CHAPTER 1

INTRODUCTION

1.1. INTRODUCTION

Security of the computer files and folders have been a core issue ever since the advent of the windows. Passwords were then introduced to solve this issue but they themselves lend a host of disadvantages. This chapter gives a description about what are the disadvantage of the passwords Also we present a way to secure our own personal folders on the devices that we normally use such as laptops and personal computers. Here we use Bluetooth as a means to authenticate the user and also use Rijndael algorithm to encrypt and thus secure the files and folders from unauthorized access. In this Bluetooth of a phone is used to register users of the device and he can specify a set of files or folder to be encrypted and locked. These files are encrypted using Rijndael algorithm and thus making them impossible to read till device is unlocked i.e. it is connected with Bluetooth. Your application will starts in the background as soon as you start your laptop or personal computer.

1.2.OBJECTIVE

In present day, the increasing reliance on computer systems has led to the dependence on confidential security measures. In this chapter we proposed a Two Factor Authentication [T-FA] system utilizing Bluetooth as a factor coupled with the powerful Rijndael Encryption Algorithm. Bluetooth is the most commonly used technology for Point to Point short range of communication of devices.

Besides from being commonly used, it also offers multi connection. Rijndael algorithm is an Advanced Encryption standard, believed to be the most effective encryption and decryption cryptographic algorithm. Its minimum 10 rounds of encryption and variable key size with a minimum of 128 bits makes it difficult to crack. Coupling the widespread accessibility of Bluetooth and powerful encryption of Rijndael, a Two Factor Authentication System [T-FA] can be created which will not only efface the disadvantages of passwords, but also create a user friendly security system.

1.3.PROBLEM ANALYSIS

In Existing Systems Although passwords are usually considered in terms of authentication for a service or a device, today they are encountered in many other ways in the workplace – and existing password policies do not cover these. As a result, users adopt ad-hoc solutions, which are usually insecure. There are many reasons due to which password is considered as a weak form of protection. Passwords are user-dependent in network security chain. Users often do not take security procedures for password seriously. This leads to vulnerabilities in passwords. Major problems faced by passwords are follows:

- Noting down of difficult passwords
- Periodic change of passwords
- Using dictionary words as passwords
- Personal information. Example: Username, initials etc.
- Use of default passwords. Example: password
- Double words
- Reverse words
- Mixed case dictionary

Vulnerability is an imperfection in the system which can be victimized by the intruder to weaken the system. This imperfection may be present in design, implementation or maintenance of the system. We can easily block threats if we establish control over the vulnerability.

Various kinds of vulnerabilities exist in the password protection system. Synthesizing a strong password and generating a high extremity on the frequency of guesses to minify cracking. Stronger policies could also be implemented using Single SignOn. The load on user shrinks with the help stronger passwords. Opportunistic misuse of unattended desktops can be palliated with the help of screen locks and time-out. Password expiry and prevention of recently used passwords also helps reduce the attack on passwords. Different problems faced by passwords have different solutions. To overcome this two factor authentication is used. It provides single solution to all the problems faced by passwords.

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. These factors include, passwords, representing ‘something you know, or physical tokens representing ‘something you have’. Additionally, biometric traits are applied, representing ‘something you are’”.

CHAPTER 2

TECHNOLOGY USED

2.1 PyQt5

PyQt is a Python binding of the cross-platform GUI toolkit Qt, implemented as a Python plug-in. PyQt is free software developed by the British firm Riverbank Computing. It is available under similar terms to Qt versions older than 4.5; this means a variety of licenses including GNU General Public License and commercial license, but not the GNU Lesser General Public License. PyQt supports Microsoft Windows as well as various flavours of UNIX, including Linux.

PyQt implements around 440 classes and over 6,000 functions and methodsincluding:

- a substantial set of GUI widgets
- classes foraccessing SQL databases (ODBC, MySQL, PostgreSQL, Oracle, SQLite)
- QScintilla, Scintilla-based rich text editor widget
- data aware widgets that are automatically populated from a database
- an XML parser
- SVG support
- classes for embedding ActiveX controls on Windows (only in commercial version)

2.1.1 QtGui

QtGui basically Deals with the graphical elements.

2.1.2 QtCore

QtCore deals with other non-GUI essentials.

2.1.3 Qtwidgets

QtGui.QWidget has many member functions, but some of them have little direct functionality; for example, PySide.QtGui.QWidget has a font property.

To automatically generate these bindings, Phil Thompson developed the tool SIP, which is also used in other projects.In August 2009, Nokia, the then owners of the Qt toolkit, released PySide, providing similar functionality, but under the LGPL,after failing to reach an agreement with Riverbank Computing to change its licensing terms to include LGPL as an alternative license.

PyQt5 contains the following Python modules:

- QtQml Module
- QtQtuick Module
- QtCore Module
- QtGui Module
- QtPrintSupport Module
- QtWidgets Module
- QGLContext ModuleQGLFormat Module
- QGLWidget Module
- QtWebKit Module
- QtWebKitWidgets Module

2.2 PYTHON

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable.

It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages.

Python has simple syntax, modular architecture, rich text processing tools and the ability to work on multiple operating systems which make it a desirable choice for developing desktop-based applications. There are various GUI toolkits like wxPython, PyQt or PyGtk available which help developers create highly functional Graphical User Interface (GUI).

2.3 PyBluez

PyBluez is a Python extension module written in C that provides access to system Bluetooth resources in an object oriented, modular manner. It is written for the Windows XP (Microsoft Bluetooth stack) and GNU/Linux . Bluetooth Python extension module to allow Python ” “developers to use system Bluetooth resources. **PyBluez** works ” “with GNU/Linux and Windows XP.**PyBluez** is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

2.4 SQL

SQL is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS). It is particularly useful in handling structured data where there are relations between different entities/variables of the data. SQL offers two main advantages over older read/write APIs like ISAM or VSAM. First, it introduced the concept of accessing many records with one single command; and second, it eliminates the need to specify how to reach a record, e.g. with or without an index.

Originally based upon relational algebra and tuple relational calculus, SQL consists of many types of statements which may be informally classed as sublanguages, commonly: a data query language (DQL), a data definition language (DDL), a data control language (DCL), and a data manipulation language (DML). The scope of SQL includes data query, data manipulation (insert, update and delete), data definition (schema creation and modification), and data access control. Although SQL is often described as, and to a great extent is, a declarative language (4GL), it also includes procedural elements. SQL was one of the first commercial languages for Edgar F. Codd's relational model. The model was described in his influential 1970 paper, "A Relational Model of Data for Large Shared Data Banks".Despite not entirely adhering to the relational model as described by Codd, it became the most widely used database language. SQL became a standard of the American National Standards Institute (ANSI) in 1986, and of the International Organization for Standardization (ISO) in 1987. Since then, the standard has been revised to include a larger set of features. Despite the existence of such standards, most SQL code is not completely portable among different database systems without adjustments.

SQL was initially developed at IBM by Donald D. Chamberlin and Raymond F. Boyce after learning about the relational model from Ted Codd in the early 1970s. This version, initially called SEQUEL (Structured English Query Language), was designed to manipulate and retrieve data stored in IBM's original quasi-relational database management system, System R, which a group at IBM San Jose Research Laboratory had developed during the 1970s. By 1986, ANSI and ISO standard groups officially adopted the standard "Database Language SQL" language definition. New versions of the standard were published in 1989, 1992, 1996, 1999, 2003, 2006, 2008, 2011, and most recently, 2016.

SQL deviates in several ways from its theoretical foundation, the relational model and its tuple calculus. In that model, a table is a set of tuples, while in SQL, tables and query results are lists of rows: the same row may occur multiple times, and the order of rows can be employed in queries (e.g. in the LIMIT clause).

Critics argue that SQL should be replaced with a language that strictly returns to the original foundation: for example, see The Third Manifesto. However, no known proof exists that such uniqueness cannot be added to SQL itself, or at least a variation of SQL.

In other words, it's quite possible that SQL can be "fixed" or at least improved in this regard such that the industry may not have to switch to a completely different query language to obtain uniqueness. Debate on this remains open.

The SQL language is subdivided into several language elements, including:

- Clauses, which are constituent components of statements and queries.
- Expressions, which can produce either scalar values, or tables consisting of columns and rows of data
- Predicates, which specify conditions that can be evaluated to SQL three-valued logic (3VL) (true/false/unknown) or Booleantruth values and are used to limit the effects of statements and queries, or to change program flow.
- Queries, which retrieve the data based on specific criteria. This is an important element of SQL.
- Statements, which may have a persistent effect on schemata and data, or may control transactions, program flow, connections, sessions, or diagnostics.
    - SQL statements also include the semicolon (";") statement terminator. Though not required on every platform, it is defined as a standard part of the SQL grammar.
- Insignificant whitespace is generally ignored in SQL statements and queries, making it easier to format SQL code for readability.

CHAPTER 3

PURPOSE OF THE APPLICATION

3.1 PROBLEM DEFINATION

Protecting data has been our primary concern for the computer users all over the world. In today's time people are entrusted with very sensitive data i.e. of personal and organizational use. Windows authentication policies provide securities to a limited extent. However, these policies do not ensure guarantee of personal and organizational security. Windows authentications policies can be broken down easily and cracked easily by the hackers. Hence it does not ensure a full proof security to the users. Windows does not provide any other security mechanism other than this. About 30% of the user's passwords are easy to guess and appear in the hacker's dictionary. Using difficult user passwords can also create a problem of remembering them. Hence people will start writing their passwords on notes, keeping them in desk drawers, etc. which will lead to more problems. People generally choose passwords related to themselves. So other people close to a user can guess the password.

Windows uses simple login authentication process for the authentication of valid users. But this login validation and authentication process is not so strong. User passwords are easily cracked by hackers as the passwords are generally user specific and related to users. The passwords kept by the users are easy to remember passwords and not so strong. These policies are often broken down by hackers to gain system access and update content of user files. Generally, users tend to keep same password for multiple accounts. Also, the frequency of changing the passwords is also very less. Hence is becomes very easy of a person knowing password for one account to get access to another account. This becomes a major drawback for users and a benefit for the intruders.

