File security in personal computer

**MEMBERS**

2014103558-**Sandhya.A.K**

sandhyaa0207@gmail.com, 9486960291

2014103557-**Sachin Kumar.S**

sachinsundar1152@gmail.com, 8939202465

2014103621-**Priyavarshini.M**

pvshini1599@gmail.com, 9894642863

**MENTOR:**Dr AROCKIA XAVIER ANNIE R

TABLE OF CONTENTS

**Chapter No. title Page No.**

ABSTRACT 5

**1 INTRODUCTION** 6

1.1 OVERVIEW 6

1.2 LITERATURE SURVEY 6

1.3 ORGANISATION OF CHAPTERS 9

**2 REQUIREMENT SPECIFICATION 10**

2.1 INTRODUCTION

2.1.1 Purpose 10

2.1.2 Scope 10

2.1.3 Glossary 10

2.2 PRODUCT DESCRIPTION

2.2.1 System Environment 11

2.2.2 Functions 12

2.2.3 Operating Environment 12

2.2.4 Design and Implementation Constraints 13

2.2.5 Assumptions and Dependencies 13

* 1. EXTERNAL INTERFACE REQUIREMENTS
     1. User Interface 13
     2. Hardware Interface 13
     3. Software Interface 13

2.4 NON FUNCTIONAL REQUIREMENTS

* + 1. Performance Requirement 14
    2. Safety Requirement 14
    3. Security Requirement 14
    4. Software Quality Attributes 14

**3 TECHNOLOGY**

3.1 C#

3.1.1 C# Programming Language 16

3.1.2 Features of C# 17

3.1.3 The .net framework 17

3.1.4 IDE for C# 18

3.2 Android code (java)

3.2.1Android SDK 19

3.2.2 Android debug bridge 20

3.3 My SQL

3.3.1 Features 21

3.4 Algorithms

3.4.1Rijndael 22

3.4.2 MD5 23

**4 SYSTEM DESIGN**

4.1 DETAILED SYSTEM ARCHITECTURE 26

4.2 MODULES DECOMPOSITION 28

4.2.1 Smart phone UI

M 1.1 Entry page 28

M 1.2 Register page 28

M 1.3 Login page 29

M 1.4 Delete account page 29

4.2.2 Personal computer UI

M 2.1 Home page 30

M 2.2 Main page 30

M2.3 31

4.3 Performance Evaluation

4.3.1.Results 31

4.3.2 Analysis and Discussion 31

**5 IMPLEMENTATIONAND TEST RESULTS**

5.1 SNAPSHOTS 32

5.2 TEST CASES 38

5.3 TEST RESULTS 41

**6 CONCLUSION AND FUTURE WORK** 43

APPENDIX a: pROJECT CLOSE-OUT APPROVAL 44

APPENDIX B: REFERENCES 45

APPENDIX C: KEY TERMS 47

**ABSTRACT**

There are possibilities that most important details in files may be hacked and can be used without proper authentication from the file owner. This may lead to malicious attack of files from the system and there are chances that they can be used inappropriately. Thus our project deals with implementation of security for files in pc using an application that is present in both the personal computer of the user and the user’s android mobile and hence enhancing security by establishing communication between the computer and the mobile phone. Thus the file systems and folders can be accessed only if both the gateways present in android mobile and the laptop provides authentication.

**CHAPTER 1**

**INTRODUCTION**

* 1. **OVERVIEW**

The project File-security in personal computer deals with securing all the files in one’s personal computer with the help of his / her android mobile phone. Thus the file security is implemented as an application that has its working in both user’s android mobile and personal computer or laptop. This enables different levels of security and at most basic level ensures that the files that are stored in this application is accessed only when the android application allows access to enter the application. The application splits the passcode into two halves and stores it in the database. The first half of the passcode is entered in the android application and validated against the database. This paves the way to scan the QR code that is generated in the windows application. Once the QR code is scanned it is cross checked and validated. For a particular user his Laptop’s MAC address is stored as a string to be generated as a QR code. Then the second half of the passcode is validated and this gives the way for the user to access his valuable files.

* 1. **LITERATURE SURVEY**

1.“BLUETOOTH ENABLED MOBILE PHONE REMOTE CONTROL FOR PC”

**Authors:**

Qadeer, M.A. ,Agrawal, R. ,Singhal A. and Umar. S

**Topic:**

International conferences on Advanced Computer Control, 2008.IEEE DOI 10.1109/ ICACC .2009.91

**Concept:**

This work confers an application which makes possible to use a Bluetooth enabled mobile phone to remote control home appliances that are connected to the PC as well as other computer applications. The datasets used are Bluetooth, mobile phones, home networking, PAN, wireless networks, J2ME, Java. In this the time for searching the device can be eradicated if the same PC

is used again and again by storing the serial port service URL and using it directly to open connection. Also by this the Bluetooth enabled mobile devices can be used to control home appliances as well.

2.“POCKETDROID-A PC REMOTE CONTROL”

**Authors:**

ChaitaliNavasare, DeepaNagdev

**Topic:**

International Conference on Information and Network Technology ,2012 vol. 37.

**Concept:**

The user can connect to any computer having Server Application running on it. It is basically an Android based Mobile Application for controlling a Target PC. User can have full access of the Target PC, provided its IP address is known. The datasets here are Android, IP address, JAVA, Linux OS, pervasive computing, remote desktop, remote visualization, smart phone, wireless handheld devices. It involves running of basic Linux or Windows Commands via android application. It provides a mechanism for graphically interacting with files and folders of target PC. It allows user to troubleshoot and solve problems faster in remote pc and Remote virtualization.

3.“SESSION KEY EXCHANGE AND MUTUAL AUTHENTICATION SCHEME BETWEEN MOBILE MACHINES IN WLAN BASED AD HOC NETWORKS”

**Authors:**

HyosunRoh, Souhwonjung - School of Electronic Engineering, Soongsil University, Korea.

**Topic:**

PUBLISHED IN: International Conference on Information and Communication Technology Convergence (ICTC).

DATE OF CONFERENCE: 17-19 Nov. 2010

**Concept:**

The main idea of this paper is that non-interactive session key exchange uses the mobile machine's ID and mutual authentication without communication with an authentication server whenever a data transmission occurs between the mobile machines. The datasets used here are Authentication, Mobile Communication, Servers ,Delays , Ad hoc networks ,Message authentication. The proposed scheme is secure against man-in-the-middle attack, impersonation attack, and modification attack.

4.“ AN ENHANCED REMOTE MUTUAL AUTHENTICATION SCHEME USING SMART CARDS ”

**Authors:**

JieGu ,ZhiXue , Yan Zhu , Fangbiao Li , Xiao Chen

**Topic:**

CONFERENCE: symposium on ICT and energy efficiency and workshop on information theory and security(CIICT 2012)

ISBN: 978-1-84919-547-8

Location: Dublin, Ireland

Conference date:4-5 July 2012.

Publisher:IET.

**Concept:**

Mutual authentication is a process or technology in which both entities in a communications link authenticate each other before conducting any business. This can help in eliminating password hacking. The datasets here are Mutual authentication ,Smart cards ,Security , Cryptanalysis. It is gaining acceptance as a tool that can minimize the risk of online fraud in e-commerce and other network application. The scheme can withstand guessing attack, forgery attack, denial of service attack and is easily realized in the practical resource-limited environment.

5. “MOBILE ENCRYPTION FOR LAPTOP DATA PROTECTION”

**Authors:**

*Y.-W*. *Kao*, X. Zhang, A. Studer, A. Perrig

**Topic:**

PUBLISHED IN:Volume 6, Issue 4, 2012 ,

pg. 291 – 298

PUBLISHER: IET

**Concepts:**

If a laptop is stolen, the data stored on it is easily leaked; which may cause serious consequences. Encrypting files by encryption keys is a general solution; however, if the decryption keys are also stored on laptops, the files can also be decrypted by adversaries easily. To solve this problem, this paper proposes the Mobile Encryption for Laptop data Protection (MELP) system. Datasets are Public and Private key cryptography , Mobile computing. Use of encryption and decryption for securing the files in pc rather than using passkey. In addition of a simple password, this method adds further security to the system are the advantages of this system.

* 1. ORGANISATION OF CHAPTERS:

This project is done in two parts as is mentioned before. The two parts are organized in various different chapters that is correspondingly in the windows side and the android mobile side. So the whole project is explained in detail based on the following organization of chapters.

Chapter 2- Requirement specifications

Chapter 3-Technology that is used in the project

Chapter 4-System design of the project

Chapter5-Implementation of the projects and its test results

Chapter6-Conclusion and future scope

CHAPTER 2

REQUIREMENT SPECIFICATION

2.1 INTRODUCTION:

**2.1.1 PURPOSE**

The main purpose of the project is to enhance file security in pc/laptop. If a laptop is stolen then the level of security should be such that the files and folders are not

accessed by the hackers in any case. This is because every laptop is tied to a unique mobile for accessing the files and folders and hence the files cannot be accessed without the android phone. This application, which is both a blend of windows application and android application implements multiple levels of security providing at most safe ensuring of users files.

**2.1.2 SCOPE**

The scope of this project is that any user can put his / her fullest trust in this application that can be used to secure the user’s files. It can be used in any educational institutions and other organizations where there is a need to secure the file systems in a much more organized and trusted way.

**2.1.3 GLOSSARY**

Authentication-the process or action of verifying the identity of a user or process

Passcode- a string of characters used as a password, especially to gain access to a computer or smartphone

QR code-a machine-readable code consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smartphone

Encryption-the process of converting information or data into a code, especially to prevent unauthorized access

Hiding-A hidden file is any file with the hidden attribute turned on. Just as you'd expect, afile or folder with this attribute toggled on is invisible while browsing through folders - you can't see any of them without explicitly allowing all of them to be seen

**2.2 PRODUCT DESCRIPTION**

**2.2.1 SYSTEM ENVIRONMENT**

This project is done in two environments: Android studio and Microsoft’s visual studio.

