Two Way Authentication using USB Flash Drive

A. Marcellus Brindha, S.Satheesh Kumar

Abstract— USB Flash Drive is used for transferring data's, audios, videos etc with in a fraction of second, it can be used for taking backup of the entire computer data's. It can also used for locking and unlocking the computer. The main aim of this project is to secure the confidential data's from unauthorized access by using the powerful and timeless Authentication process. This Authentication is made as a user-friendly option and timeless. In this project software is build to use the USB Flash Drive authentication process. In existing software there is no effective alert system and not more user friendly option. In this project there is an effective alert system i.e. when the user uses wrong USB Flash Drives or Password after the limited wrong attempts it sends the alert message to the higher authority or send alert message to the mobile phones .User can select the options they needed. It can also lock the desktop till the user specified time after the time limit it shutdowns or any other options selected by the user.

Index Terms— Authentication, Higher Authority, USB Flash Drives, User friendly.

1 INTRODUCTION

USB Flash drive is a best storage device for enormous number of data. It can store data's like audio, video, files etc. This type of files can transfer one computer to another within the fraction of seconds. So only we can say the USB Flash Drive as plug and play process. The USB Flash Drive can be used for taking backup of the files. When compared to CD, DVD and mass storage USB Flash drive is the best mass storage device. It is easy to delete and copy the files from a drive. Where other devices take time to copy the files and some storage device do not have erasable process [10].

The USB Flash drive not only store data it can be used as a authentication .In this project the USB Flash Drive is used to lock and unlock the computer. Because of this process the authentication time is less and unauthorized person cannot take the confidential data .If the unauthorized person try to access an effective alert system is made that will sent to the higher authorities or user mobile phone.

The main objective of the project is to (1) Provide security locking to the Confidential Desktop computers.(2)Unauthorized person must not access to the confidential Data.(3)Confidential Information is kept with safe locking.(4)Effective Alert System is kept to catch unauthorized accessing.

The Arrangement of this Paper is as follows. Section 2 contains the functional design of the software. Section 3 describes the proposed process. Section 4 says about the result and discussion. Section 5 describes about technological support needed. Section 6 says the benefits of the project. Section 7 describe the Conclusion. Section 8 tells the Future Works can be done.

- *A. Marcellus Brindha is currently pursuing masters degree program in Computer Science and Engineering (with Specialization in Networks), Velammal College of Engineering and Technology, Madurai, TamilNadu India, E-mail: marcellusbrindha8@gmail.com*
- *S.Satheesh Kumar is currently Assitant professor III in Velammal College of Engineering and Technology, Madurai, TamilNadu India , E-mail sks@vcet.ac.in:*

2 FUNCTION DESIGN

In this section it focuses on the function design of the proposed system. The system has the following concepts involved.

2.1 Authentication

The authentication function is used for locking the confidential data in the computer. When we use the authentication method the confidential data is safe .In this project we are using two Authentications i.e. Password and USB Flash Drive

2.2 Authorization

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. In this paper we use the authorization for USB Flash Drive. The secured USB Flash drive is used.

3 PROPOSED AUTHENTICATION METHOD

User need to run the software .It takes to the user Authentication Window. Then the user need to select the first and second authentication option that is used for login .Here we use USB Flash Drive and Password as the authentication process. The user need to select the incorrect option and number of wrong attempts that needed to implement when the authentication is wrong .After the number of wrong attempts it need to implement the incorrect option .The incorrect option contains four choices (1)Alert message to Higher Authorities (2)Alarm option(3)Shut Down (4)Alert message to Mobile phone. Select any number from 1 to 10. According to the user option the authentication takes place. After selecting it takes you to another window were we needed to select the device used for authentication and select the option when the USB

Flash drive is removed in the middle of process. Then it takes you to another second authentication process window were it used for creating, changing the password .After that when we click finish button the process are all saved. Now restart your windows. Now is asked to login then insert the USB Flash Drive device you selected in the Process it then ask for Password type the password now it will login. If you used a wrong drive or wrong password more than the wrong attempts selected it will take the selected incorrect option action. When we remove the USB Flash drive in the middle the selected action takes place. This process is divided into 5 modules .They are

- User Authentication selection.
- USB Flash Drive Authentication.
- Password Authentication.
- Alert message to higher Authorities.
- Alert message to Mobile Phones.

