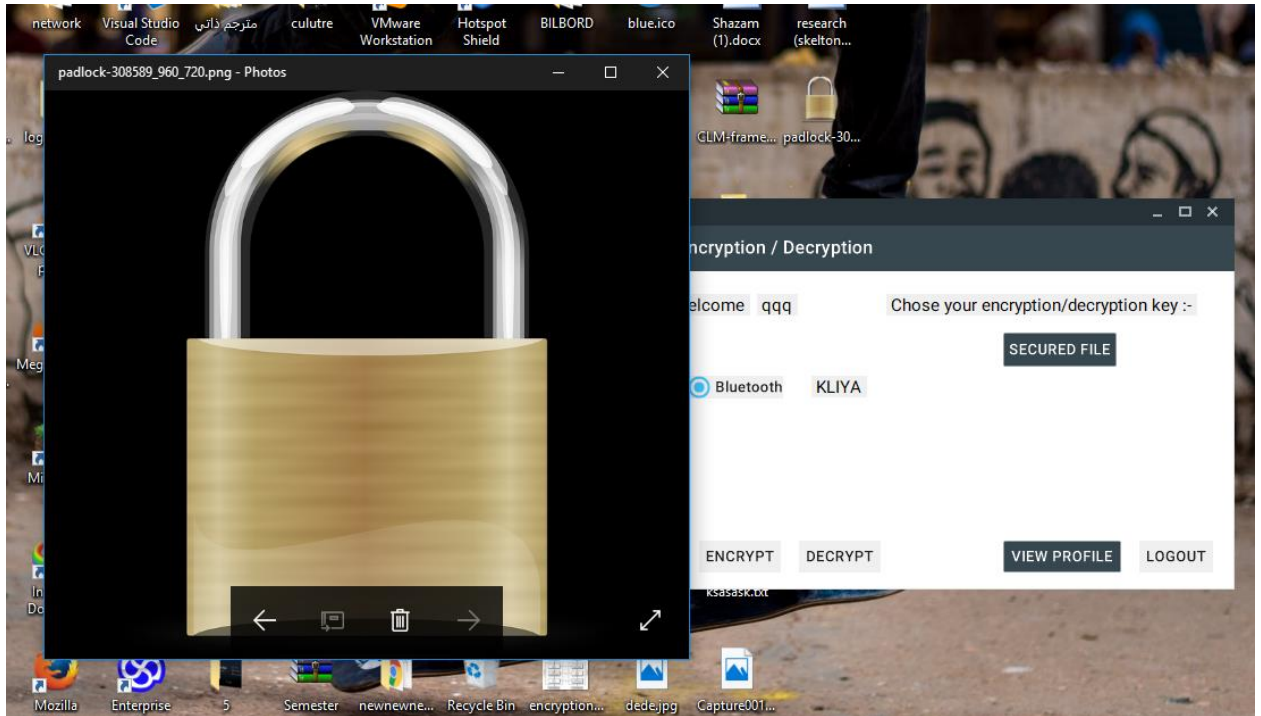


Figure 4-31: Image file before encryption

4.2.17. Encrypted Image Screen

Figure 4-32 shows Image file which is not visible also can be accessed by the user who used his key to encrypt the file.