Android Studio is the official [integrated development environment](https://en.wikipedia.org/wiki/Integrated_development_environment) (IDE) for the [Android](https://en.wikipedia.org/wiki/Android_(operating_system)) platform.It is a gradle-based build support .Android studio is based on Android-specific [refactoring](https://en.wikipedia.org/wiki/Code_refactoring) and quick fixes. It actually [Lint](https://en.wikipedia.org/wiki/Lint_(software)) tools to catch performance, usability, version compatibility and other problems. Android studio has built in [Pro-Guard](https://en.wikipedia.org/wiki/ProGuard_(software)) integration and app-signing capabilities. It has Template-based wizards to create common Android designs and components. Android Studio has rich [layout editor](https://en.wikipedia.org/wiki/Graphical_user_interface_builder) that allows users to drag-and-drop UI components, option to [preview layouts](https://en.wikipedia.org/wiki/WYSIWYG) on multiple screen configurations. It also supports for building [Android Wear](https://en.wikipedia.org/wiki/Android_Wear) apps. It has Built-in support for Google Cloud Platform, enabling integration with Google Cloud Messaging and App Engine. It is an Android Virtual Device that is used to run and debug apps.

Microsoft Visual Studio is an [integrated development environment](https://en.wikipedia.org/wiki/Integrated_development_environment) (IDE) from [Microsoft](https://en.wikipedia.org/wiki/Microsoft). It is used to develop [computer programs](https://en.wikipedia.org/wiki/Computer_program) for [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows), as well as [web sites](https://en.wikipedia.org/wiki/Web_site), [web apps](https://en.wikipedia.org/wiki/Web_app), [web services](https://en.wikipedia.org/wiki/Web_service) and [mobile apps](https://en.wikipedia.org/wiki/Mobile_app). Visual Studio uses Microsoft software development platforms such as [Windows API](https://en.wikipedia.org/wiki/Windows_API), [Windows Forms](https://en.wikipedia.org/wiki/Windows_Forms), [Windows Presentation Foundation](https://en.wikipedia.org/wiki/Windows_Presentation_Foundation), [Windows Store](https://en.wikipedia.org/wiki/Windows_Store) and [Microsoft Silverlight](https://en.wikipedia.org/wiki/Microsoft_Silverlight). It can produce both [native code](https://en.wikipedia.org/wiki/Native_code) and [managed code](https://en.wikipedia.org/wiki/Managed_code).

Visual Studio includes a [code editor](https://en.wikipedia.org/wiki/Code_editor) supporting [IntelliSense](https://en.wikipedia.org/wiki/IntelliSense) (the [code completion](https://en.wikipedia.org/wiki/Code_completion) component) as well as [code refactoring](https://en.wikipedia.org/wiki/Code_refactoring). [The integrated debugger](https://en.wikipedia.org/wiki/Microsoft_Visual_Studio_Debugger) works both as a source-level debugger and a machine-level debugger. Other built-in tools include a forms designer for building [GUI](https://en.wikipedia.org/wiki/GUI) applications, [web designer](https://en.wikipedia.org/wiki/Web_designer), [class](https://en.wikipedia.org/wiki/Class_(computing)) designer, and [database schema](https://en.wikipedia.org/wiki/Database_schema) designer. It accepts plug-ins that enhance the functionality at almost every level—including adding support for [source control](https://en.wikipedia.org/wiki/Source_control) systems (like [Subversion](https://en.wikipedia.org/wiki/Subversion_(software))) and adding new toolsets like editors and visual designers for [domain-specific languages](https://en.wikipedia.org/wiki/Domain-specific_language) or toolsets for other aspects of the [software development lifecycle](https://en.wikipedia.org/wiki/Software_development_lifecycle) (like the [Team Foundation Server](https://en.wikipedia.org/wiki/Team_Foundation_Server) client: Team Explorer).

Visual Studio supports different [programming languages](https://en.wikipedia.org/wiki/Programming_language) and allows the code editor and debugger to support (to varying degrees) nearly any programming

language, provided a language-specific service exists. Built-in languages include [C](https://en.wikipedia.org/wiki/C_(programming_language)), [C++](https://en.wikipedia.org/wiki/C%2B%2B) and [C++/CLI](https://en.wikipedia.org/wiki/C%2B%2B/CLI) (via [Visual C++](https://en.wikipedia.org/wiki/Visual_C%2B%2B)), [VB.NET](https://en.wikipedia.org/wiki/VB.NET) (via [Visual Basic .NET](https://en.wikipedia.org/wiki/Visual_Basic_.NET)), [C#](https://en.wikipedia.org/wiki/C_Sharp_(programming_language)) (via [Visual C#](https://en.wikipedia.org/wiki/Visual_C_Sharp)), and [F#](https://en.wikipedia.org/wiki/F_Sharp_(programming_language)) (as of Visual Studio 2010). Support for other languages such as [Python](https://en.wikipedia.org/wiki/Python_(programming_language)), [Ruby](https://en.wikipedia.org/wiki/Ruby_(programming_language)), [Node.js](https://en.wikipedia.org/wiki/Node.js), and [M](https://en.wikipedia.org/wiki/MUMPS) among others is available via language services installed separately.

It also supports [XML](https://en.wikipedia.org/wiki/XML)/[XSLT](https://en.wikipedia.org/wiki/XSLT), [HTML](https://en.wikipedia.org/wiki/HTML)/[XHTML](https://en.wikipedia.org/wiki/XHTML), [JavaScript](https://en.wikipedia.org/wiki/JavaScript) and [CSS](https://en.wikipedia.org/wiki/Cascading_Style_Sheets). Java (and J#) were supported in the past.

**2.2.2 FUNCTIONS**

This project has multiple functions.The basic functionality includes login and registration in both android phone and user’s laptop/pc. While registering the application sets a unique phone number with a unique laptop (by identifying its mac address) pair such that one laptop’s app can only be opened using onephone only. The next functions are to set the passcode and in the backend the passcode is divided into two by its length and stored in DB. Then comes the QR code generation part in the windows laptop and QR code scanning part in the android part. The functions in the laptop includes viewing the files or protecting the files. Viewing incorporates the functions of just displaying the folder where the user wished to save the encrypted files. Protecting has the functions of creating a folder of user’s wish to save the files, encrypting the files that are to be saved in that folder and finally hiding the files in their original location. All the passwords and passcodes used in this application are encrypted and saved in the backend using MD5 encryption algorithm.

**2.2.3 OPERATING ENVIRONMENT**

The operating environment of the project is any android platforms like Ice cream sandwich, Jellybean, Marsh mellow and Windows operating system(8.1,8,10)for the Laptop or personal computer side.

**2.2.4 DESIGN AND IMPLEMENTATION CONSTRAINTS:**

As for the design side the constraints for this application are, it can be developed only in the latest versions of Android Studio IDE and Microsoft Visual Basic IDE. When it comes for the implementation part it can be downloaded and implemented in any latest versions of android platforms and in the windows operating system of the Laptop. It cannot be run in the MAC operating system or Linux operating system in the Laptop side.

**2.2.5 ASSUMPTIONS AND DEPENDENCIES**

This project asks a few basic set of personal questions to the user at the time of registration for the first time. These questions are asked at the time of change is either passcode or password or in the case of resetting of password when the user forgets it. So it is assumed that the user provides a valid set of personal questions and remembers the answers for those questions. The dependency is that the android phone should have the ability to scan the QR code which is generated in the windows laptop.

* 1. **EXTERNAL INTERFACE REQUIREMENTS**

**2.3.1 USER INTERFACE**

The user interface is the operating system of the android application and the windows Laptop. Thus it can be any latest version of the android platforms and Microsoft windows (8,8.1,10).

**2.3.2 SOFTWARE INTERFACE**

* Android
* Microsoft Visual studio
* Xampp Control Panel

**2.3.3 HARDWARE INTERACE**

* The Android Phone of the user with built in camera to scan the QR code.
* The windows laptop of the user.

**2.4 NON FUNCTIONAL REQUIREMENTS**

**2.4.1 PERFORMANCE REQUIREMENT**

The application’s performance is mainly based on the performance of the user’s phone and the laptop.

* Response Time:

The scanning process should be done easily so that in no time the user can get access for the application in the laptop. Also the time taken for establishing connection with the database for password verifications must take minimal amount of time for better performance.

* Workload:

Simultaneous requests to the database must be handled efficiently. Inconsistency must be avoided while concurrent access to the database.

* Degree of Precision:

The QR code scanning is done with utmost accuracy to enable efficient acknowledgement being recognized by the personal computer.

**2.4.2 SAFETYAND SECURITY REQUIREMENT**

* Since the main idea behind this project is to protect the files in the personal computer, the application itself must be protected from being damaged.
* The database where the user details are stored must be protected well against possible attacks.
* The protected files and folders must also be protected against any damage.

**2.4.3 SOFTWARE QUALITY ATTRIBUTES**

**S**ecurity, Availability, Reusability, reliability and usability are the software quality attributes of this application.

* Reusability:

The modules used in this project can be reused or enhanced so that multiple levels of security can provided.

* User Qualities:

The user is guided through appropriate prompts while interacting with the system

* Supportability:

The system raises appropriate exceptions and error information in case of any failure in the application at any point of time.

* Reliability:

The system provides more reliability by providing multiple levels of security.

**CHAPTER 3**

**TECHNOLOGY**

This section focuses on technologies used in PC interface and mobile interface.

**3.1 C#**

C# is a multi paradigm programming language encompassing strong typing, imperative, declarative, functional, generic, object oriented(class based), and component oriented programming disciplines. It was developed by Microsoft within .NET initiative and later approved as a standard ECMA( ECMA-334) and ISO (ISO/IEC 23270:2006$). C# is one of the programming languages designed for the Common Language Infrastructure.

**3.1.1 C# PROGRAMMING LANGUAGE**

C# is a modern, general-purpose, object-oriented programming language developed by Microsoft and approved by European Computer Manufacturers Association (ECMA) and International Standards Organization (ISO).C# was developed by Anders Hejlsberg and his team during the development of .Net Framework.C# is designed for Common Language Infrastructure (CLI), which consists of the executable code and runtime environment that allows use of various high-level languages on different computer platforms and architectures.