We now need some other security mechanism(s) to ensure our security. This additional security layer must provide us automated services when we are not in the proximity of the laptop/computer device. In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. Attacker can access the system to steal or make unauthorized changes in sensitive information, commit fraud, or disrupt operations.Primary source of threats that are encountered are employees or insider attack and malicious hackers or outsider attack. Both can reach the private data and penetrate the security system. The overall aim of the proposed system is protecting any private data from illegal access or from damage and keeping the used keys in the encryption process safe against any pilfering by applying a new method. This method is a three layer encryption with a new key management system approach using windows registry.

3.2 SCOPE

This technology makes data theft a much more difficult task for hackers. It encrypts all the files, and when you access them, it decrypts them behind the scenes and re-encrypts them when you're done. However, if another user attempts to access the file, by opening, renaming, moving, etc., they will receive an access-denied message. Only the user that *encrypted* the file can open it. Everyone, from individuals to corporations, wants be reassured that their confidential information.

The main idea of the system depends on file encryption plaintext transformation- using encryption algorithm to make it meaningless data that cannot be read without decrypting the data back into its meaningful form. The system target is to keep a file unreadable to anyone except those possessing special knowledge, usually referred to as a key. Keys are saved with authenticated parties to be kept on their personal smart devices.

The proposed system applies a decentralized security system by using the unique MAC Address which guarantees that the decryption did not occur until the Bluetooth device is connected to the system. Inconsequence if the insider or outsider attack can get the encrypted data cannot get the MAC Address and the keys which are stored in the Windows Registry which cannot be accessed unless the user is the administrator The used keys in the encryption process are generated internally in the system and no one have authority to get their contents which is called a ―blind technology‖ that guarantees the keys safeness against keylogger attack. It is a tool designed to record –log– every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. After the encryption process of the private data completes the encrypting keys are encrypted with cryptography algorithm stored in the Registry. The proposed system prevents any insider or outsider attacks in the private data by encrypting the specified data with a Rijndael block cipher algorithm and prevents any access without having the used keys. The system deletes the initial plaintext and intermediate cipher texts that are generated through the encryption process and keep only the final cipher text.

Bluetooth is selected as a short range technique that is used to transmit the used keys to the authorized parties. Bluetooth has built-in authentication and encryption systems. The authentication between two devices covers only the knowledge of a common secret key called PIN and the knowledge of the device addresses. Encryption is a separate process that starts after authentication is successfully finished.

CHAPTER 4

METHOD FOR SOLVING THE PROBLEM

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. Attacker can access the system to steal or make unauthorized changes in sensitive information, commit fraud, or disrupt operations.

4.1 PROPOSE WORK

Primary source of threats that are encountered are employees or insider attack and malicious hackers or outsider attack. Both can reach the private data and penetrate the security system.

The overall aim of the proposed system is protecting any private data from illegal access or from damage and keeping the used keys in the encryption process safe against any pilfering by applying a new method. This method is a three layer encryption with a new key management system approach using windows registry.

This research focuses on Two Factor Authentication system introducing the use of mobile phones tokens employing Bluetooth and Rijndael Encryption.

Bluetooth is enabled in your laptop or PC. An interface is written to discover the Bluetooth devices by their MAC address and the same is authenticated with the Admin password.

Registry of system stores the MAC address. Application is initiated as a background process along with the PC. The folder in which the user is currently working on is selected in the configuration mode. A Handshake protocol is implemented by the program every 5 seconds so that whenever the authenticated Bluetooth device moves away from the PC, all the working files and folders are encrypted and account is logged off. After a successful log in, the program will search for the authenticated Bluetooth device and prompt for the password. Successful password matching then decrypts all the files and folders user was working on. In case of mismatch of Bluetooth devices, the application never demands for the password.

In our system there is the client side and the server side.

A. **Server Side (Computer)**

MAC address of the phone and the key is stored into the registry. Bluetooth device is registered into the system. The system searches for the phone if in range or not, if not in range then selected folders get encrypted. While decryption system finds various devices in range and authenticates the authorized phone device to provide access by checking the MAC address stored into the registry.

B. **Client Side (Phone)**

An application is installed into the phone that is provided to enter the key to the system while decryption when the system authenticates the phone. This key is fetched by the system with the help of Bluetooth.

C. **Bluetooth**

Here we are using Bluetooth as the wireless medium for communication between the computer and the phone.

As it provides reliable connection and is easily available in all devices it is being used.

The operation of searching discoverable devices is known as inquiry. It provides low cost in terms of cost and power consumption. It provides speed of 1 to 2 mb/sec.

D. MAC Address

Media Access Control (MAC) is a unique identifier assigned to network interfaces for communication. It has six groups of two hexadecimal digits separated by hyphens or colons, in transmission order. Another convention is using three groups of four hexadecimal digits. A host cannot determine from the MAC address of another host whether that host is on same link as the sending host or on network segment bridged to that network segment. Using MAC address of the electronic device movement of every one in a city can be tracked.

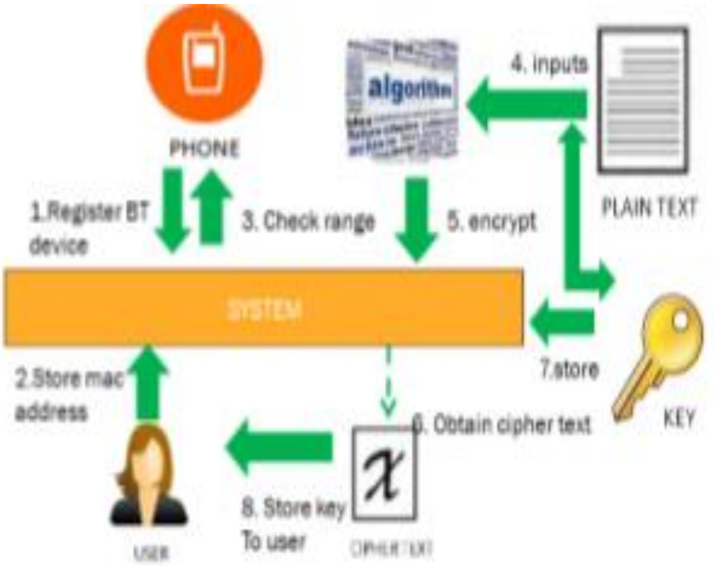


Fig 4.1 Architecture of Proposed System

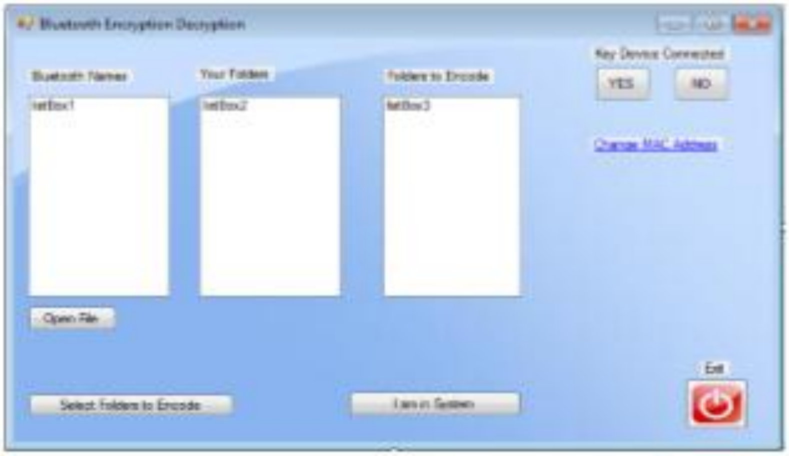


Fig 4.2 Proposed Work

4.2 FUNCTIONS & FEATURES

- Two way authentication
- Bluetooth device
- MAC address
- Encryption
- Decryption

4.3 SECURING COMPUTER FOLDERS WITH RIJNDAEL SECURITY EXTENSION & YOUR BLUETOOTH ENABLED MOBILE PHONE

4.3.1 Bluetooth

Almost every mobile phone device now-a-days is equipped with the Bluetooth technology. Also, most of the computer devices are equipped with this.

Bluetooth technology gives us the feature of communicating with the devices in proximity. Hence only devices near to each other can communicate with each other.

Bluetooth, a wireless technology for the transmission of data among two devices in close propinquity of each other has veritably changed the world.

Securing Computer Folders using Bluetooth and Rijndael Encryption operate on Personal Area Network(PAN).The major advantage that Bluetooth offers for T-FA is its range of network which is just 100 meters and is enough to personify an authenticated user's presence. Bluetooth is a Radio Frequency (RF) specification for short range voice and data transfer, whether it be point-to-point or point to multiple points. Bluetooth will empower the users to connect to a wide range of computing and telecommunications devices without the need for proprietary cables that often fall short in terms of ease-of-use. The technology constitutes an opportunity for the industry to deliver wireless solutions that are ubiquitous across a broad range of devices. The strength and direction of the underlying Bluetooth standard will ensure that all solutions meet stringent expectations for ease-of-use and interoperability (Smart Handheld Group). Bluetooth is unremarkably used in Mobile Phone Market. Almost every phone presently contains Bluetooth in it which makes it a very cost effective T- FA Authenticator. The operational terms of Bluetooth in terms of processing power and battery is also very minimalistic.

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.

4.3.2 Rijndael Algorithm

Rijndael (pronounced rain-dahl) is the algorithm that has been selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). It was selected from a list of five finalists, that were themselves selected from an original list of more than 15 submissions. Rijndael will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years in many cryptography applications. The algorithm was designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose surnames are reflected in the cipher's name. Rijndael has its origins in Square, an earlier collaboration between the two cryptologists.

The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys.

Rijndael uses a variable number of rounds, depending on key/block sizes, as follows:

9 rounds if the key/block size is 128 bits

11 rounds if the key/block size is 192 bits

13 rounds if the key/block size is 256 bits

Rijndael is a substitution linear transformation cipher, not requiring a Feistel network. It use triple discreet invertible uniform transformations (layers). Specifically, these are: Linear Mix Transform; Non-linear Transform and Key Addition Transform. Even before the first round, a simple key addition layer is performed, which adds to security. Thereafter, there are Nr-1 rounds and then the final round. The transformations form a State when started but before completion of the entire process.

The State can be thought of as an array, structured with 4 rows and the column number being the block length divided by bit length (for example, divided by 32). The cipher key similarly is an array with 4 rows, but the key length divided by 32 to give the number of columns. The blocks can be interpreted as unidimensional arrays of 4-byte vectors.

The exact transformations occur as follows: the byte subtransformation is nonlinear and operates on each of the State bytes independently - the invertible S-box (substitution table) is made up of 2 transformations. The shiftrow transformation sees the State shifted over variable offsets. The shift offset values are dependent on the block length of the State.