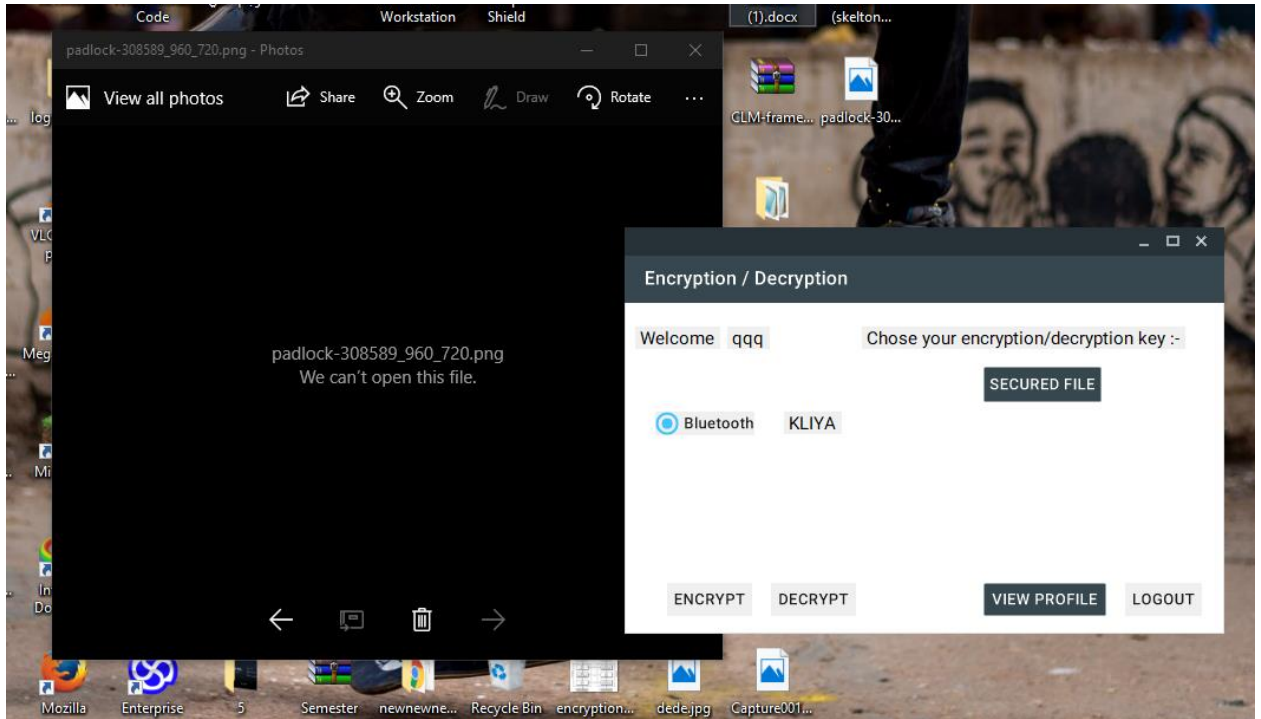
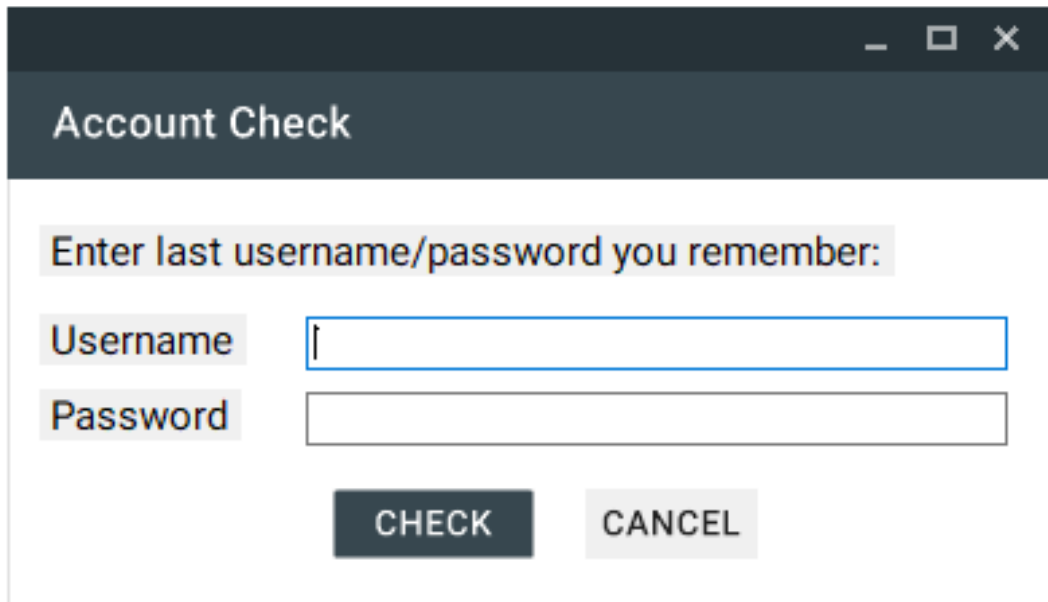


Figure 4-33: Image file after encryption

4.2.18.Account Check Screen

After the user clicks on “HARD RESET” Figure 4-34 appears to the user to verify that he have an existing account that he can’t access by providing the application with the username and password and after clicking “CHECK” it proceeds to the next step and can also click “CANCEL” to cancel and return to login screen.



The screenshot shows a window titled "Account Check" with a dark header. Below the header, there is a prompt: "Enter last username/password you remember:". Underneath this prompt are two input fields: "Username" and "Password". The "Username" field has a blue border and a cursor. Below the input fields are two buttons: "CHECK" (dark grey) and "CANCEL" (light grey).

