**FILE SECURITY SYSTEM IN PC**

SACHIN KUMAR 2014103557

A.K.SANDHYA 2014103558

M.PRIYAVARSHINI 2014103621

**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.

**Introduction:**

* The project deals with the security of file systems in personal computers.
* To prevent the hacking activities, the proposed system can protect the confidential files by authorizing the person from both the smart phone and the personal computer i.e., by providing mutual authentication features.

This system has two parts:

* 1. The application that runs on the user’s smart phone.
* 2. The application that runs on the Personal computer.

It implements 5 levels of security:

1. The username and password that the user has to enter to get in to the android application in the smart phone. The first half of the pass code to view the files is entered in the Smart phone. If correct the confirmation is sent to the PC.
2. The second half of the password is entered in the PC to access the files.
3. Restriction even to the admin to make the changes in the database content.
4. Set of personal questions to reset or change the password which is answerable by the user alone.
5. The files if accessed by someone accidentally other than the user, they cannot be copied or edited.

This application as said before runs in two phases.The first phase works in android mobile side and the other in the user’s computer.Whenever the user wants to access the files or folders he or she must first login into the application in the android phone.The user cannot login from any mobile phone but he or she has to login from a registered mobile phone i.e the phone from which its mobile number is registered.Thus in case of stolen laptops also, hacking is impossible because access is given only when the mobile phone sends acknowledgement to the laptop.

In the first phase of the application which runs on the android mobile side, the user has to login to the application with a username and a password which is general to the application.If the user is not a registered user or if he or she is going to login to the first time in the application, then the user has to register the passcode first and then has to login to the application.Once successfully logged into the application, the user has to type the first half of the passcode in the application. This is crosschecked with the backend data that is priorly saved and if the validation turns out to be true then an acknowledgement message is sent to the user’s laptop.

Once the passcode is to be saved in the database its length is found out and the splitted into two halves so that the first half of the passcode is entered in the first column of the databse and then the second half of the passcode is entered in the second column of the database.

In the second phase of the application that runs in the laptop the second half of the passcode is typed once and only when the acknowledgement message from the user’s android mobile phone reaches the laptop through wireless transfer. If the second half of the passcode passes the validation against the data saved in the backend then the user is given access to the files and folders which is present inside the windows application of the laptop.

As the final level of security, this application prevents normal editing of the files. If in case the user if wants to do some changes in the files or if the user want to edit the files and folders, then the user wants to give another password which allows editing of the files present.

**Related works:**

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:**

Chaitali Navasare, 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:**

Hyosun Roh, Souhwon jung - 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:**

Jie Gu , Zhi Xue , 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.

**Problem statement**:

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.

**Solution:**

Increasing the strength of security and enhancing the levels of security for the users file system is the only possible way for this problem. Now-a-days even the finger print authentication is being hacked. So if that is the current scenario, then we have to ensure most difficult levels of security for securing our files and documents from the hackers and other attacks that they are prone to. So we thought of doing this in an application that works in two phase and implements multiple levels of security as mentioned and explained before.

**CONTRIBUTION:**

**Analysis Design Coding Testing**

**1.User Interface:**

**Android:** sandhyasachin Priya sachin

**Windows:**  sachin priya sandhya priya

**2.Database:** Priya sandhya sachin sandhya

**Architechture / Block diagram:**

**Module design:**

**MODULES**

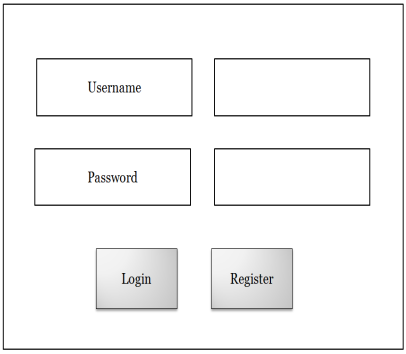
**MODULE 1:SMART PHONE UI  
 M 1.1 : ENTRYPAGE 1**