The mixcolumn transformation sees the State columns take on polynomial characteristics over a Galois Field values (28), multiplied x4 + 1 (modulo) with a fixed polynomial. Finally, the roundkey transform is XORed to the State. The key schedule helps the cipher key determine the round keys through key expansion and round selection.

Overall, the structure of Rijndael displays a high degree of modular design, which should make modification to counter any attack developed in the future much simpler than with past algorithm designs.

1. KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial round key addition:
    1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

9, 11 or 13 rounds:

a. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

b. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

c. MixColumns—a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.

d. AddRoundKey

4. Final round (making 10, 12 or 14 rounds in total):

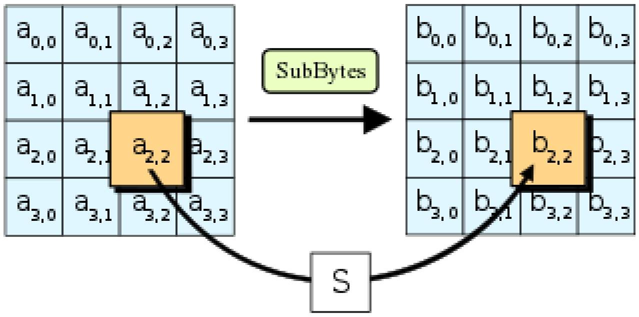
   a. SubBytes

   b. ShiftRows

   c. AddRoundKey

The SubBytes step

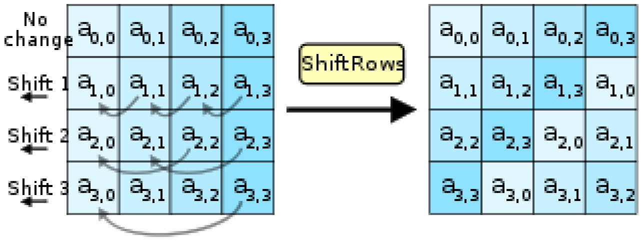
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

In the SubBytes step, each byte in the state array is replaced with a SubByte using an 8-bit substitution box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF(2^8), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), i.e., and also any opposite fixed points, i.e., . While performing the decryption, the InvSubBytes step (the inverse of SubBytes) is used, which requires first taking the inverse of the affine transformation and then finding the multiplicative inverse.

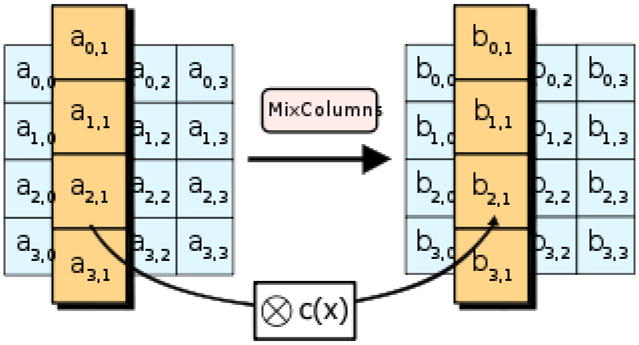
The ShiftRows step

In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.


No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. The importance of this step is to avoid the columns being encrypted independently, in which case AES degenerates into four independent block ciphers.

The MixColumns step


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\otimes$ c(x)

In the MixColumns step, each column of the state is multiplied with a fixed polynomial .

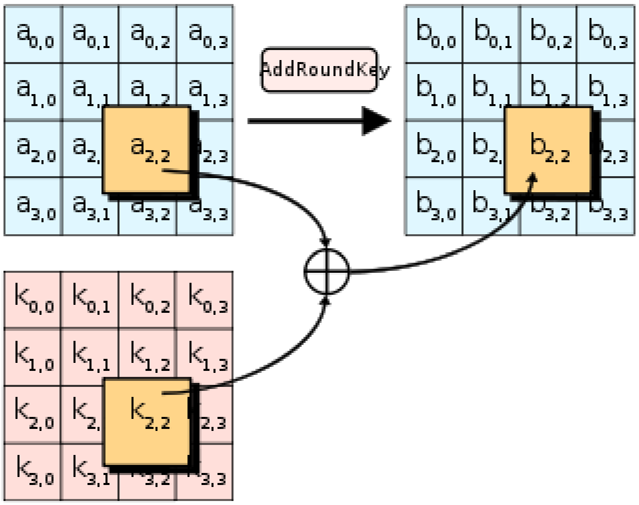
In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher.

During this operation, each column is transformed using a fixed matrix (matrix left-multiplied by column gives new value of column in the state):

Matrix multiplication is composed of multiplication and addition of the entries. Entries are 8-bit bytes treated as coefficients of polynomial of order . Addition is simply XOR. Multiplication is modulo irreducible polynomial . If processed bit by bit, then, after shifting, a conditional XOR with 1B$_{16}$ should be performed if the shifted value is larger than FF$_{16}$ (overflow must be corrected by subtraction of generating polynomial). These are special cases of the usual multiplication in .

In more general sense, each column is treated as a polynomial over and is then multiplied modulo with a fixed polynomial . The coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from . The MixColumns step can also be viewed as a multiplication by the shown particular MDS matrix in the finite field . This process is described further in the article RijndaelMixColumns.

The AddRoundKey Step


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XORoperation (⊕).

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

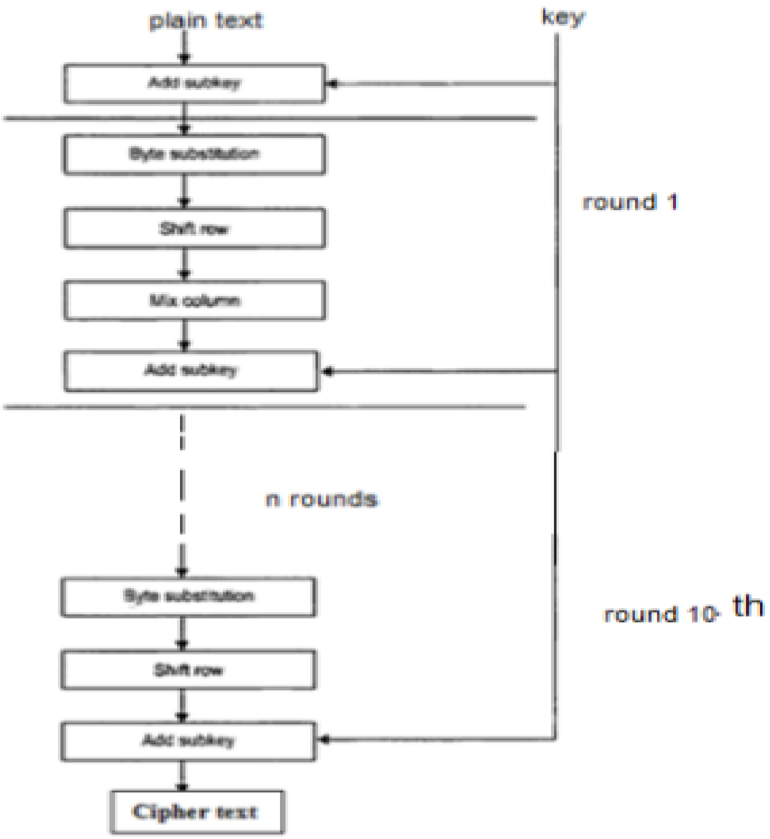


Fig 4.3 Rijndael Algorithm Workflow

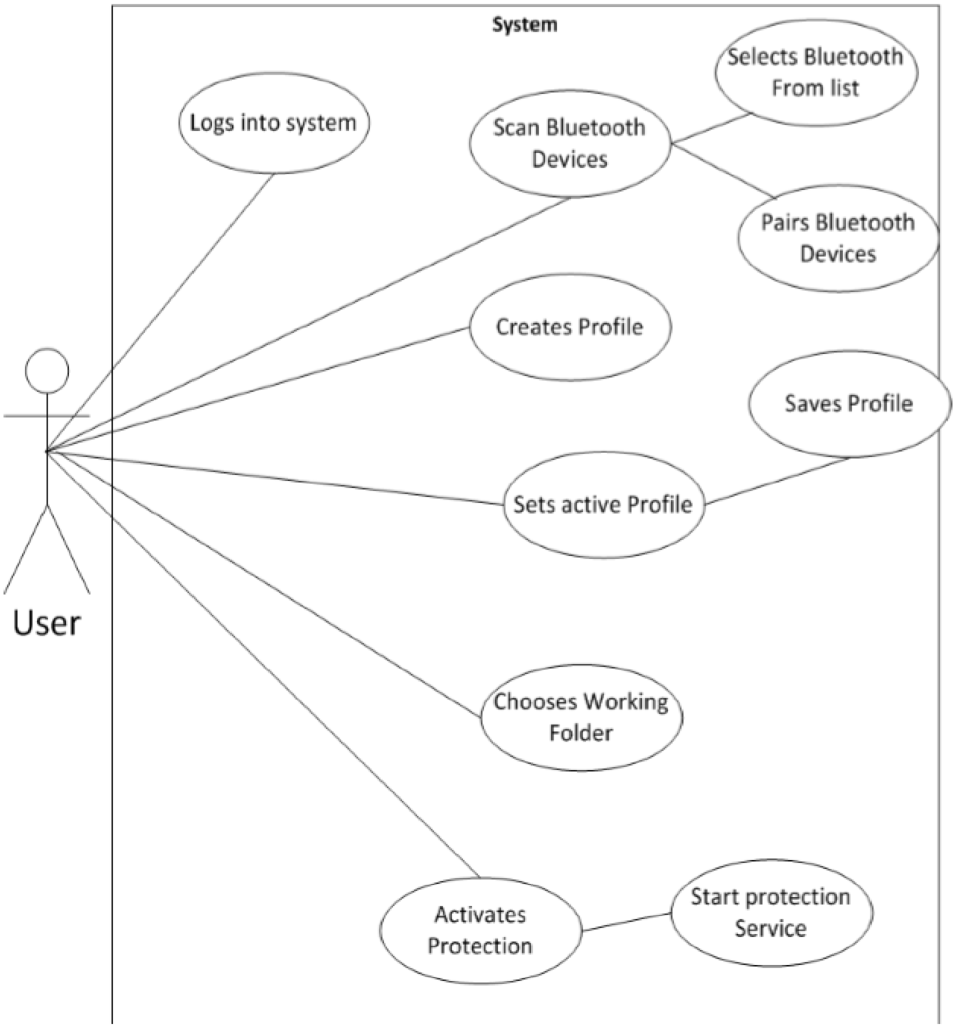
4.3.3 Two Phase Authentication

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 (T- FA) comes in very handy mainly because it focusses on combination of both factors. Christian Rathgeb says in his research, “These factors include, passwords, representing ‘something you know’, or physical tokens, such as smart-cards, representing ‘something you have’.