Figure 4-35: check account

4.2.19. Email Verification Screen

After verifying that the user have an account on the application it requests the user to fill in their e-mail to make sure it belongs to that user and on clicking the button “SEND” the user receives an e-mail from the application containing a verification code will be used in Figure 4-36.

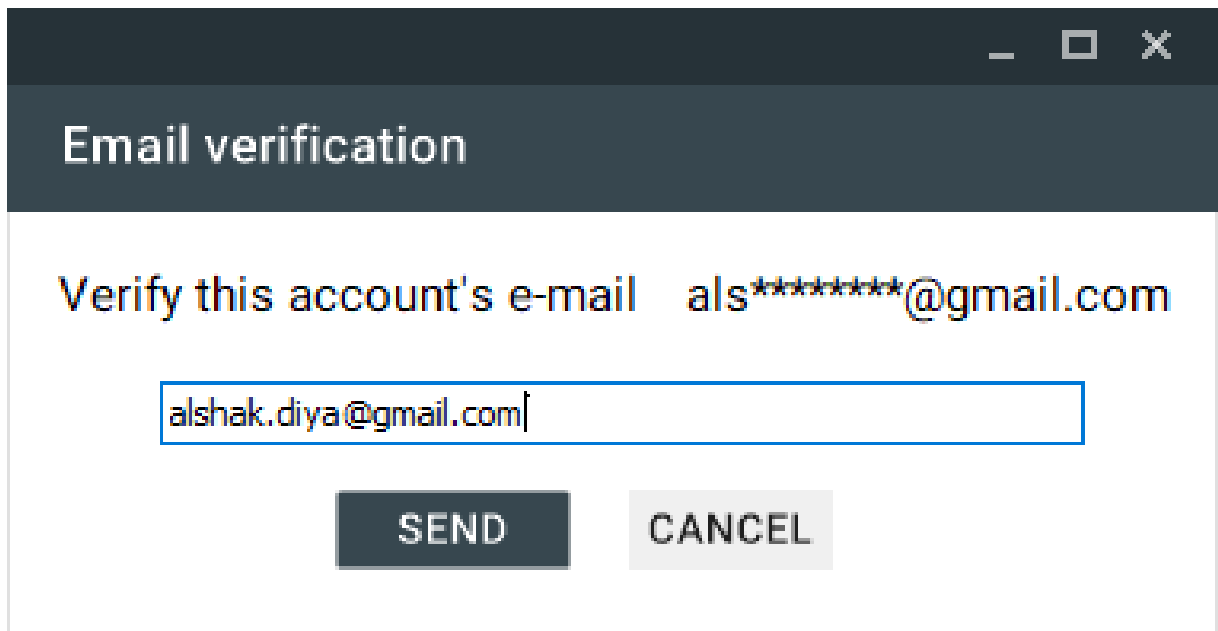


Figure 4-37: email verification

4.2.20. Verification Code Message:

After clicking on “SEND” button the system sends a message to the user’s e-mail that contains the verification code for his process. Figure 4-38 shows the E-mail inbox.