The following reasons make C# a widely used professional language:

* It is a modern, general-purpose programming language
* It is object oriented.
* It is component oriented.
* It is easy to learn.
* It is a structured language.
* It produces efficient programs.
* It can be compiled on a variety of computer platforms.
* It is a part of .Net Framework.

C#, as part of the .NET framework, is compiled to Microsoft Intermediate Language (MSIL), which is a language similar to Java's bytecode. MSIL allows C# to be platform independent and runs using just in time compiling. Therefore programs running under .NET gain speed with repeated use. Furthermore, because the other languages that make up the .NET platform (including VB and Cobol) compile to MSIL, it is possible for classes to be inherited across languages. The MSIL, like bytecode, is what allows C# to be platform independent.The potential for C# is great if the .NET platform succeeds. C# is designed to take advantage of the design of .NET, and Microsoft has poured a great deal of money into .NET.

**3.1.2 FEATURES OF C#**

Although C# constructs closely follow traditional high-level languages, C and C++ and being an object-oriented programming language. It has strong resemblance with Java, it has numerous strong programming features that make it endearing to a number of programmers worldwide.

Following is the list of few important features of C#:

* Boolean Conditions
* Automatic Garbage Collection
* Standard Library
* Assembly Versioning
* Properties and Events
* Delegates and Events Management
* Easy-to-use Generics
* Indexers
* Conditional Compilation
* Simple Multithreading
* LINQ and Lambda Expressions
* Integration with Windows

**3.1.3 THE .NET FRAMEWORK:**

The .Net framework is a revolutionary platform that helps you to write the following types of applications:Windows applications, Web applications, Web services.

The .Net framework applications are multi-platform applications. The framework has been designed in such a way that it can be used from any of the following languages: C#, C++, Visual Basic, Jscript, COBOL, etc. All these languages can access the framework as well as communicate with each other.

The .Net framework consists of an enormous library of codes used by the client languages such as C#. Following are some of the components of the .Net framework:

* Common Language Runtime (CLR)
* The .Net Framework Class Library
* Common Language Specification
* Common Type System
* Metadata and Assemblies
* Windows Forms
* ASP.Net and ASP.Net AJAX
* ADO.Net
* Windows Workflow Foundation (WF)
* Windows Presentation Foundation
* Windows Communication Foundation (WCF)
* LINQ

**3.1.4 INTEGRATED DEVELOPMENT ENVIRONMENT(IDE) FOR C#**

Microsoft provides the following development tools for C# programming:

* Visual Studio 2015 (VS)
* Visual C# 2015 Express (VCE)
* Visual Web Developer

The last two are freely available from Microsoft official website. Using these tools, you can write all kinds of C# programs from simple command-line applications to more complex applications. You can also write C# source code files using a basic text editor, like Notepad, and compile the code into assemblies using the command-line compiler, which is again a part of the .NET Framework.

Visual C# Express and Visual Web Developer Express edition are trimmed down versions of Visual Studio and has the same appearance. They retain most features of Visual Studio. In this tutorial, we have used Visual C# 2015 Express.

**3.2 ANDROID CODE(JAVA)**

Android software development is the process by which new applications are created for the [Android operating system](https://en.wikipedia.org/wiki/Android_(operating_system)). Applications are usually developed in [Java](https://en.wikipedia.org/wiki/Java_(programming_language)) programming language using the Android [software development kit](https://en.wikipedia.org/wiki/Software_development_kit) (SDK), but other development environments are also available.

**3.2.1 ANDROID SDK**

The Android [software development kit](https://en.wikipedia.org/wiki/Software_development_kit) (SDK) includes a comprehensive set of development tools. These include a [debugger](https://en.wikipedia.org/wiki/Debugger), [libraries](https://en.wikipedia.org/wiki/Software_library), a handset [emulator](https://en.wikipedia.org/wiki/Emulator) based on [QEMU](https://en.wikipedia.org/wiki/QEMU), documentation, sample code, and tutorials. Currently supported development platforms include computers running [Linux](https://en.wikipedia.org/wiki/Linux_kernel) (any modern desktop [Linux distribution](https://en.wikipedia.org/wiki/List_of_Linux_distributions)), [Mac OS X](https://en.wikipedia.org/wiki/Mac_OS_X) 10.5.8 or later, and [Windows 7](https://en.wikipedia.org/wiki/Windows_7) or later. As of March 2015, the SDK is not available on Android itself, but software development is possible by using specialized Android applications.

Enhancements to Android's SDK go hand in hand with the overall Android platform development. The SDK also supports older versions of the Android platform in case developers wish to target their applications at older devices. Development tools are downloadable components, so after one has downloaded the

latest version and platform, older platforms and tools can also be downloaded for compatibility testing.

Android applications are packaged in [.apk](https://en.wikipedia.org/wiki/APK_(file_format)) format and stored under **data** folder on the Android OS (the folder is accessible only to the root user for security reasons). APK package contains .dex files (compiled byte code files called [Dalvik](https://en.wikipedia.org/wiki/Dalvik_Virtual_Machine) executables), resource files, etc.

#### 3.2.2. ANDROID DEBUG BRIDGE

The Android Debug Bridge (ADB) is a toolkit included in the Android SDK package. It consists of both client and server-side programs that communicate with one another. The ADB is

typically accessed through the [command-line interface](https://en.wikipedia.org/wiki/Command-line_interface),although numerous [graphical user interfaces](https://en.wikipedia.org/wiki/Graphical_user_interface) exist to control ADB.

In a security issue reported in March 2011, ADB was targeted as a vector to attempt to install a rootkit on connected phones using a "resource exhaustion attack".

**3.3 MY SQL**

MySQL is the most popular Open Source Relational SQL database management system. MySQL is one of the best RDBMS being used for developing web-based software applications.

MySQL is becoming so popular because of these following reasons:

* MySQL is an open-source database so you don't have to pay a single penny to use it.
* MySQL is a very powerful program so it can handle a large set of functionality of the most expensive and powerful database packages.
* MySQL is customizable because it is an open source database and the open-source GPL license facilitates programmers to modify the SQL software according to their own specific environment.
* MySQL is quicker than other databases so it can work well even with the large data set.
* MySQL supports many operating systems with many languages like PHP, PERL, C, C++, JAVA, etc.
* MySQL uses a standard form of the well-known SQL data language.
* MySQL is very friendly with PHP, the most popular language for web development.
* MySQL supports large databases, up to 50 million rows or more in a table. The default file size limit for a table is 4GB, but you can increase this (if your operating system can handle it) to a theoretical limit of 8 million terabytes (TB).

**3.3.1 FEATURES**

Major features as available in MySQL 5.6:

* A broad subset of [ANSI SQL 99](https://en.wikipedia.org/wiki/SQL:1999), as well as extensions
* Cross-platform support
* [Stored procedures](https://en.wikipedia.org/wiki/Stored_procedure), using a procedural language that closely adheres to [SQL/PSM](https://en.wikipedia.org/wiki/SQL/PSM)
* [Triggers](https://en.wikipedia.org/wiki/Database_trigger)
* [Cursors](https://en.wikipedia.org/wiki/Cursor_(databases))
* Updatable [views](https://en.wikipedia.org/wiki/View_(SQL))
* [Online DDL](https://en.wikipedia.org/wiki/Data_Definition_Language) when using the InnoDB Storage Engine.
* [Information schema](https://en.wikipedia.org/wiki/Information_schema)
* Performance Schema that collects and aggregates statistics about server execution and query performance for monitoring purposes.
* A set of SQL Mode options to control runtime behavior, including a strict mode to better adhere to SQL standards.
* [X/Open XA](https://en.wikipedia.org/wiki/X/Open_XA) [distributed transaction processing](https://en.wikipedia.org/wiki/Distributed_transaction_processing) (DTP) support; [two phase commit](https://en.wikipedia.org/wiki/Two-phase_commit_protocol) as part of this, using the default [InnoDB](https://en.wikipedia.org/wiki/InnoDB) storage engine
* Transactions with [savepoints](https://en.wikipedia.org/wiki/Savepoint) when using the default InnoDB Storage Engine. The NDB Cluster Storage Engine also supports transactions.
* [ACID](https://en.wikipedia.org/wiki/Atomicity,_consistency,_isolation,_durability) compliance when using InnoDB and NDB Cluster Storage Engines
* [SSL](https://en.wikipedia.org/wiki/Secure_Sockets_Layer) support
* Query [caching](https://en.wikipedia.org/wiki/Cache_(computing))
* Sub-[SELECTs](https://en.wikipedia.org/wiki/Select_(SQL)) (i.e. nested SELECTs)
* Built-in [replication](https://en.wikipedia.org/wiki/Database_replication) support (i.e., master-master replication and master-slave replication) with one master per slave, many slaves per master. [Multi-master replication](https://en.wikipedia.org/wiki/Multi-master_replication) is provided in [MySQL Cluster](https://en.wikipedia.org/wiki/MySQL_Cluster), and multi-master support can be added to unclustered configurations using Galera Cluster.
* Full-text [indexing](https://en.wikipedia.org/wiki/Index_(database)) and searching
* Embedded database library
* [Unicode](https://en.wikipedia.org/wiki/Unicode) support
* Partitioned tables with pruning of partitions in optimizer
* [Shared-nothing](https://en.wikipedia.org/wiki/Shared-nothing) clustering through [MySQL Cluster](https://en.wikipedia.org/wiki/MySQL_Cluster)
* Multiple storage engines, allowing one to choose the one that is most effective for each table in the application.
* Native storage engines [InnoDB](https://en.wikipedia.org/wiki/InnoDB), [MyISAM](https://en.wikipedia.org/wiki/MyISAM), Merge, Memory (heap), [Federated](https://en.wikipedia.org/wiki/MySQL_Federated), Archive, [CSV](https://en.wikipedia.org/wiki/Comma-separated_values), Blackhole, NDB Cluster.
* Commit grouping, gathering multiple transactions from multiple connections together to increase the number of commits per second.