Android UI designing can be done either in XML or programmatically in application. But the Android UI designer mostly prefer XML for defining UI because it separate the presentation from the code and makes easier to visualize, manage, edit and debug the App.

4.3.4 Use Case Diagram

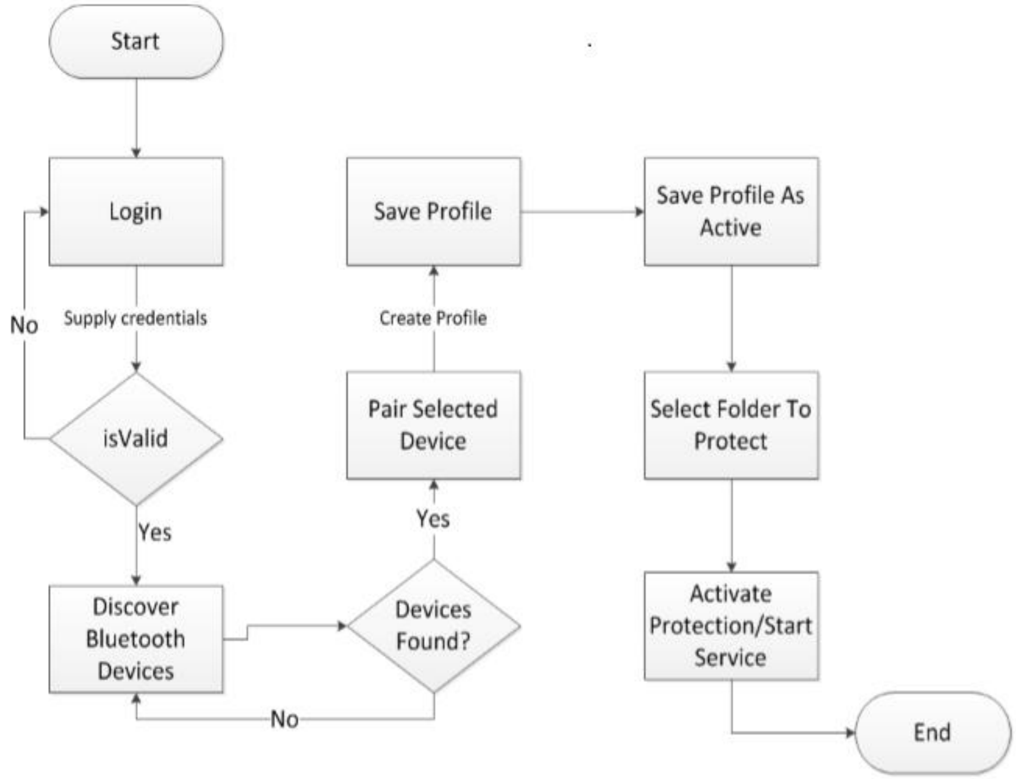


.

Use-case modeling is a technique used to describe the functional requirements of a system. It makes it easier to show the functional requirements in an abstract way that can easily be understood even by the stakeholders of the system, therefore acting more like a communicating tool between the stakeholders and developers.

4.3.5 Flow Chart Diagram

Windows Form Application:



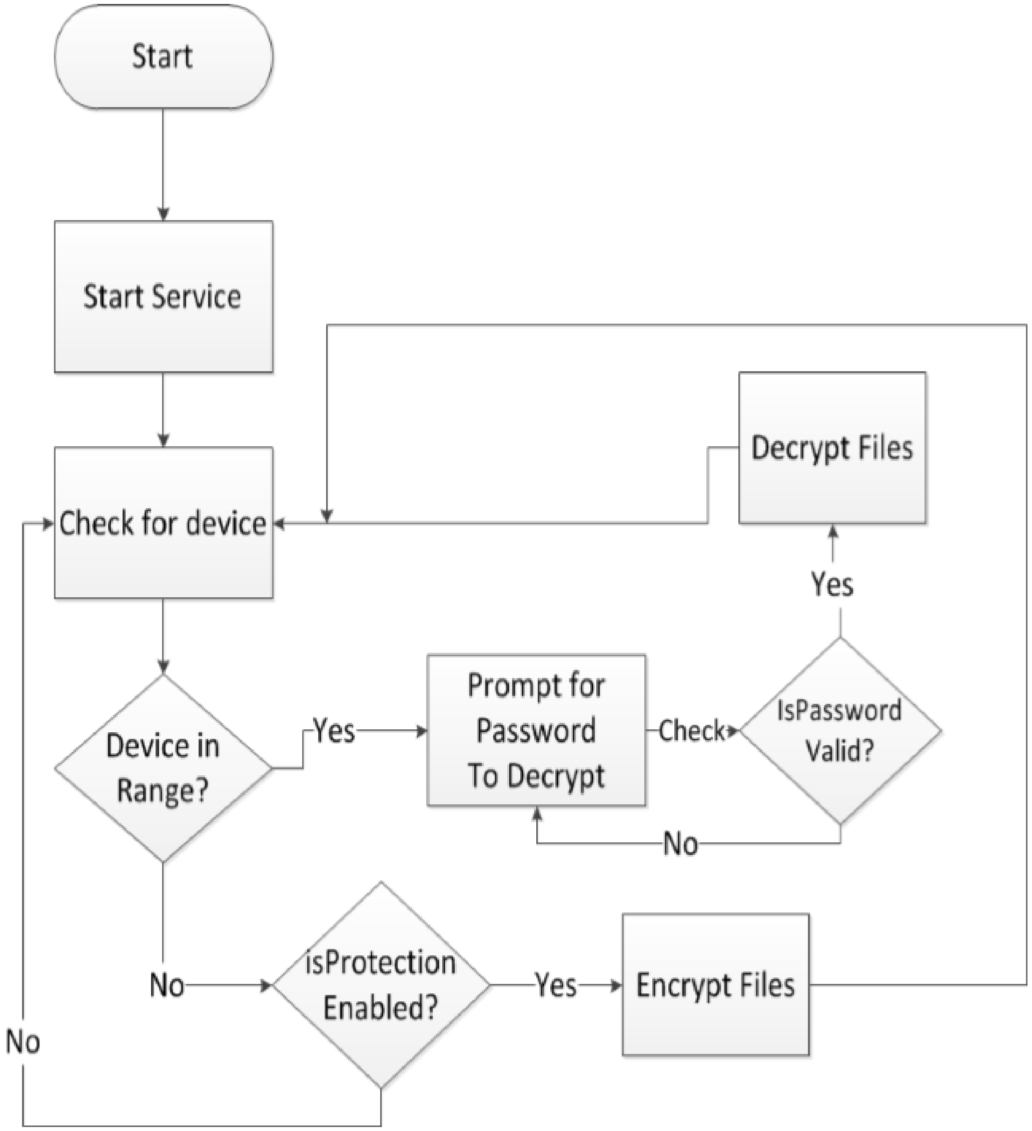
Windows Service:

This is the service that runs in the background for the lifetime of the computer system runtime and will automatically be started when the computer boots. This service has functional requirements that it has to fulfill in order to be fully operational.

<u>Lifetime service</u> – Service must run for the whole time the windows system is running.

<u>Scan Bluetooth Proximity</u> – Service should be able to recognize when a particular Bluetooth device is range. This particular device is the one that is saved in the database as the active profile. It should match the service records of the Bluetooth that match the MAC address of that device.

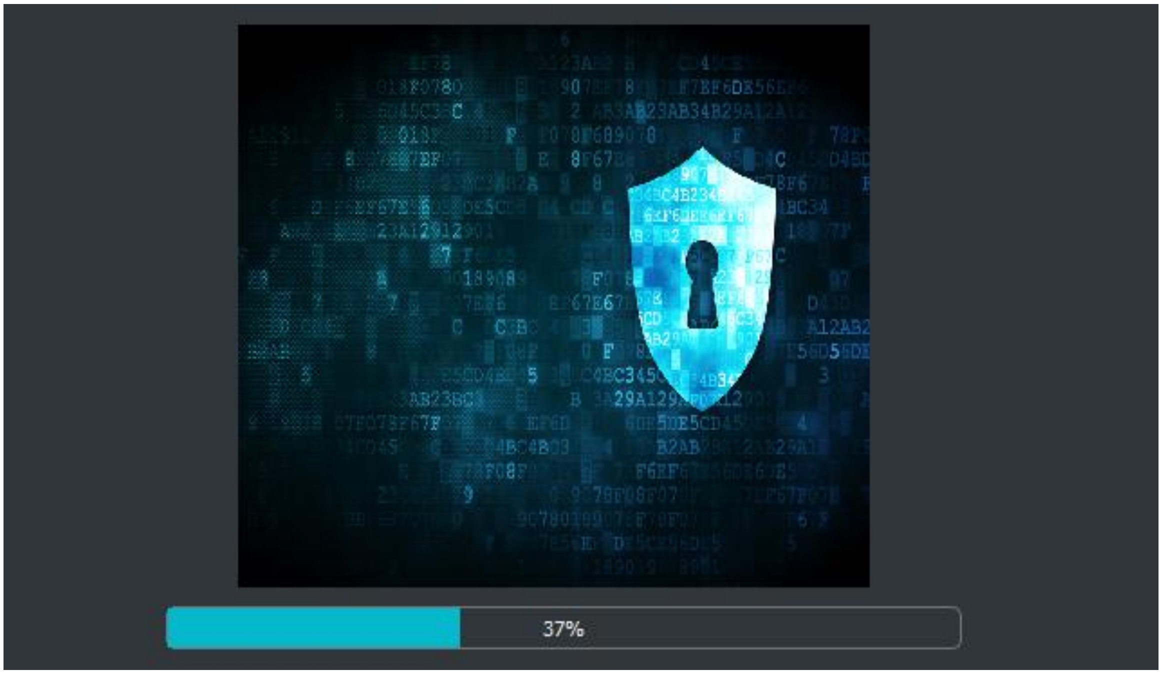
Encrypt Files – Should be able to encrypt files in the working folder whenever the Bluetooth device goes out of range. Lock workstation – The service should automatically lock the windows workstation when the authenticated Bluetooth device is out of range.