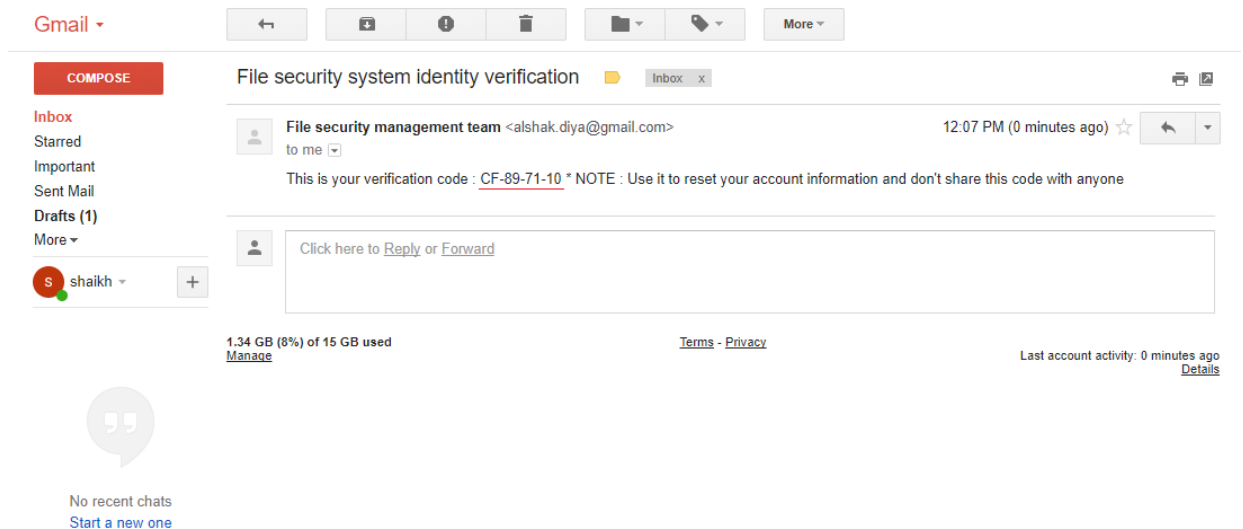
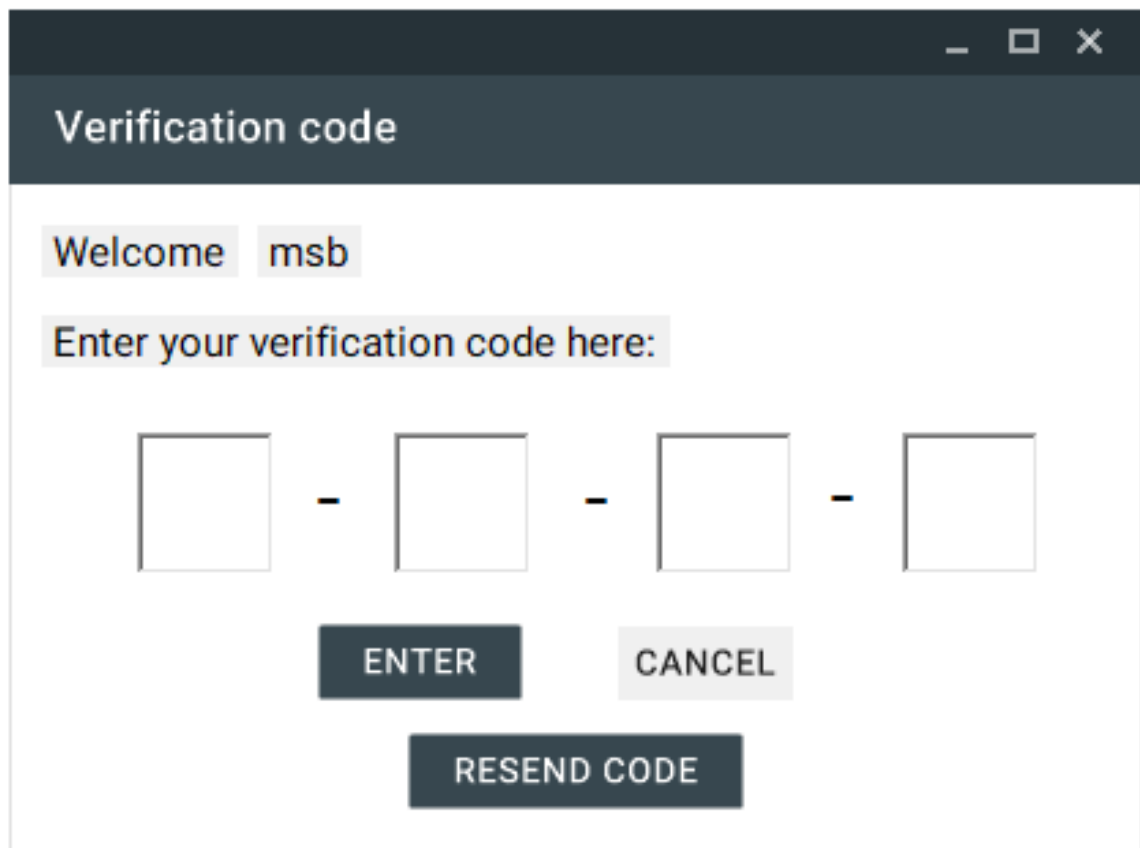


Figure 4-39: verification code message

4.2.21.Account Check Screen

After the user receive his e-mail and enter the code on Figure 4-40 below the user can click “ENTER” to redirect the application to the rest interface to which the user can update his keys and information, or resending other verification code on the email by clicking on “RESEND CODE” and canceling the process and going back to the locking screen by clicking on “CANCEL”.