**3.4 ALGORITHMS**

This section focuses on algorithms used in project

**3.4.1. RIJNDAEL**

# Rijndaelis the[algorithm](http://whatis.techtarget.com/definition/algorithm)that has been selected by the u.s. national institute of standards and technology as the candidate for the advanced encryption standard .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**](http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard)) - and later triple des - over the next few years in many[cryptography](http://searchsoftwarequality.techtarget.com/definition/cryptography)applications. the algorithm was designed by two belgian cryptologists, vincentrijmen and joandaemen, whose surnames are reflected in the cipher's name. Rijndael has its origins in square, an earlier collaboration between the two cryptologists. We use rijndael to encrypt and decrypt user’s confidential

# files. The rijndael encryption method is based on replacing, changing and performing xor operations on bytes.

#### The method looks like this:

* From the 128-bit key, Rijndael generates 10 keys of 128 bits each.
* These keys are placed into 4x4 arrays.
* The plain text is also divided into 4x4 arrays (128 bits each).
* Each of the 128-bit plain-text items is processed in 10 rounds (10 rounds for 128-bit-keys, 12 for 192, 14 for 256).
* After the 10th round the code is generated.
* Each single byte is substituted in an S box and replaced by the reciprocal on GF (2 8).
* Then a bit-wise modulo-2 matrix is applied, followed by an XOR operation with 63.
* The lines of the matrices are sorted cyclically.
* The columns of the matrix multiplication are interchanged on GF (2 8).
* The subkeys of each round are subjected to an XOR operation.

The security level of this encryption method increases if Rijndael is performed several times with different subkeys.

**Strengths of rijndael:**

Daemen and Rijmen have specified Rijndael's advantages based on implementation aspects, simplicity of design, variable block length and extensions. Rijndael's implementation is very flexible since it can be used with varying key sizes and block sizes. It is also possible to change the sequence of some steps in Rijndael without affecting the cipher. The cipher is has a simple and elegant structure. It does not hide its structure by using complex components. Instead, it benefits from the advantages gained by the use of simple components in a well defined structure. Rijndael's security is based on the interaction of the cipher's individual components.

Rijndael is described as having a 'rich algebraic structure' which allows the cipher's security to be easily assessed in a limited time frame. This is an advantage over more complex designs that require extensive thinking, searching and 'bit tracing'. Rijndael is consistently a very good performer in both hardware and software across a wide range of computing environments. Its key setup time is excellent, and its key agility is good. Rijndael's very low memory requirements make it very well suited for restricted-space environments. There is additional security in that Rijndael's operations are among the easiest to defend against power and timing attacks.

**3.4.2 MD5**

MD5 is an [algorithm](http://whatis.techtarget.com/definition/algorithm) that is used to verify [data integrity](http://searchdatacenter.techtarget.com/definition/integrity) through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. MD5, which was developed by Professor Ronald L. Rivest of MIT, is intended for use with [digital signature](http://searchsecurity.techtarget.com/definition/digital-signature) applications, which require that large files must be compressed by a secure method before being encrypted with a [secret key](http://searchsecurity.techtarget.com/definition/private-key), under a [public key](http://searchsecurity.techtarget.com/definition/public-key) cryptosystem. MD5 is currently a standard, Internet Engineering Task Force ([IETF](http://searchsoa.techtarget.com/definition/IETF)) Request for Comments ([RFC](http://whatis.techtarget.com/definition/Request-for-Comments-RFC)) 1321.

According to the standard, it is "computationally infeasible" that any two messages that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through apprehension of the message digest. MD5 is the third message digest algorithm created by Rivest. All three (the others are MD2 and MD4) have similar structures, but MD2 was optimized for 8-bit machines, in comparison with the two later formulas, which are optimized for 32-bit machines. The MD5 algorithm is an extension of MD4, which the critical review found to be fast, but possibly not absolutely secure. In comparison, MD5 is not quite as fast as the MD4 algorithm, but offers much more assurance of data security.We use MD5 to store password in database as encrypted form.

MD5 algorithm consists of 5 steps:

Step 1: Appending Padding Bits. The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. The padding rules are:

* The original message is always padded with one bit "1" first.
* Then zero or more bits "0" are padded to bring the length of the message up to 64 bits fewer than a multiple of 512.

Step 2: Appending Length. 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes. The rules of appending length are:

* The length of the original message in bytes is converted to its binary format of 64 bits. If overflow happens, only the low-order 64 bits are used.
* Break the 64-bit length into 2 words (32 bits each).
* The low-order word is appended first and followed by the high-order word.

Step 3: Initializing MD Buffer. MD5 algorithm requires a 128-bit buffer with a specific initial value. The rules of initializing buffer are:

* The buffer is divided into 4 words (32 bits each), named as A, B, C, and D.
* Word A is initialized to: 0x67452301.
* Word B is initialized to: 0xEFCDAB89.
* Word C is initialized to: 0x98BADCFE.
* Word D is initialized to: 0x10325476.

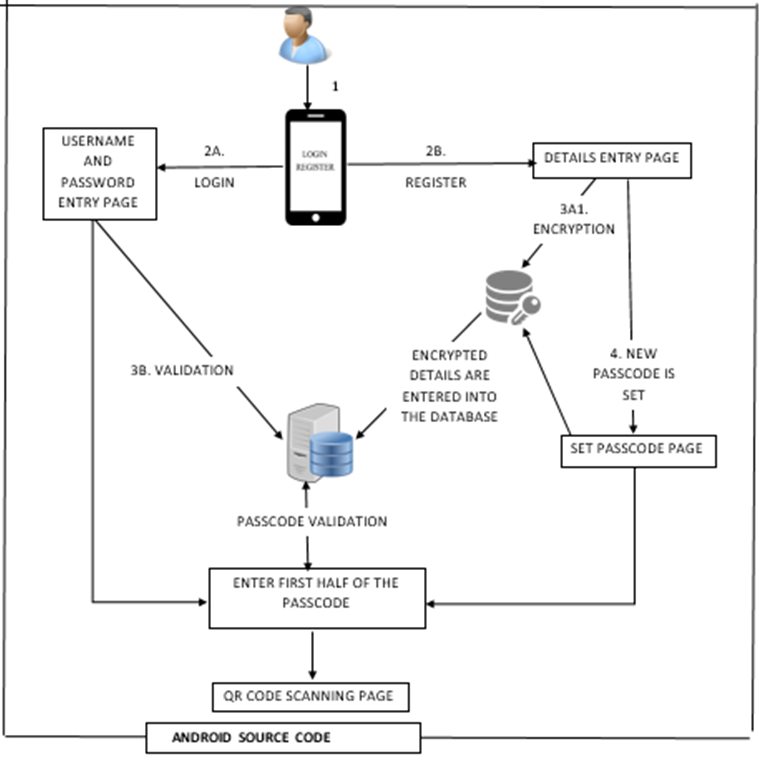
Step 4: Processing Message in 512-bit Blocks. This is the main step of MD 5 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, 4 rounds of operations are performed with 16 operations in each round. This step can be described in the following pseudo code slightly modified from the RFC 1321's version.

Step 5: Output. The contents in buffer words A, B, C, D are returned in sequence with low-order byte first.

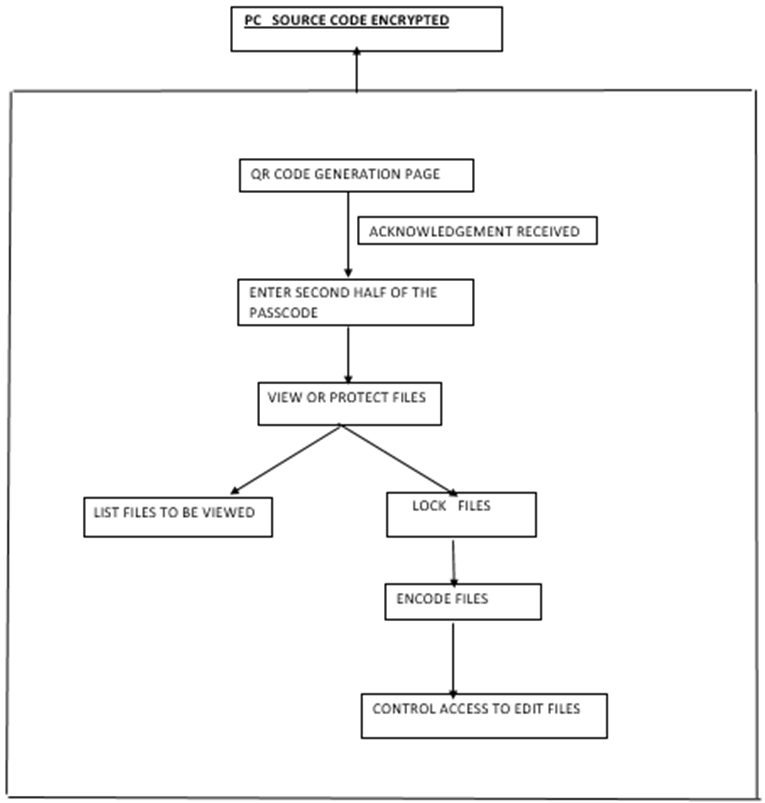
**CHAPTER 4**

**SYSTEM DESIGN**

**4.1 DETAILED SYSEM ARCHITECHTURE:**

****

**Fig 4.1 Android part**

****

**Fig 4.2 Windows Part**

**4.2 MODULES DECOMPOSITION**

**4.2.1 MODULE 1: SMART PHONE UI**

**M 1.1 : ENTRY PAGE**

* INPUT : User name and password entered by the user.
* OUPUT :

1) Register : Redirected to M 1.2

2) Login : Redirected to M 1.3

3) Delete: Redirected to M 1.4

* PROCESS : Validating and authenticating the user by comparing the input with the DB contents.
* ALGORITHM :

Login:

1.Enter username and password in Smartphone entry page.

2.if ((username && password)==valid)

3. Redirect to login page

4. else

Reenter username and password

Register:

Redirect to Register page.