CHAPTER 5

SNAPSHOTS OF APPLICATION

5.1 SPLASH SCREEN



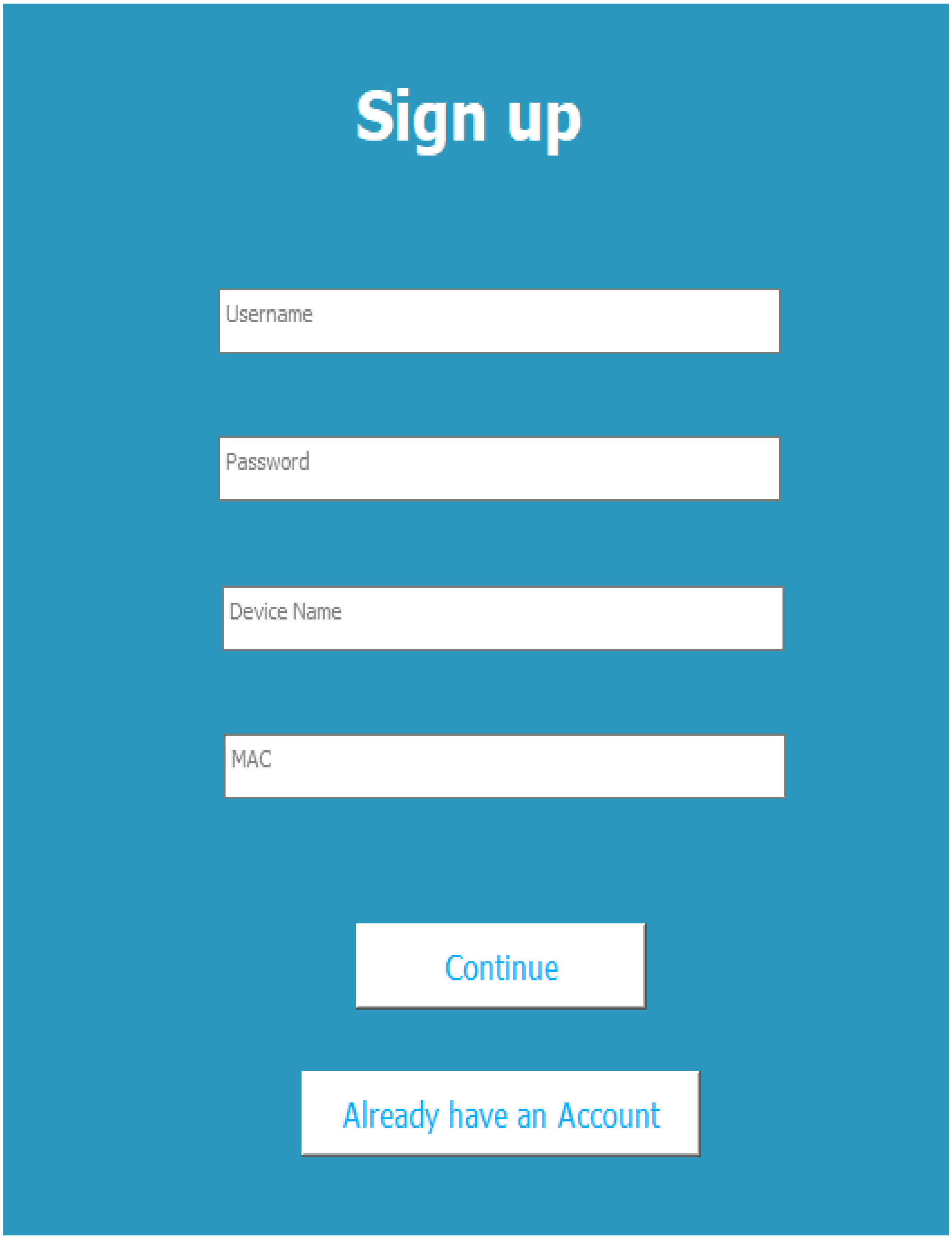
This is the splash screen which will appear when we use our application.

5.2 SIGN UP

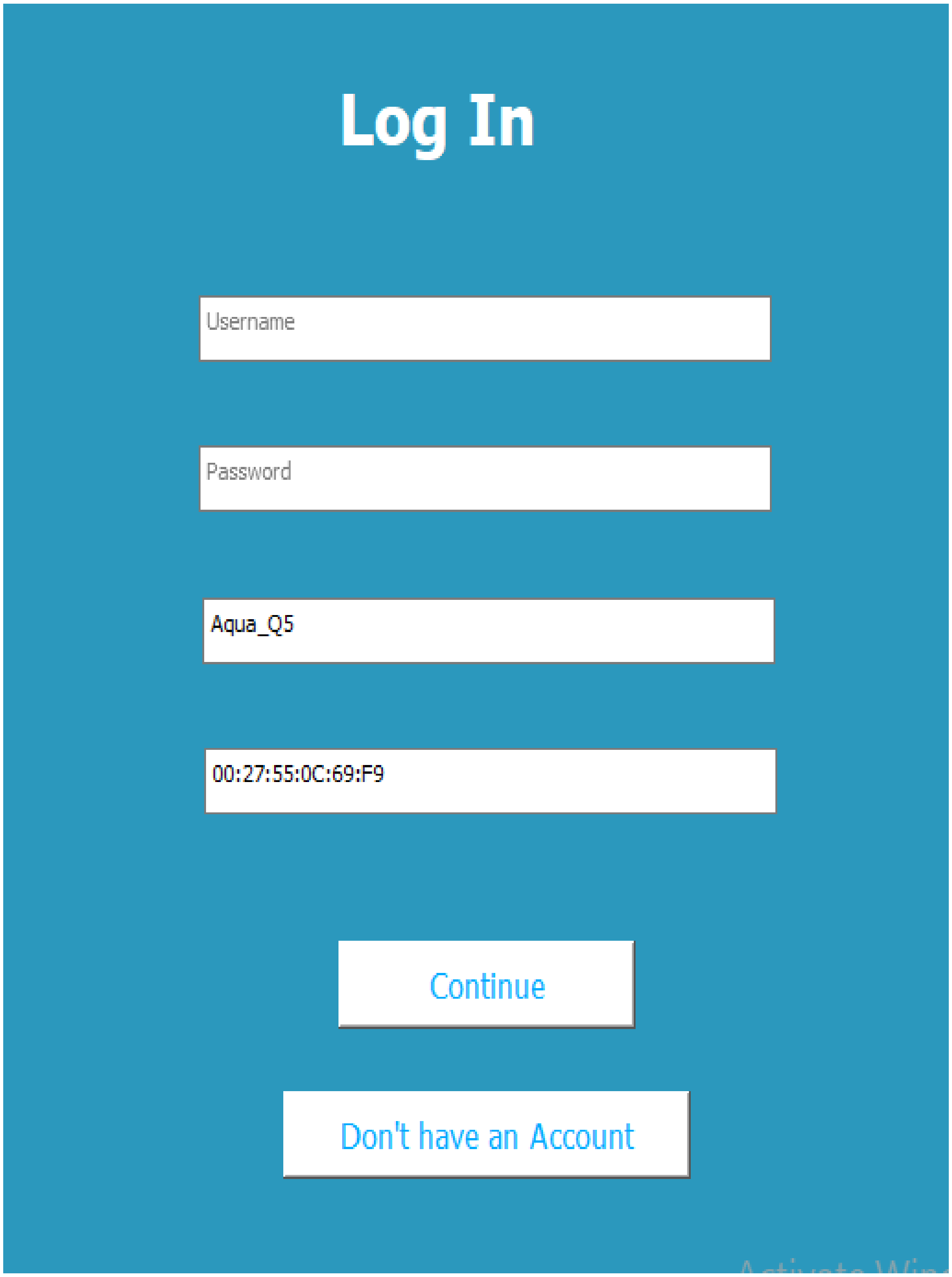
This is the sign up page for our project. In this sign up page a user must enter username and password.

Password does not have restriction for special symbol or number.All fields are compulsory in this page.

If user is already registered then user have to go on “Already have an Account” then it directly goes to the login page.