The image shows a software interface for entering a verification code. At the top, there is a dark grey header bar with the text "Verification code" in white. Below the header, the text "Welcome msb" is displayed. A light grey box contains the instruction "Enter your verification code here:". Underneath this instruction are four empty square input fields arranged horizontally, separated by small dashes. Below the input fields are three buttons: a dark grey button labeled "ENTER", a light grey button labeled "CANCEL", and a dark grey button labeled "RESEND CODE".

Figure 4-41: verification code

Chapter 5

Results, conclusion and Recommendations

5.1. Introduction

This chapter introduces the research conclusions understanding and what is learned during the development of this system and the difficulties that lead to the results that have been achieved by this system's operations and recommendations for future studies.

5.2. Results

This application supports different file types to give the same results intended in the project objectives as:

- Successfully registered non-existing users into the system gathering their necessary information and keys used in encrypting their files
- Providing a portable encryption platform to encrypt and decrypt user's data even on public computers.
- Providing other level on security on top of user's data by encrypting them.

5.3. Conclusion

In conclusion of this project the operation of completely securing user's data could be nearly impossible, but with a good level of security awareness the user can keep his critical data secured by choosing the appropriate way to secure the data, and while using Windows OS data securing methods will not allow the user to use the data in other devices that prevents it from being available at any time and also using the second approach by compressing and adding a password on the compressed data can cause the corruption of data or can be accessed using the password if it's compromised and that will mean an unauthorized access to the data which is too risky, Another problem is that anyone who has

access to your system drive can break EFS encryption and If you copy the file to a floppy disk or to any other file system, the file is no longer encrypted, also Once an EFS folder is created, any files created in the folder will always be encrypted by the creator of the file .But when using this project’s methodology it guarantees that the data will never be corrupted as shown in the previous chapters as the algorithm used in this application only alters the values of the data using the unique identifier for a device which is unique around the world and which means even if a third party has the same software can’t access the data unless the key exists[12].

Also taking advantage of every day's portable devices using them as an encryption key is good for security while every single device holds a unique identifier but also insecure taken what could happen to them, but providing the user with a backup password guarantees the user's access to his data whenever needed. And also the ability to reset physical keys using the user’s verified e-mail address gives the user the ability to replace his keys whenever lost.

5.4. Recommendations

After the completion of this project and applied it, here are some recommendations to improve the system:





- Implementing the application across web to provide distribution of data so that the user can access his data from the cloud.
- Providing face recognition identification to guide the user directly to their main page
- Providing the user with the option of choosing the encryption algorithm to be used on their data based on the importance of the files.
- Use asymmetric encryption algorithm requiring the user to use two keys for his encryption.





References

- [1] <http://searchsecurity.techtarget.com/definition/information-security-infosec>
- [2] <https://des.az.gov/about-des/welcome-to-des>
- [3] https://www.tutorialspoint.com/cryptography/triple_des.htm
- [4] j. h. r. (. Department of Computer Cs. & Engg shri jagdishprasad Jhabarmal tibrewala University, "Performance Evaluation of Java File Security System (JFSS)," 5 2 2010.
- [5] S. M. C. Willis H. ware (the RAND Corporation, "Security and Privacy in Computer Systems," 17 4 1967.
- [6] D. o. C. E. D. U. Seung-Ju Jang, "Developing File Security for Windows Operation System," 6 5 2010.
- [7] D. o. E. (. a. S. P. L. R. B. R. C. o. E. L. R. N. K. D. M. (. B. R. R. (. (. P. D. o. E. (. a. S. Peketi Divya (M.Tech Student, "Data Security System Using Encryption Key in Digital Image for Secret Communication," 1 2015.
- [8] <http://searchsoftwarequality.techtarget.com/definition/Unified-Modeling-Language>
- [9] [https://msdn.microsoft.com/en-us/library/fx6bk1f4\(v=vs.90\).aspx](https://msdn.microsoft.com/en-us/library/fx6bk1f4(v=vs.90).aspx)
- [10] <https://32feet.codeplex.com/documentation>
- [11] [https://msdn.microsoft.com/en-us/library/system.management.managementobjectsearcher\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.management.managementobjectsearcher(v=vs.110).aspx)
- [12] [https://msdn.microsoft.com/en-us/library/windows/desktop/aa364223\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa364223(v=vs.85).aspx)

Appendix

Appendix (I) explain the symbols used in the modeling and analysis system using UML diagrams.

 Actor			 USE CASE
User	Connect	Connect task depending on other task	Task

			
Begin	Finish	Connect	Activity