**M 1.2 : REGISTER PAGE**

* INPUT : Pass code entered by the user.
* OUTPUT : Redirected to M 1.3
* PROCESS: The first half of the entered pass code is stored in one column and the other half in the other column
* ALGORITHM:

1.Set Passcode

2.Length=Strlen(passcode)

3.for(i=o to length/2)

Store in Column1;

for(Length/2 to length)

Store in column2;

4.Redirect to M1.3

**M 1.3 : LOGIN PAGE**

* INPUT : First half of the pass code
* OUTPUT: Alert message in the smart phone and acknowledgement is sent to the PC .
* PROCESS: Verifying the entered pass code with the DB contents
* ALGORITHM :

1.Enter Passcode1.

2.If(passcode1==Valid)

Do scanning process

Scan the QR code that is generated in pc by the smart phone.

Once correctly scanned change the acknowledgement message from 0 to 1 in the database

3.else

Reenter passcode1

**M 1.4 :DELETE ACCOUNT PAGE**

* INPUT : User name and password entered by the user.
* OUTPUT: Whether the account is successfully deleted or not.
* PROCESS: Verifying the entered username and password with the DB contents .
* ALGORITHM:

If entered Username and password are correct

Delete the account from the database.

**4.2.2 MODULE 2: PERSONAL COMPUTER UI  
M 2.1 : HOME PAGE**

* INPUT : 1)QR code is generated and waiting for ack to be received.

2) Second half of the pass code entered by the user .

* OUTPUT : Redirected to M 2.2
* PROCESS : Verifying the entered pass code with the DB contents .
* ALGORITHM:

After the acknowledgement is received from user's smart phone

do

1) Read the second half of the pass code from pc.

2) Check whether the entered pass code matches with the DB contents.

-yes ,leave the current module and redirect to M.2.2.

-else ,throw error message.

**M 2.2 : MAIN PAGE**

* CONTENT : List of all folders and files imported by the user. Two buttons –view files and protect files
* OPERATIONS :

1) The user can view the contents of the files and folders.

2) The page gets redirected to M 2.3 when the user tries to protect the file.

**M 2.3**

* INPUT : File to be protected
* OUTPUT : File contents encrypted and stored in the folder selected by the user and the original file is hidden in the location.
* PROCESS : Encryption and saving and hiding.
* ALGORITHM :

1) Encrypt using Rijndael algorithm.

2) Store the file in the folder selected by the user.

3)Hide the file from the original location.

**4.3 PERFORMANCE EVALUATION**

**4.3.1 RESULTS**

The end result of file security system is that the user can secure any file in his / her laptop in any folder according to his / her wish thus incorporating multiple levels of security so that it is very difficult for the hackers even to trace the location of the files. Thus this keeps the user’s files very secure.

**4.3.2 ANALYSIS AND DISCUSSIONS**

The analysis is that once a file is placed within a folder in this application the folder is locked and then even the user can access the file using his smart phone by carrying out the procedure from the start. So accessing a file in the Laptop becomes a level of difficulty for laptop hackers because every laptop is tied to an unique mobile number and every laptop( identified by the MAC address ) is tied to a phone number.

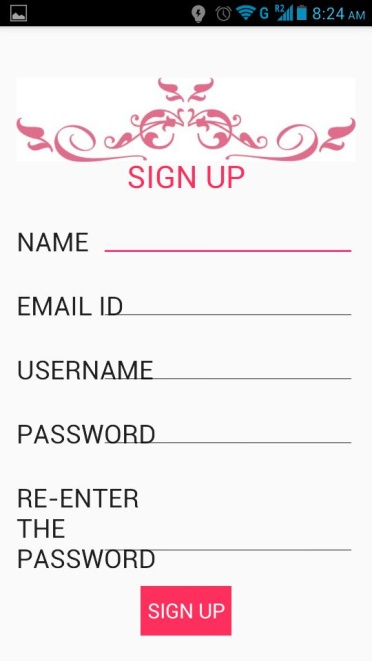
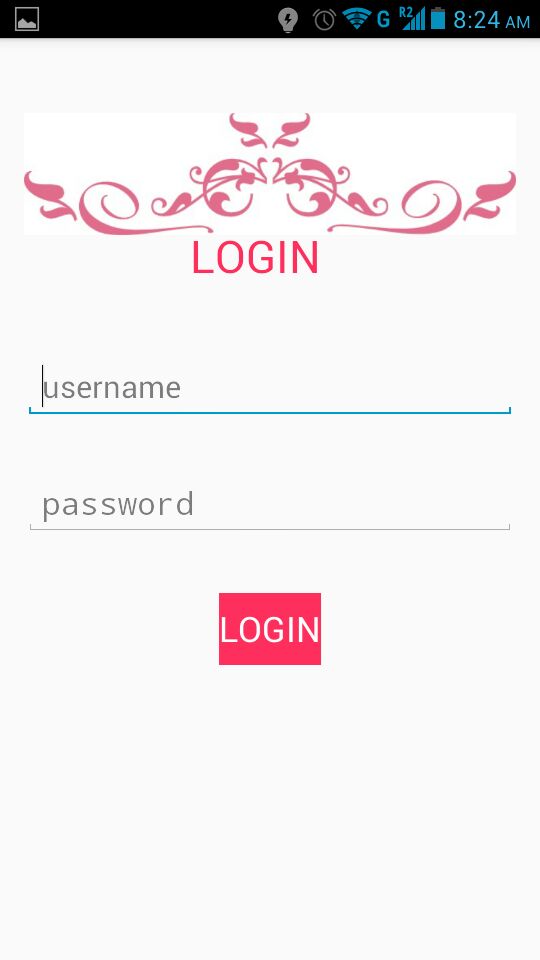
.

**CHAPTER 5**

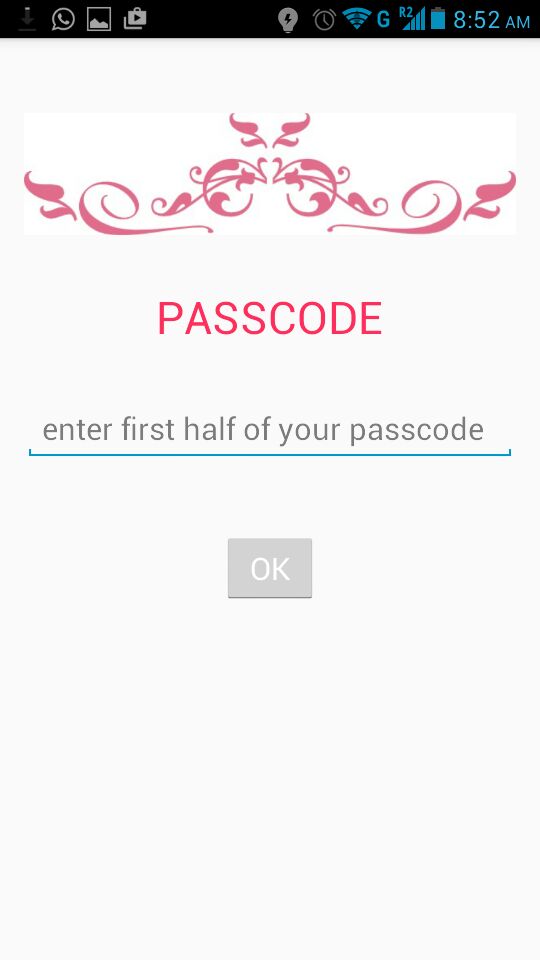
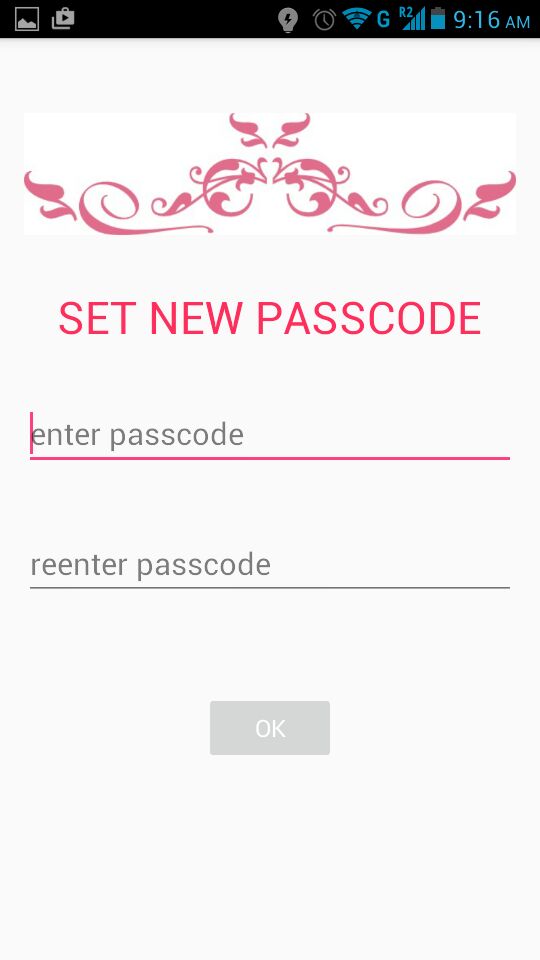
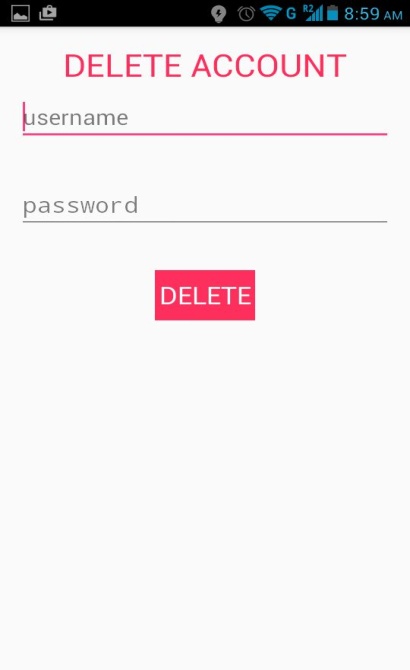
**IMPLEMENTATION AND TEST RESULTS**