Sign up
Username
Password
Device Name
MAC
Continue
Already have an Account

5.2LOGIN



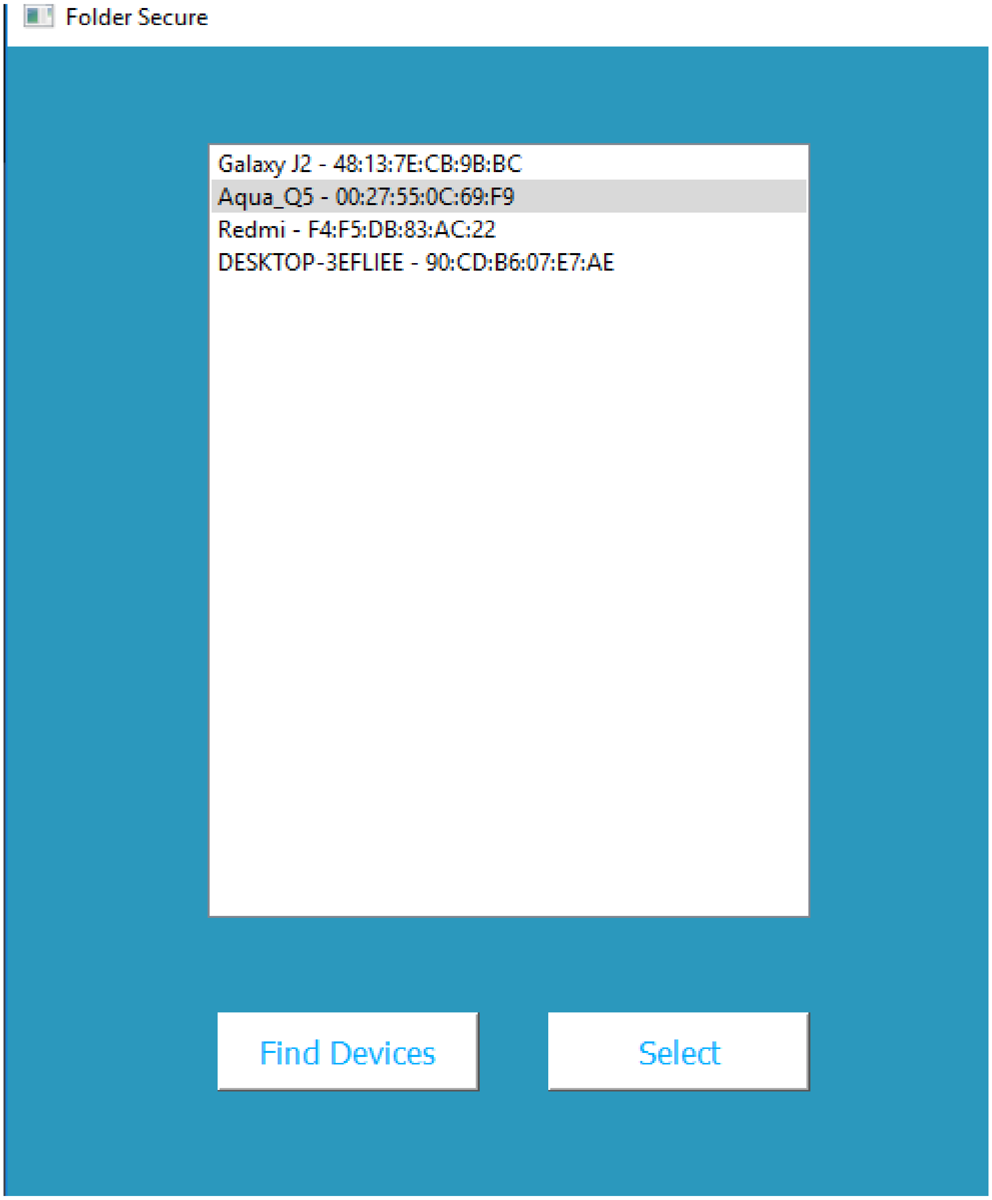
Aqua_Q5

00:27:55:0C:69:F9

This is the login page if the user already registered so by clicking on login button the login page will open. The user give its id or password or mac address with device name for login.

If you was not registered then click on “Don’t have an Account” button to move back to the sign up page.

5.3FINDING AND SELECTING BLUETOOTH DEVICE

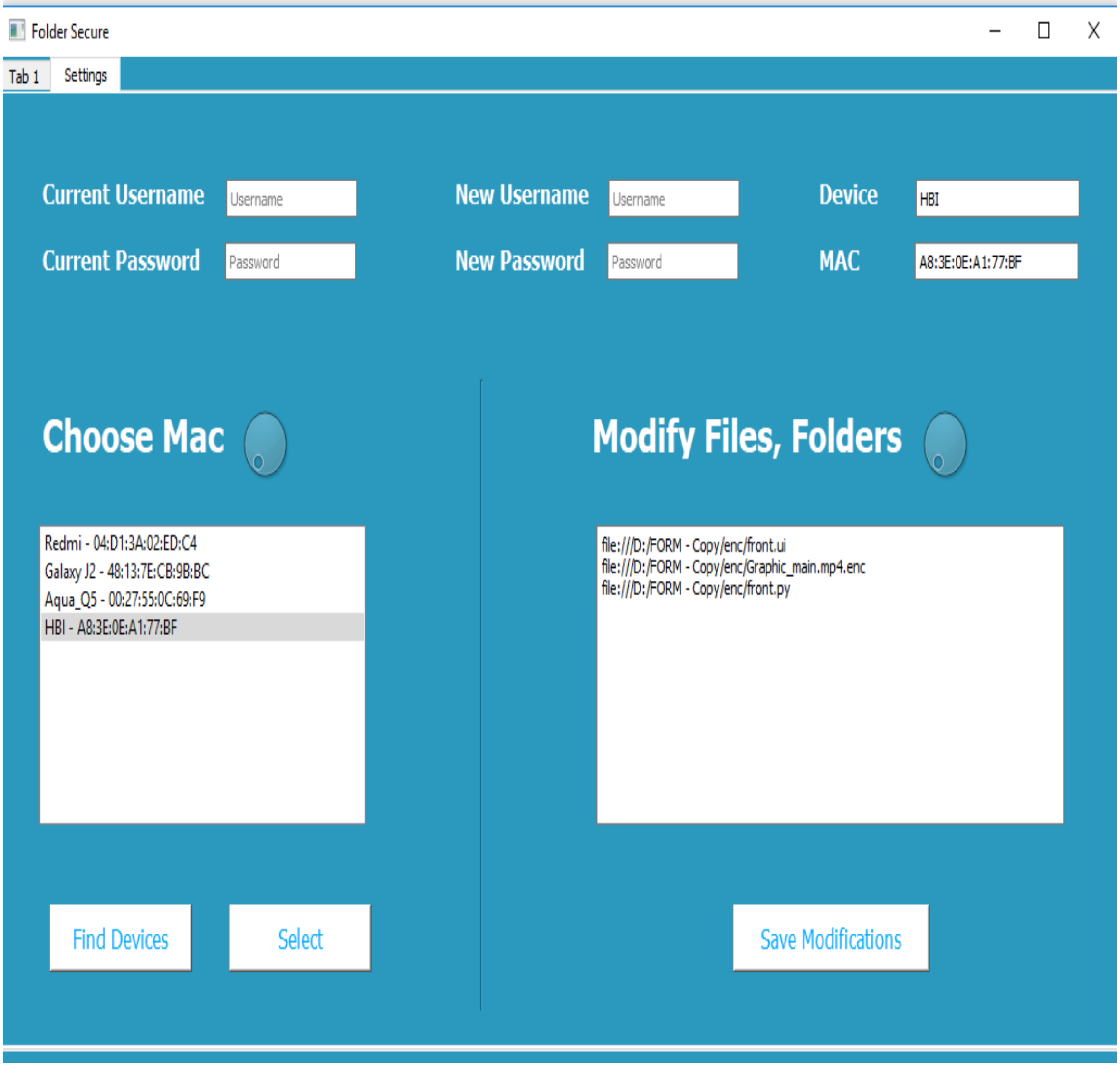


Galaxy J2 - 48:13:7E:CB:9B:BC
Aqua_Q5 - 00:27:55:0C:69:F9
Redmi - F4:F5:DB:83:AC:22
DESKTOP-3EFLIEE - 90:CD:B6:07:E7:AE

After completing tregistration or login process, the user has to find the Bluetooth device which he/she wants to use. There must be a list of all Bluetooth devices nearby.

If your Bluetooth device is in the list then use “Select” otherwise use “Find Devices” option for more Bluetooth device.

5.4 SELECT FILE AND FOLDERS



Device: HBI

MAC: A8:3E:0E:A1:77:BF

Redmi - 04:D1:3A:02:ED:C4
Galaxy J2 - 48:13:7E:CB:9B:BC
Aqua_Q5 - 00:27:55:0C:69:F9
HBI - A8:3E:0E:A1:77:BF

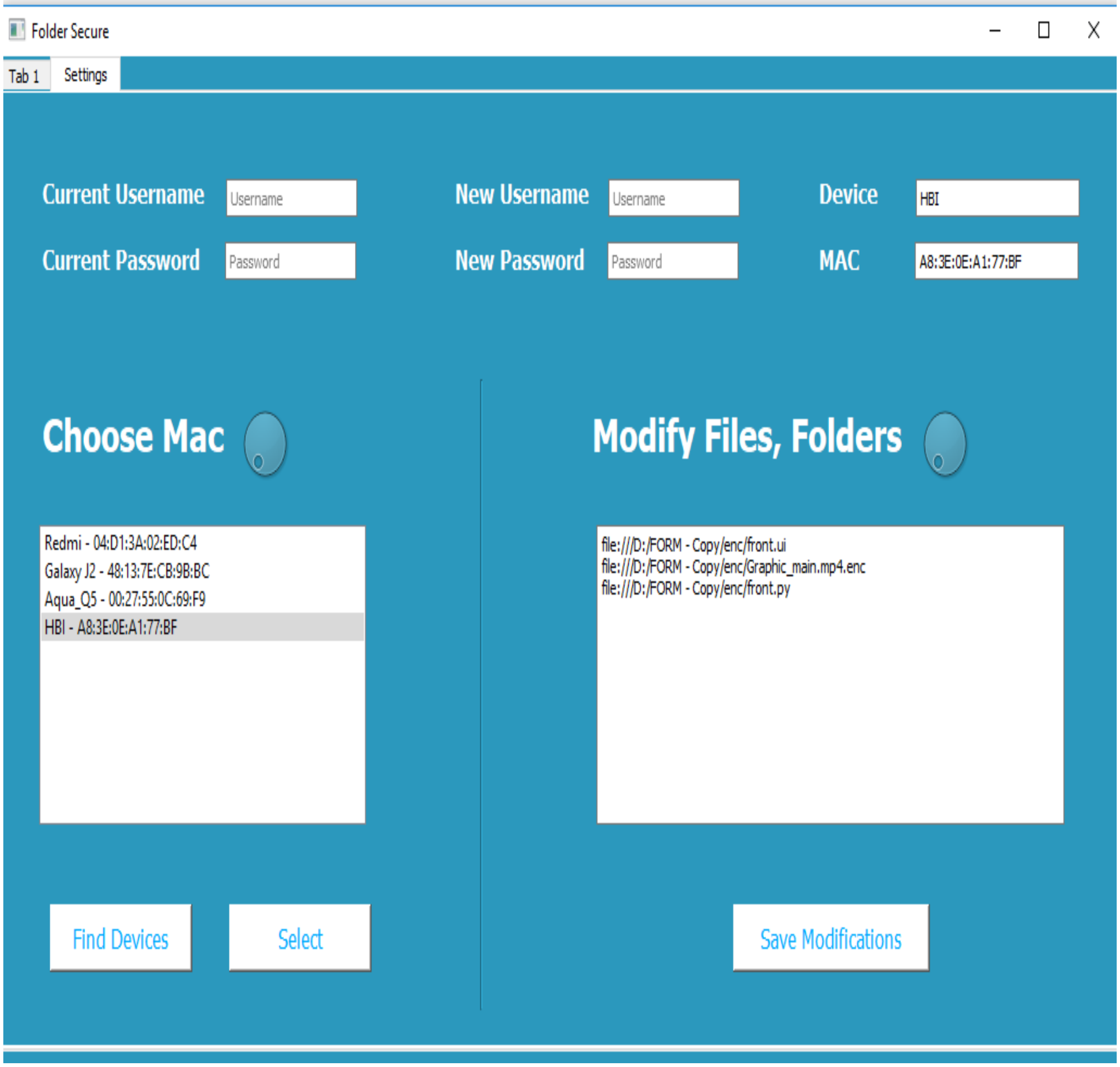
file:///D:/FORM - Copy/enc/front.ui
file:///D:/FORM - Copy/enc/Graphic_main.mp4.enc
file:///D:/FORM - Copy/enc/front.py

In this page , if we want to change our username or password then it also done with the help of this page. In this the mac address should be choosen by the user and then choose files or folders for encryption or decryption.