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

1) Register : Redirected to M 1.2

2) Login : Redirected to M 1.3

* 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

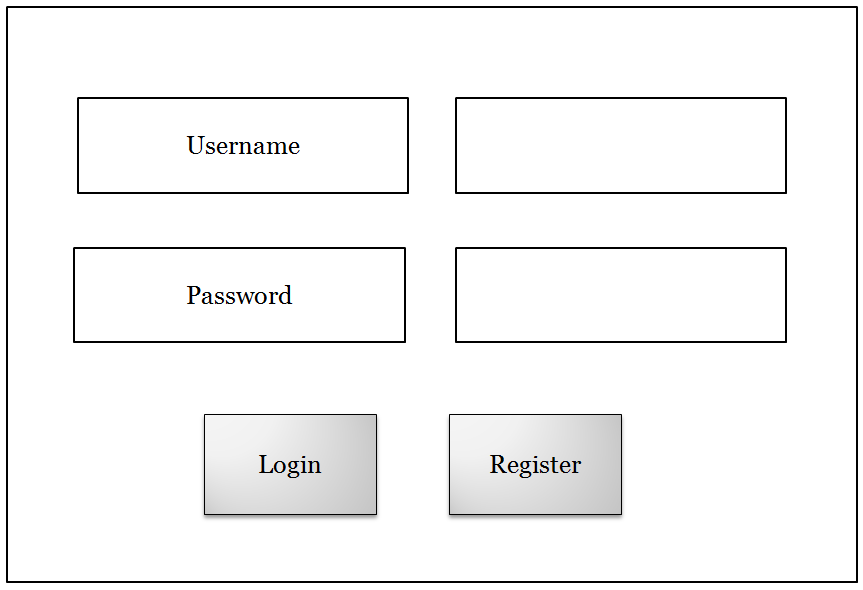
Reenter username and password

* 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

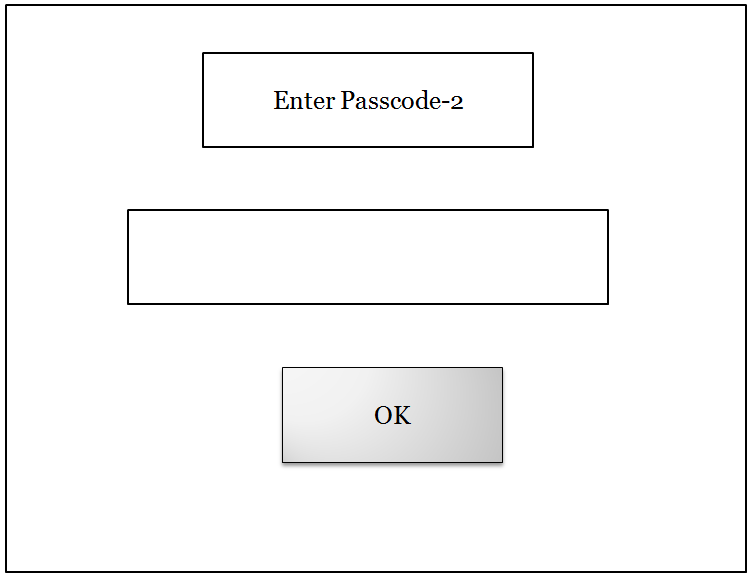
**MODULE 2: PERSONAL COMPUTER UI  
M 2.1 : HOME PAGE**

* INPUT :

1) Acknowledgement received from the smart phone.

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.

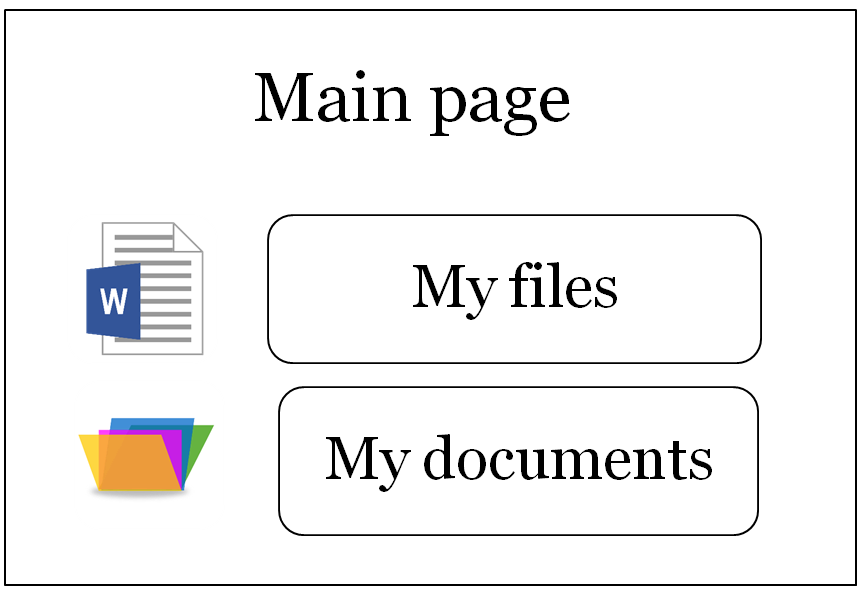
-else ,throw error message.

**M 2.2 : MAIN PAGE**

* CONTENT : List of all folders and files imported by the user.
* OPERATIONS :

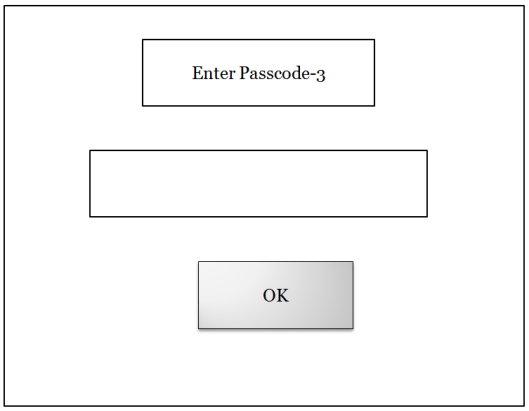
1) The user can view the contents of the files and folders.

2) The page gets redirected to M 2.3 when the user tries to edit or copy the file.



**M 2.3**

* INPUT : Pass code entered by the user .
* OUTPUT : Enables the user to edit or copy the file.
* PROCESS : Verifying the entered pass code with the DB contents .