**5.1 SNAPSHOTS**

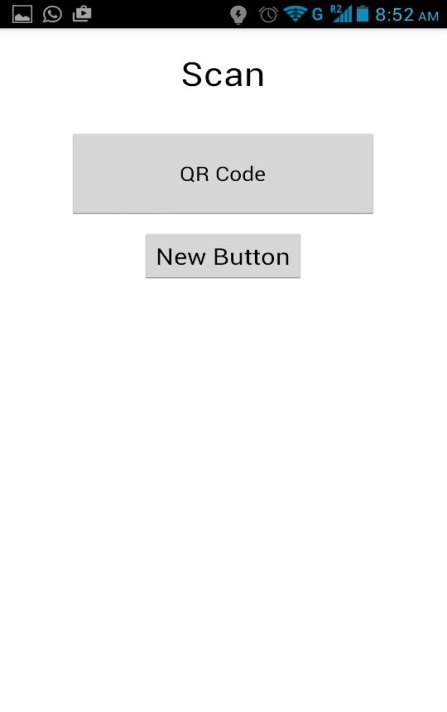
**5.1.1 ANDROID EVIRONMENT**:

**Fig 5.1 Main screen Fig 5.2 Login Page Fig 5.3 Sign up page**



**Fig 5.4 Delete account page Fig 5.5 Set new pass code page Fig 5.6 First half passcode entry**

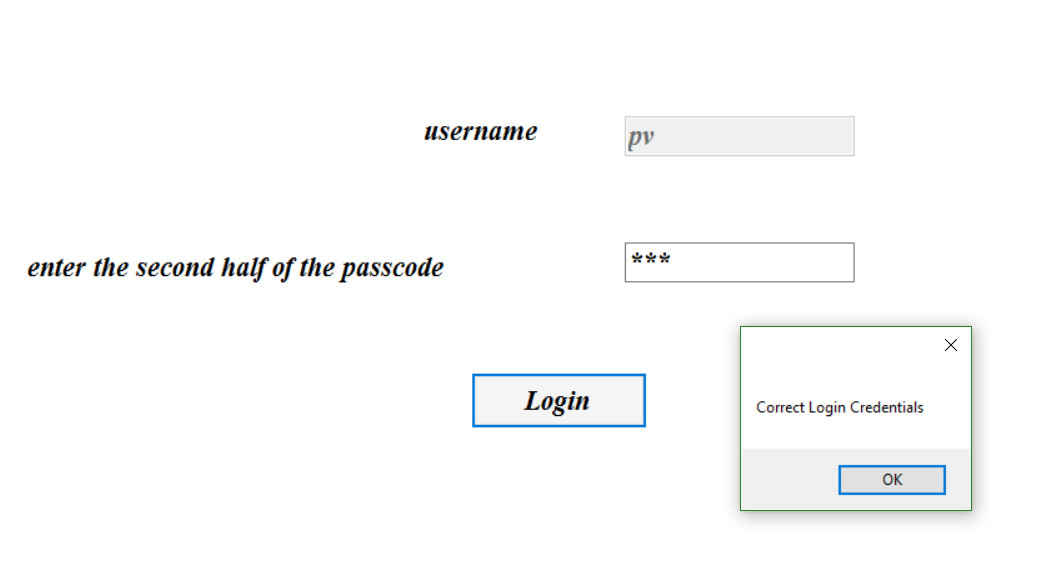
**Fig 5.7 QR code scanning page Fig 5.8 Scanned qr code with its contents**

**5.1.2 WINDOWS ENVIRONMENT:**

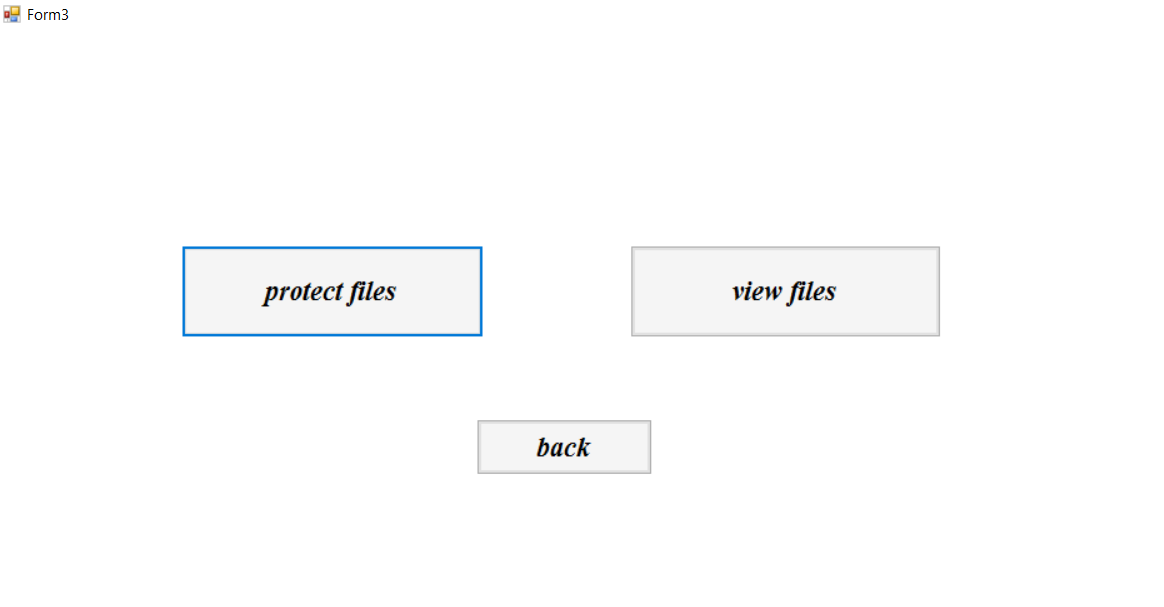
SUCCESS PATH:



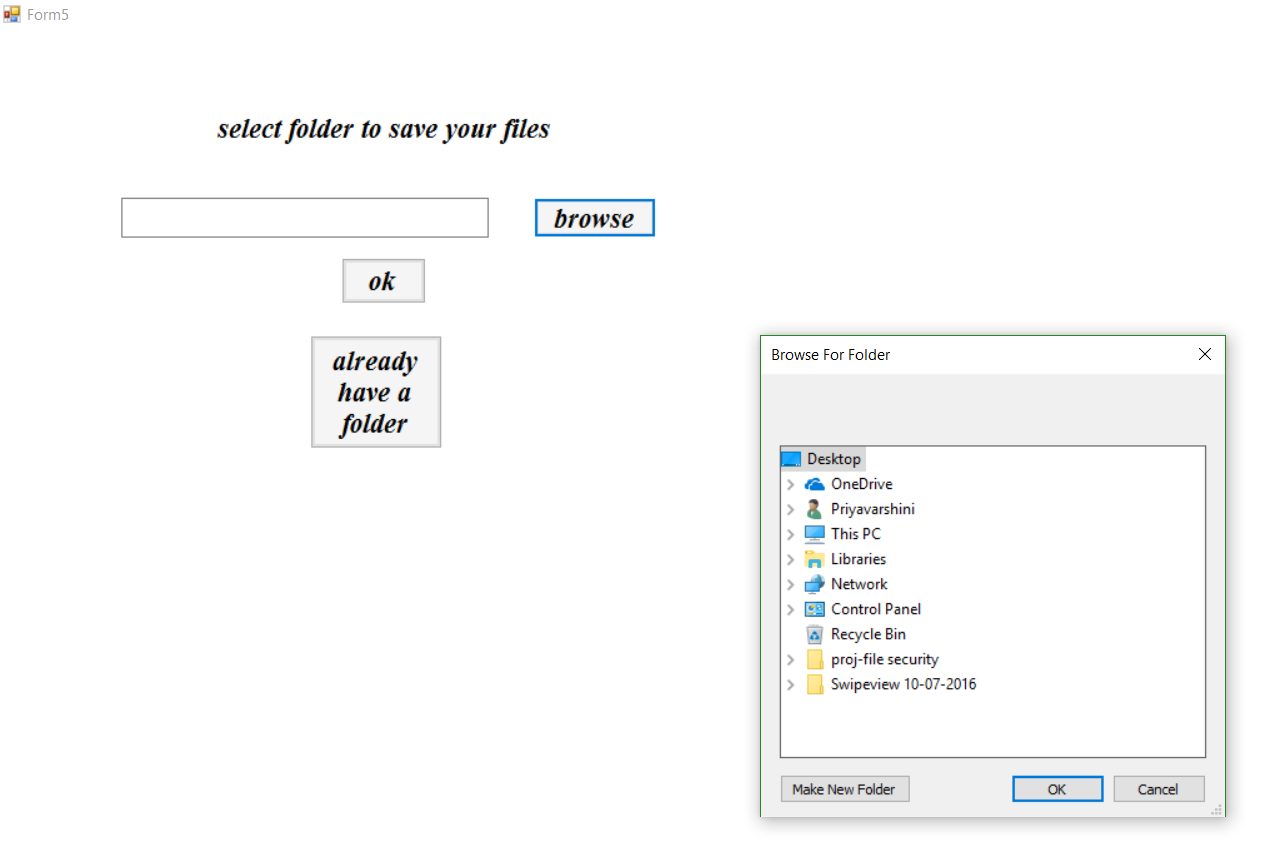
**Fig 5.9 Waiting for the acknowledgement from the android mobile**