\

In “Modify Files, Folders” column wr also scroll the address of file or folder and then paste on this column. There is no restriction for writing the address of file or folders, scrolling of address must also done.

5.5 ENCRYPTION



Current Username: Username

Current Password: Password

New Username: Username

New Password: Password

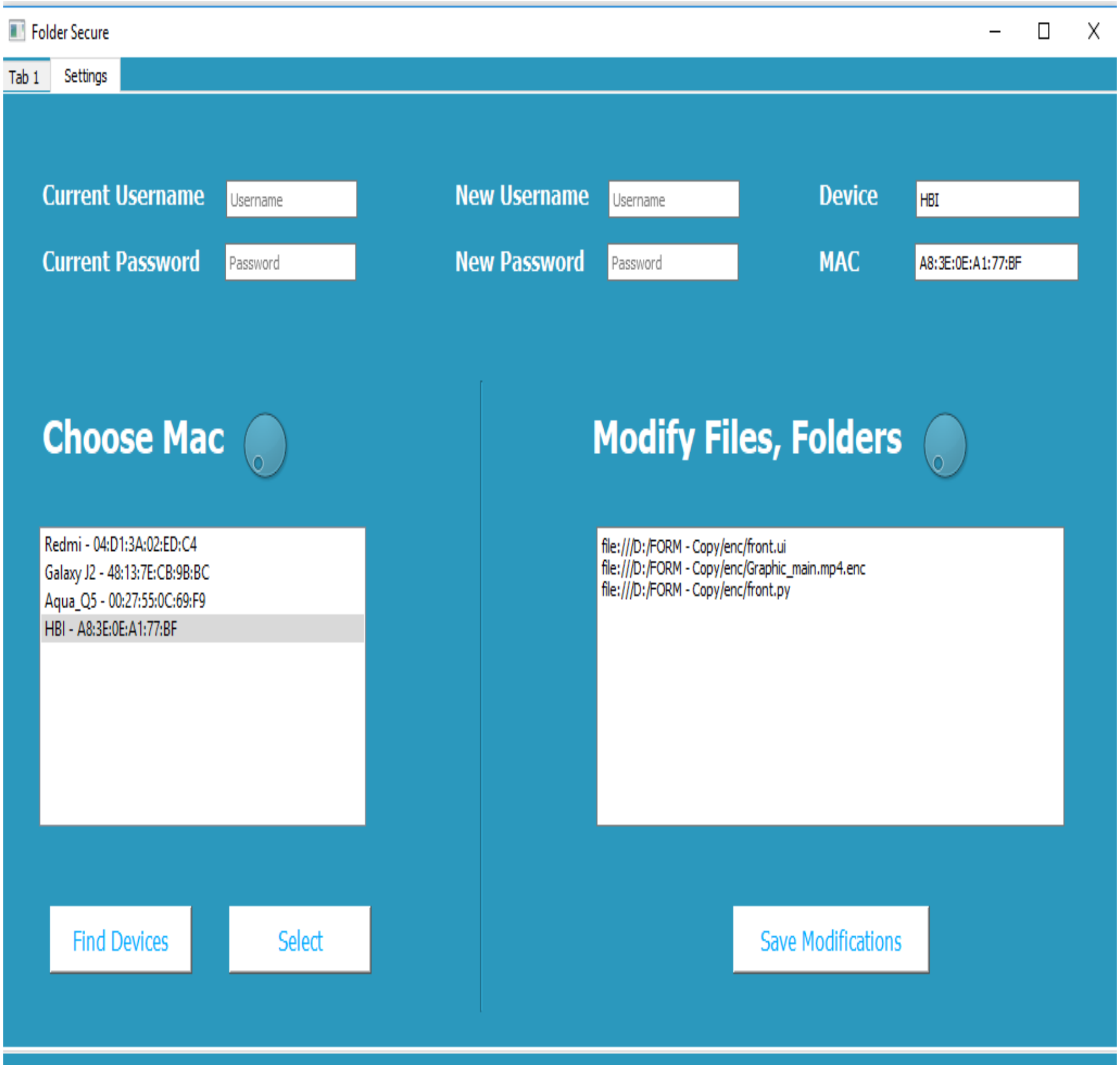
Device: HBI

MAC: A8:3E:0E:A1:77:BF

Redmi - 04:D1:3A:02:ED:C4
Galaxy J2 - 48:13:7E:CB:9B:BC
Aqua_Q5 - 00:27:55:0C:69:F9
HBI - A8:3E:0E:A1:77:BF

file:///D:/FORM - Copy/enc/front.ui
file:///D:/FORM - Copy/enc/Graphic_main.mp4.enc
file:///D:/FORM - Copy/enc/front.py

5.6 DECRYPTION



Current Username: Username
Current Password: Password
New Username: Username
New Password: Password
Device: HBI
MAC: A8:3E:0E:A1:77:BF

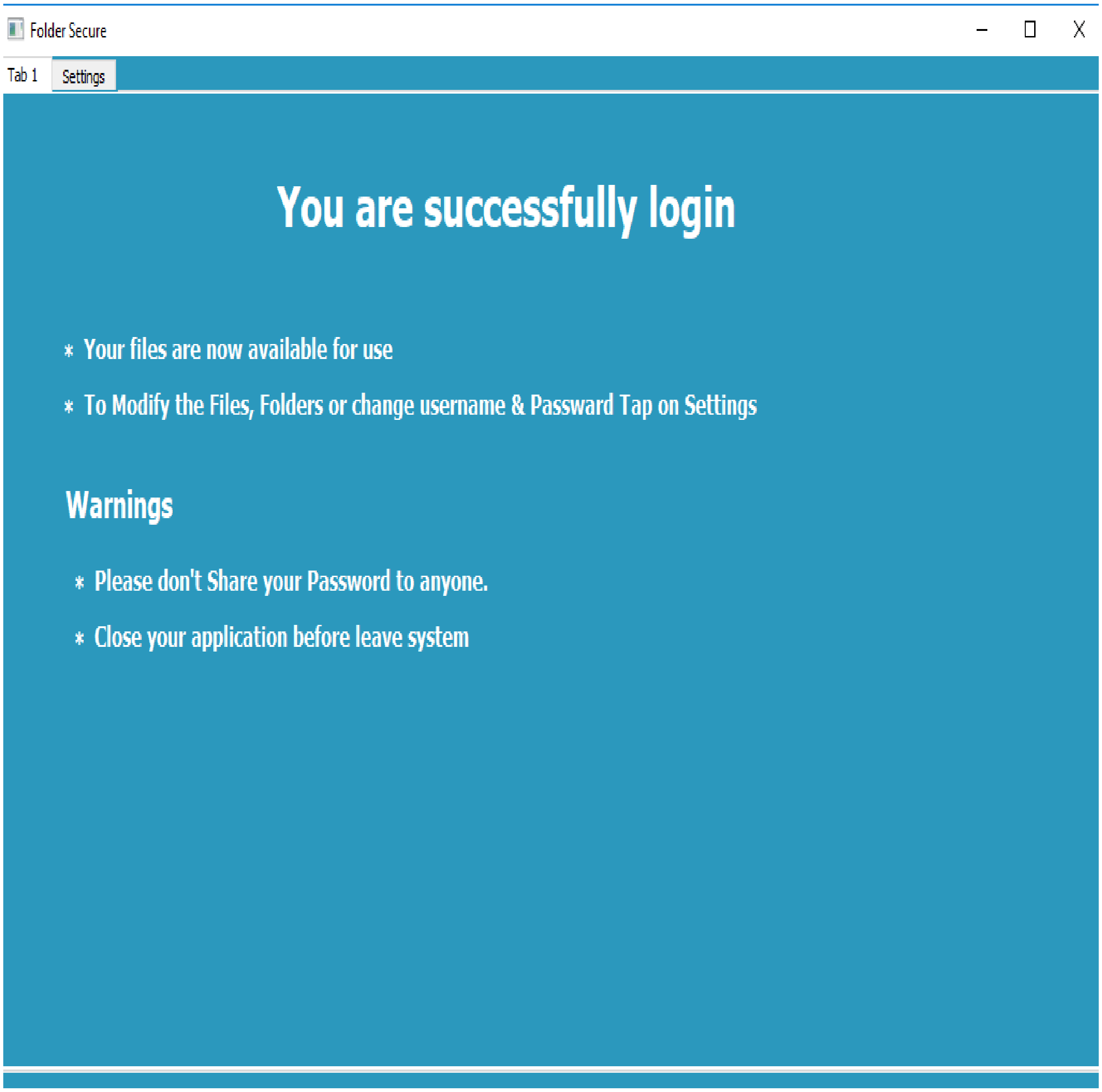
Redmi - 04:D1:3A:02:ED:C4
Galaxy J2 - 48:13:7E:CB:9B:BC
Aqua_Q5 - 00:27:55:0C:69:F9
HBI - A8:3E:0E:A1:77:BF

```
file:///D:/FORM - Copy/enc/front.ui
file:///D:/FORM - Copy/enc/Graphic_main.mp4.enc
file:///D:/FORM - Copy/enc/front.py
```

5.7 AUTHENTICATION

Valid

This is the page where all details are correct or matched with the sign up page. If user name, password, device name and mac address are correctly registered then user will successfully login.