**ALGORITHM**

1) enter the pass code.

2) Check for if correctness

-yes , allow to copy or edit

-no , prompt to re-enter the pass code.

**Implementation:**

**Initial setup/tools:**

* Android studio - smart phone user interface
* Visual Studio - PC user interface
* PHP code – connecting the front end with the back end database.
* DATA SET: Mutual Authentication , Security , Mobile to PC data transfer ,Wireless communication ,Authentication.

**SUPPORT INFORMATION :**

**BLUETOOTH ENABLED MOBILE PHONE REMOTE CONTROL FOR PC**

* This work confers an application which makes possible to use a Bluetooth enabled mobile phone to remote control home appliances such electric fan, LEDs and stepper motor, connected to the personal computer.
* It can also be used to control other computer applications such as multimedia players and facilitates the user while giving presentation on slides.
* It is a client – server based application which makes use of powerful java technology to achieve its end.
* The program works on a variety of Bluetooth enabled mobile phone and is compatible with majority of Bluetooth stacks.

**POCKETDROID-A PC REMOTE CONTROL**

* 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.
* PocketDroid surrounds the Client and Server application. In which, the Server application has been implemented in JAVA and Client application in Android. As both JAVA and Android are open source platform thus they allows the development of new ideas and tests them with a set of open standards.
* One can use PocketDroid to share files between PC and android device, start and stop the applications installed on the Target PC, shutdown the Target PC and much more.
* This application also contributes for IT Administrators to remotely control any computer present in the network, allowing them to troubleshoot and solve problems faster.

**SESSION KEY EXCHANGE AND MUTUAL AUTHENTICATION SCHEME BETWEEN MOBILE MACHINES IN WLAN BASED AD HOC NETWORKS**

* 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 proposed scheme is secure against man-in-the-middle attack, impersonation attack, and modification attack.

**AN ENHANCED REMOTE MUTUAL AUTHENTICATION SCHEME USING SMART CARDS**

* 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.
* 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.

**MOBILE ENCRYPTION FOR LAPTOP DATA PROTECTION**

* 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.
* 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.

**Surveyed content:**

**Reference 1:**

**BLUETOOTH ENABLED MOBILE PHONE REMOTE CONTROL FOR PC**

[**http://ieeexplore.ieee.org/document/4777442/**](http://ieeexplore.ieee.org/document/4777442/)

**Reference 2:**

**POCKETDROID-A PC REMOTE CONTROL**

[**https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=0ahUKEwiOq8qFktvRAhWBHZQKHQ77DccQFggbMAA&url=http%3A%2F%2Fwww.ipcsit.com%2Fvol37%2F015-ICINT2012-I090.pdf&usg=AFQjCNFAmjQmZFRoi51Rcs6bYFO8iF09Gw&sig2=D53ZpaL\_tNVz69NgdrrR2Q**](https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=0ahUKEwiOq8qFktvRAhWBHZQKHQ77DccQFggbMAA&url=http%3A%2F%2Fwww.ipcsit.com%2Fvol37%2F015-ICINT2012-I090.pdf&usg=AFQjCNFAmjQmZFRoi51Rcs6bYFO8iF09Gw&sig2=D53ZpaL_tNVz69NgdrrR2Q)

**Reference 3:**

**SESSION KEY EXCHANGE AND MUTUAL AUTHENTICATION SCHEME BETWEEN MOBILE MACHINES IN WLAN BASED AD HOC NETWORKS**

[**http://ieeexplore.ieee.org/document/5674797/**](http://ieeexplore.ieee.org/document/5674797/)

**Reference 4:**

**AN ENHANCED REMOTE MUTUAL AUTHENTICATION SCHEME USING SMART CARDS**

[**http://ieeexplore.ieee.org/document/6513836/**](http://ieeexplore.ieee.org/document/6513836/)

**Reference 5:**

**MOBILE ENCRYPTION FOR LAPTOP DATA PROTECTION**

[**http://ieeexplore.ieee.org/document/6404337/**](http://ieeexplore.ieee.org/document/6404337/)

**References:**

* 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 .
* POCKETDROID-A PC REMOTE CONTROL, Chaitali Navasare, DeepaNagdev International Conference on Information and Network Technology.2012 vol 37.
* SESSION KEY EXCHANGE AND MUTUAL AUTHENTICATION SCHEME BETWEEN MOBILE MACHINES IN WLAN BASED AD HOC NETWORKS, Hyosun Roh, Souhwon jung - School of Electronic Engineering, Soongsil University, Korea.PUBLISHED IN: International Conference on Information and Communication Technology Convergence (ICTC). 17-19 Nov. 2010.
* AN ENHANCED REMOTE MUTUAL AUTHENTICATION SCHEME USING SMART CARDS ,Jie Gu , Zhi Xue , Yan Zhu , Fangbiao Li , Xiao Chen.CONFERENCE: symposium on ICT and energy efficiency and workshop on information theory and security(CIICT 2012).ISBN: 978-1-84919-547-8.Location: Dublin, Ireland.Conference date:4-5 July 2012.Publisher: IET.
* 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