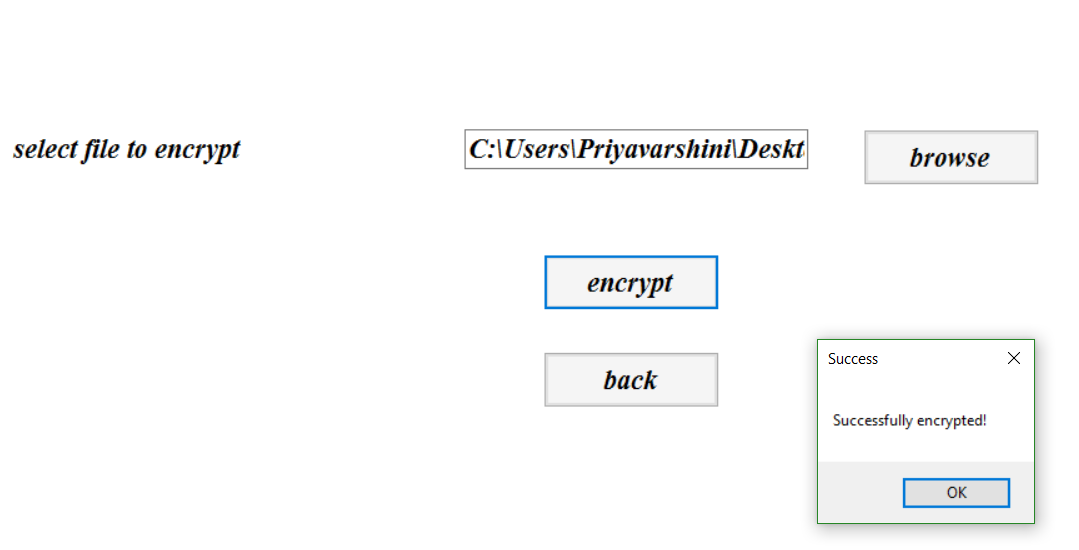
**Fig 5.10 second half of the pass code entry page**



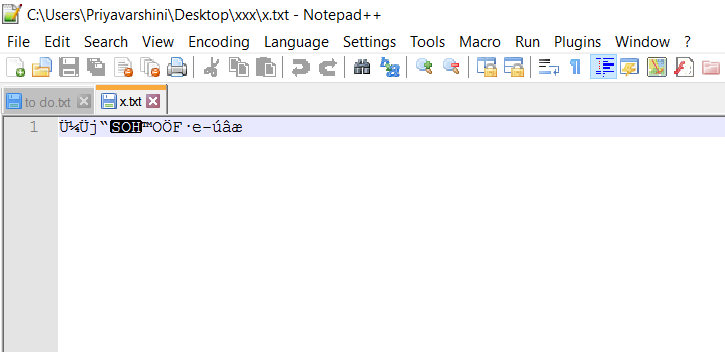
**Fig 5.11 Choice selection page**

****

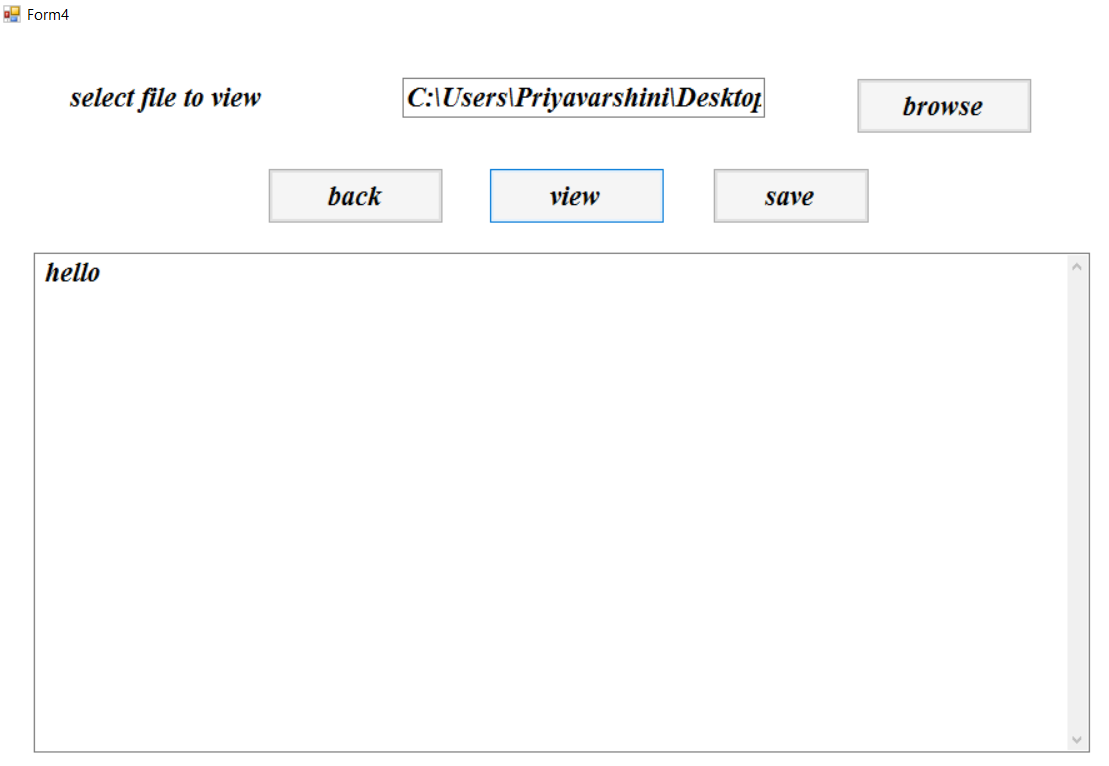
**Fig 5.12 Folder selection page for the first time users**



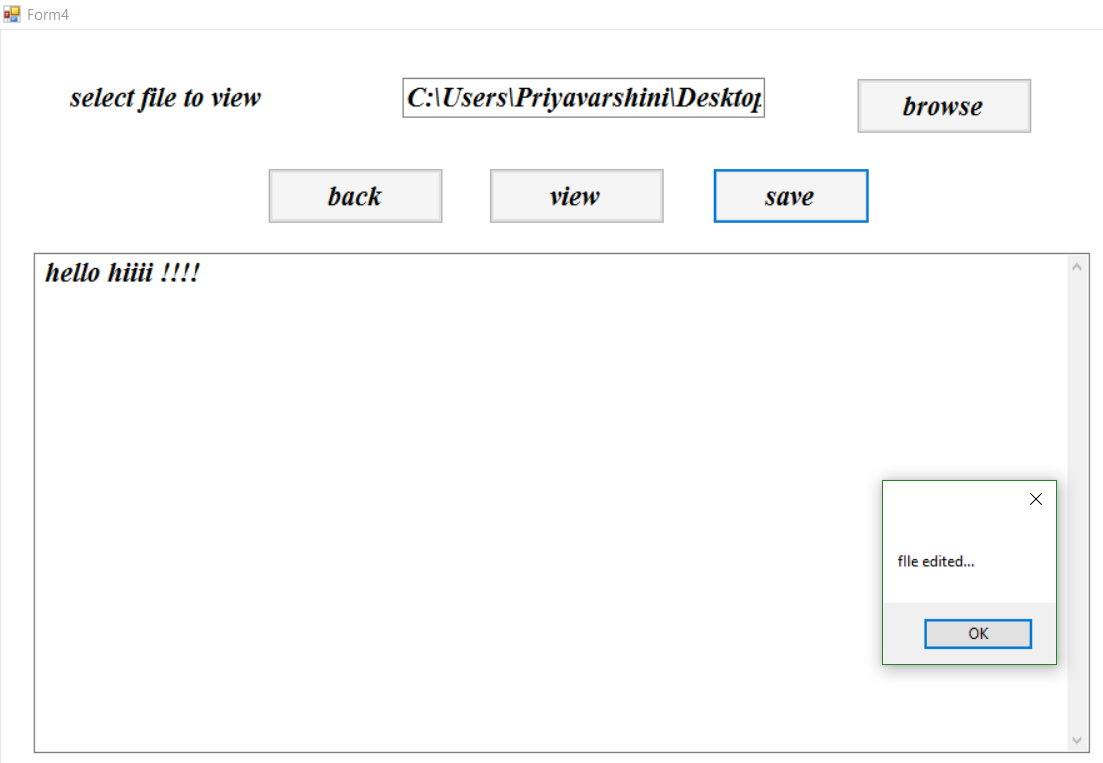
**Fig 5.13 File encryption page**



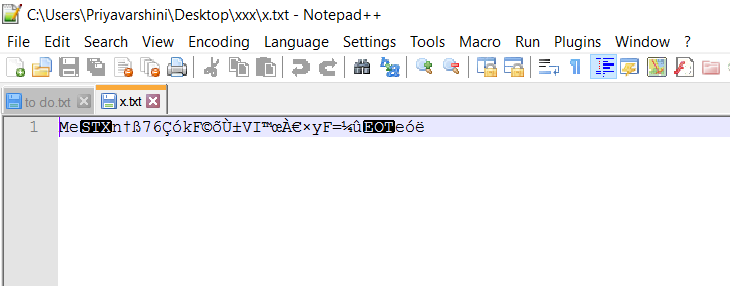
**Fig 5.14 Encrypted contents of the file**



**Fig 5.15 File decryption page and the decrypted contents**



**Fig 5.16 Editing of the file is made here**



**Fig 5.17 contents of the file after editing in the encrypted format**

**5.2 TEST CASES:**

5.2.1 ANDROID ENVIRONMENT:

* REGISTER:

The user has to register to use this software only through the android mobile. While registering the application checks if the user is already registered. This username and password is used to login into the android application afterwards.

* LOGIN:

During logging into the android application, the username and password are validated against the contents of the database.

* DELETE:

This application also allows to delete the existing account after verifying the correctness of the details asked.

* FIRST PASSCODE:

The first half of the pass code entered in the android application is validated to continue to the qr code scanning page.

* QR CODE SCANNING:

The QR generated in the PC is entered in the database or else validated against the already entered contents to generate the appropriate acknowledgement.

**5.2.2 WINDOWS ENVIRONMENT**:

* ACKNOWLEDGEMENT:

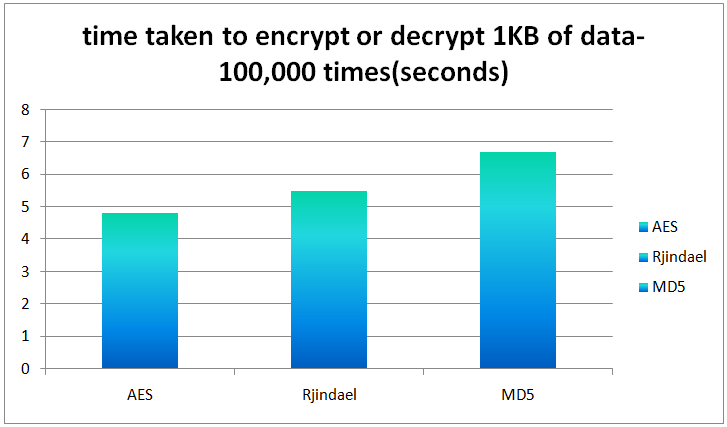
The software that runs in the PC waits until an acknowledgement is received from the android mobile. This is tested by the contents of the database.