You are successfully login

* Your files are now available for use
* To Modify the Files, Folders or change username & Passward Tap on Settings

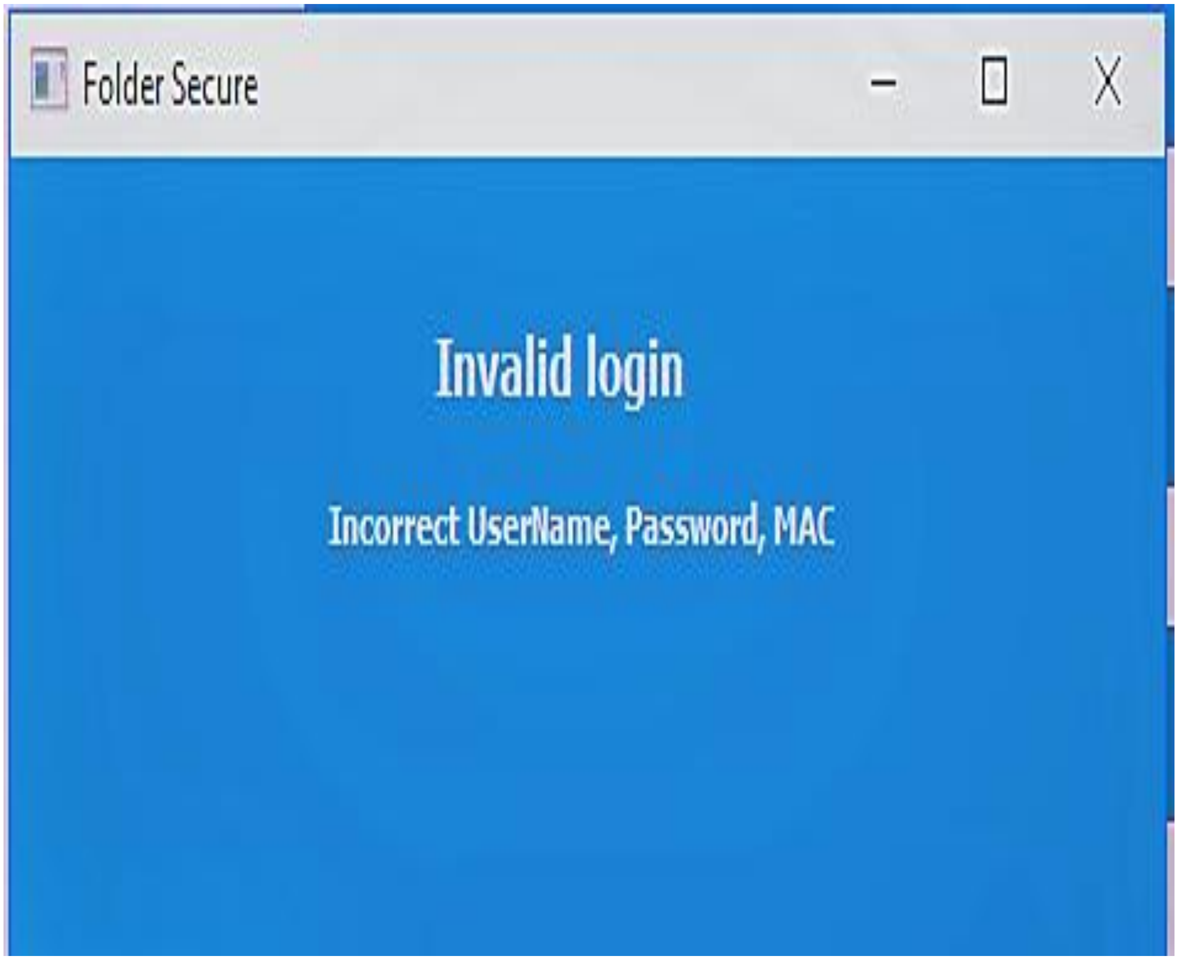
Warnings

* Please don't Share your Password to anyone.
* Close your application before leave system

If user successfully login then files or folders are available for encryption or decryption. For any modification in username or password go to setting option.

There are two warnings written in this page which should be kept in mind by the user for further encryption or decryption process.

Invalid



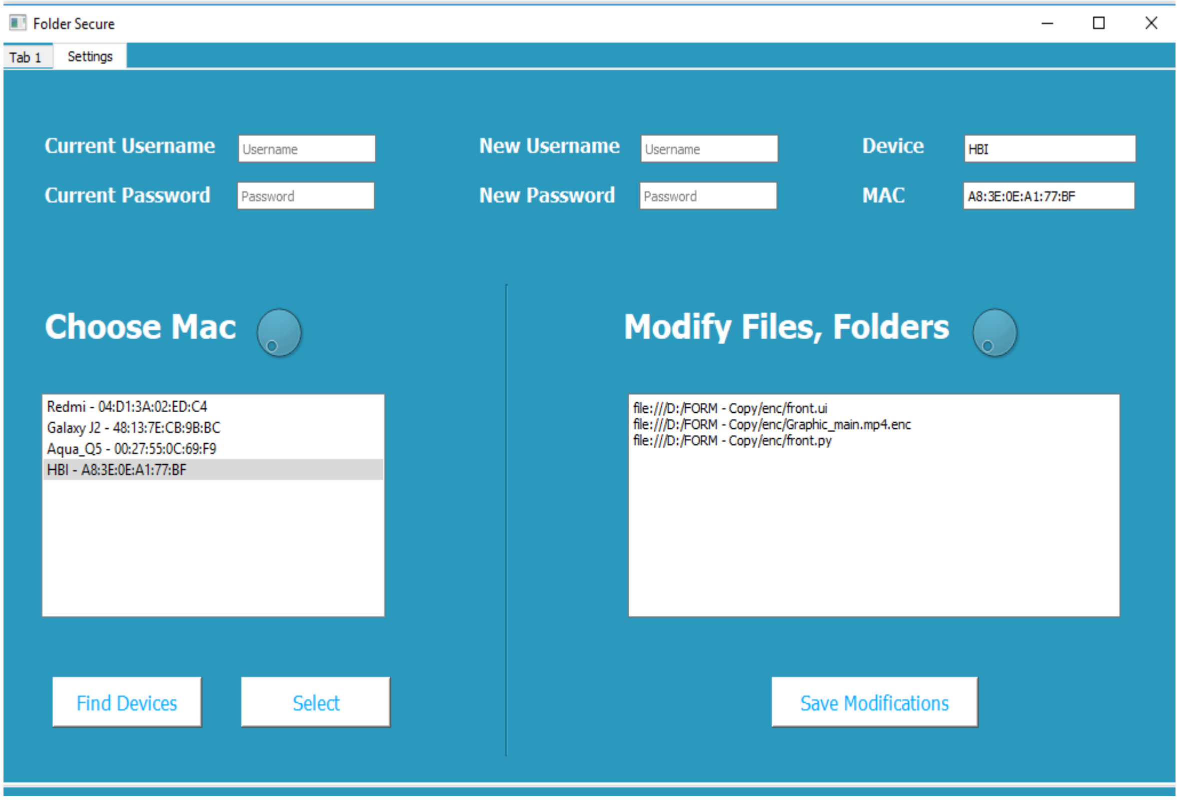
Invalid login

Incorrect UserName, Password, MAC

This is the invalid page. If the authentication of user is not correct then this page will appear in your screen.

Correct username, password, MAC address is compulsory otherwise invalid login will occur.

5.8 PROFILE



Current Username: Username
Current Password: Password
New Username: Username
New Password: Password
Device: HBI
MAC: A8:3E:0E:A1:77:BF

Redmi - 04:D1:3A:02:ED:C4
Galaxy J2 - 48:13:7E:CB:9B:BC
Aqua_Q5 - 00:27:55:0C:69:F9
HBI - A8:3E:0E:A1:77:BF

file:///D:/FORM - Copy/enc/front.ui
file:///D:/FORM - Copy/enc/Graphic_main.mp4.enc
file:///D:/FORM - Copy/enc/front.py

CHAPTER 6

EXPERIMENTAL SETUP AND RESULTS

Platform/Language:

- Python
- PyQT5
- SQL
- PyBluez

Hardware Requirements:

- For laptop:

  - 512MB RAM
  - Bluetooth inbuilt Device

- For Mobile:

  - Minimum Android Version required is above 4.4(KitKat)
  - 512MB Ram

Software Requirements:

- Bluetooth

CHAPTER 7

ADVANTAGES & DISADVANTAGES

7.1 ADVANTAGES

- Rijndael Algorithm, A Cryptographic Algorithm, is widely conceived as one of the best algorithms for encryption. Efficient implementation of the algorithm is due to the chasteness of its design which makes the effectuation easy to understand.
- It also facilitates understanding the mechanisms that give the algorithm its high resistance against differential cryptanalysis and linear cryptanalysis, to date the most important general methods of cryptanalysis in symmetric cryptography".
- Two way authentication is provided by us i.e, Bluetooth & MAC address which is must better than a password.

7.2 DISADVANTAGES

- If Bluetooth is off in between the process then whole process is halted until Bluetooth device will on.
- For implementing Rijndael algorithm, its very time consuming.
- A Handshake protocol is implemented by the program every 5 seconds so that whenever the authenticated Bluetooth device moves away from the PC, all the working files and folders are encrypted and account is logged off.

CHAPTER 8

FUTURE SCOPE

- Decreasing the execution time of programs.
- Installing Bluetooth module in a wearable technology and using it as a reference check for connectivity.
- This technology can be extended for securing other computing devices such as computerized locks in cars, house, offices, etc.

CHAPTER 9

CONCLUSION

This application program would ensure user authentication by the windows password login further authentication to most private files employing their Bluetooth enabled mobile phones..By using this method we can secure our computer devices and our vital data from being exposed easily. This can be additional security mechanism to our normal windows authentication process. Using this technology also does not cost any extra cost to the user. Also this proposed solution overcomes the disadvantages of other solutions proposed by others till now. So in a way it has been noted that the system has simplified the daily work lives of several people due to its simplicity and automated protection mechanism. It is therefore safe to say the system is indeed effective in protecting files and also in improving password policies.

CHAPTER 10

REFERENCES

1. https://www.academia.edu/32942779/Securing_Computer_Folders_using_Bluetooth_and_Rijndael_Encryption
2. http://inpressco.com/wp-content/uploads/2015/02/Paper71397-400.pdf
3. http://inpressco.com/category/ijcet
4. www.aircccj.org/cscp/volume2/csit2417.pdf
5. https://iarjset.com/upload/2015/february-15/IARJSET4.pdf
6. https://ijireeice.com/upload/2017/july-17/IJIREEICE%202.pdf
7. https://www.engpaper.com/aes-2017.html
8. https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data