* SECOND PASSCODE:

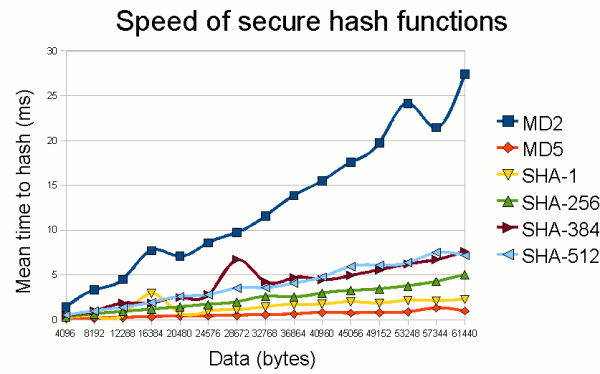
Here the user has to enter the second half of the pass code that he set up during registering in the android application. This second pass code is also validated.

* FOLDER SELECTION:

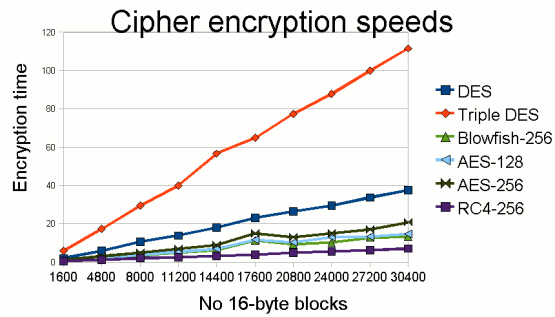
The user is asked to choose a folder where he wants to save the important files and folders. This folder path is entered into the database if the user is using the application for the first time. If a folder was already chosen, the user cannot choose another folder.



**Fig 5.1 comparison between time taken by various algorithms to encrypt and decrypt 1 kilobytes of data**



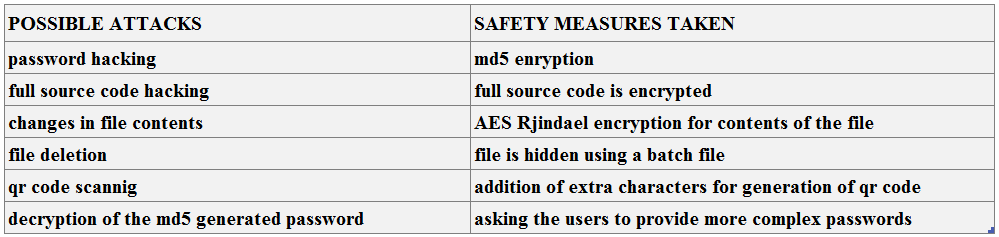
**Fig 5.2 comparison between the speed of various hashing functions**



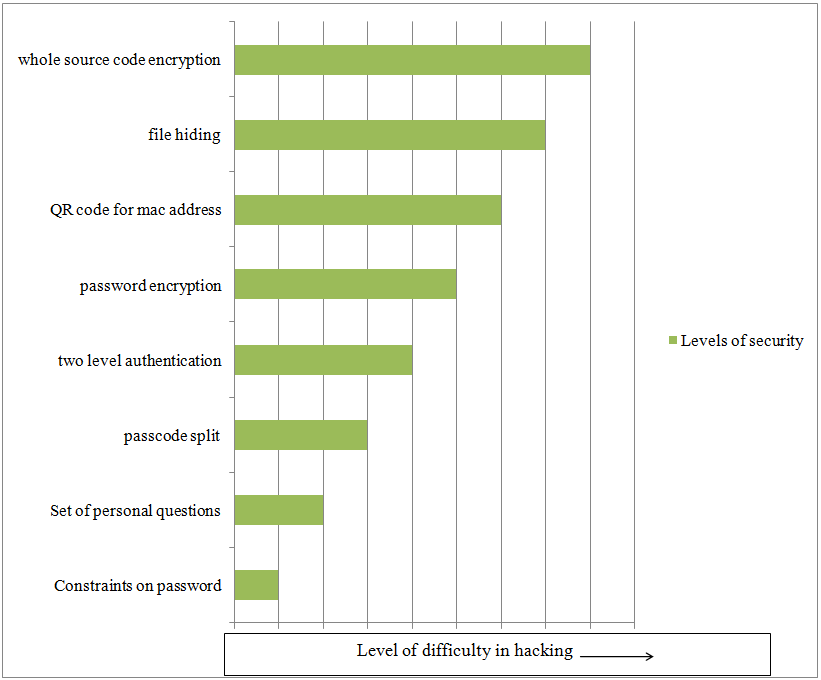
**Fig 5.3 comparison between the cipher encryption speeds of various encryption algorithms**

**5.3 TEST RESULTS:**

* The result of file security system is that the user can secure any file in his / her laptop in any folder according to his / her wish and incorporating multiple levels of security so that it is very difficult for the hackers even to trace the location of the files.
* The analysis is that once a file is placed within a folder in this application the folder is locked and then even the user can only access the file using his smart phone by carrying out the procedure from the start.
* Every laptop is tied to a unique user. Hence other users cannot store the files in the same PC.

****

**Fig 5.4 Table describing the possible attacks on the file security system and the measures taken to avoid those attacks**

****

**Fig 5.5 Various levels of security provided**

**CHAPTER 6**

**CONCLUSION AND FUTURE WORK**

**6.1 CONCLUSION**

Thus this system provides multiple levels of security for protecting the files and folders in the personal computer by mutual authentication by the android application and the windows application. Hence even if the PC goes into unauthorized person and even they manage to log into the windows account they may not be able to find the files and folders that are protected by this application. The only way to view those files and folders is by using this application. Even if they manage to find the location of the files, the contents are encrypted that makes it difficult to understand the contents of the file.

**6.2 FUTURE WORK**

Further protection can be provided preventing the deletion of the protected files and folders. Centralized cloud database can be used for storing the user details and the backup of folders in case the account or the folder is to be deleted.

Appendix A:

The undersigned acknowledge they have completed the <Project> and agree with the approach it presents.

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: |  | Date: |  |
| Name: | SACHIN KUMAR.S |  |  |
| Signature: |  | Date: |  |
| Print Name: | SANDHYA.A.K |  |  |
| Signature: |  | Date: |  |
| Print Name: | PRIYAVARSHINI.M |  |  |

Appendix B: References

The following table summarizes the documents referenced in this document.

[1] BLUETOOTH ENABLED MOBILE PHONE REMOTE CONTROL FOR PC - Qadeer, M.A. , Agrawal, R. ,Singhal A. and Umar. S.International conferences on Advanced Computer Control, 2008.IEEE DOI 10.1109/ ICACC .2009.91 .

[2] POCKETDROID-A PC REMOTE CONTROL - ChaitaliNavasare, DeepaNagdev International Conference on Information and Network Technology.2012 vol 37.

[3] SESSION KEY EXCHANGE AND MUTUAL AUTHENTICATION SCHEME BETWEEN MOBILE MACHINES IN WLAN BASED AD HOC NETWORKS - HyosunRoh, Souhwonjung - School of Electronic Engineering, Soongsil University, Korea.PUBLISHED IN: International Conference on Information and Communication Technology Convergence (ICTC). 17-19 Nov. 2010.

[4] AN ENHANCED REMOTE MUTUAL AUTHENTICATION SCHEME USING SMART CARDS - JieGu, ZhiXue, Yan Zhu, Fangbiao Li, Xiao Chen. CONFERENCE: symposium on ICT and energy efficiency and workshop on information theory and security(CIICT 2012).ISBN: 978-1-84919-5478.Location: Dublin, Ireland.Conference date:4-5 July 2012.Publisher: IET.

[5] MOBILE ENCRYPTION FOR LAPTOP DATA PROTECTION- Y.W. Kao, X. Zhang, A. Studer, A. Perrig .PUBLISHED IN:Volume 6, Issue 4, 2012 ,pg. 291 – 298.PUBLISHER: IET

[6] https://www.tutorialspoint.com/db2/db2\_database\_security.htm

[7] http://www.techrepublic.com/blog/microsoft-office/prevent-users-from-changing-data-by-using-access-form-control-properties/

[8] http://www.makeuseof.com/tag/how-to-connect-your-cell-phone-to-your-pc-through-bluetooth/

[9] http://www.instantfundas.com/2009/04/how-to-prevent-file-copying-deletion.html

[10] http://www.exnol.com/prevent-file-data-copy-pc-usb-drive

[11] http://paper.ijcsns.org/07\_book/201005/20100506.pdf

[12] https://technet.microsoft.com/en-us/library/ff936144.aspx

[13] https://msdn.microsoft.com/en-us/library/windows/desktop/aa364399(v=vs.85).aspx

[14] https://www.tutorialspoint.com/operating\_system/os\_security.htm

[15] https://labs.portcullis.co.uk/blog/new-restricted-admin-feature-of-rdp-8-1-allows-pass-the-hash/

Appendix C: Key Terms

The following table provides definitions for terms relevant to this document.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| AUTHENTICATION | The process or action of verifying the identity of a user or process  Passcode- a string of characters used as a password, especially to gain access to a computer or smartphone |
| QR code | a machine-readable code consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smartphone  Encryption-the process of converting information or data into a code, especially to prevent unauthorized access |
| HIDING | A hidden file is any file with the hidden attribute turned on. Just as you'd expect, afile or folder with this attribute toggled on is invisible while browsing through folders - you can't see any of them without explicitly allowing all of them to be seen |