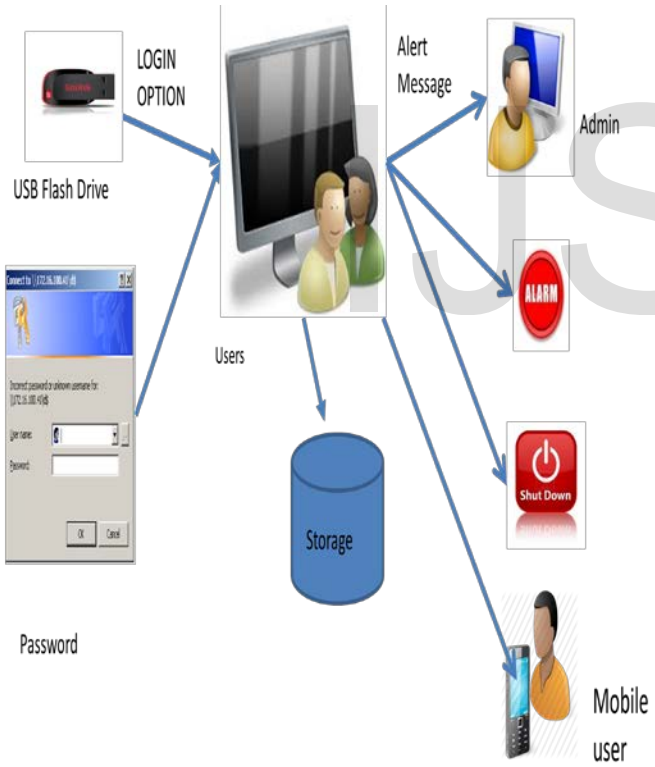

FIG 1: SYSTEM ARCHITECTURE

3.1 User Authentication Selection

The User can select the Authentication process that should be used for locking and unlocking the computer .There are two Authentications used in the process. They are USB Flash Drive and Password Authentication. This module is used for selecting which is the First and Second Authentication used to lock the computer. User can select the incorrect option and Number of wrong attempts by their own.

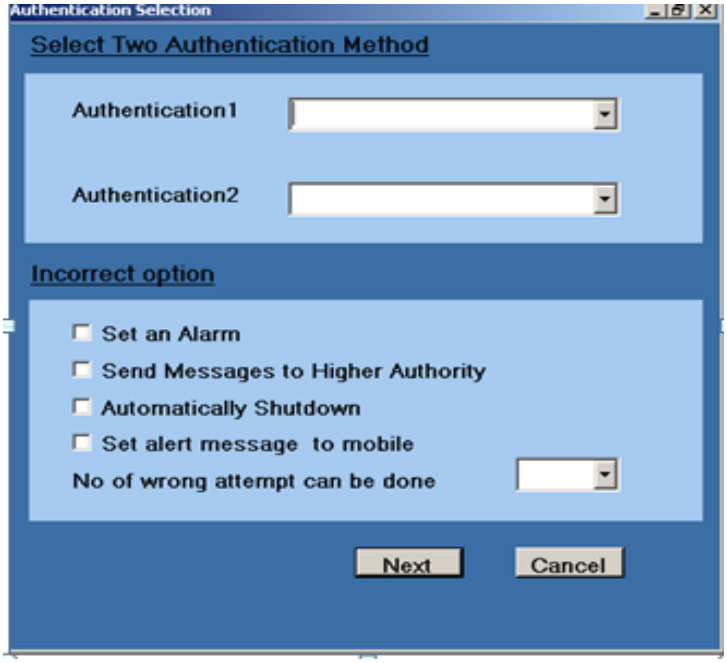

FIG 2: MODULE 1 SCREENSHOT

3.2 USB Flash Drive Authentication

When the USB Flash Drive option is selected this module start working. The selection of USB Flash Drive Device for Authentication is chose. With the selected USB flash drive only it will lock and unlock the computer. If the USB flash Drive removed in the middle then the user choice to do the action.

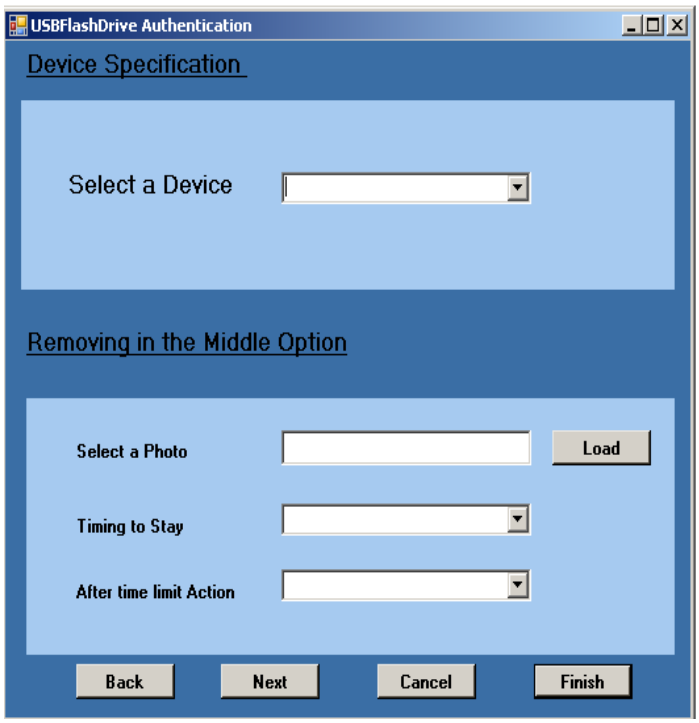

FIG 3: MODULE 2 SCREENSHOT

3.3 Password Authentication

The selected Password Authentication can do these operations

- To create Password to login the computer.
- To change the old Password.
- Creation of new Password.

These operations are done first. If the user selects First Authentication option as Password the above operation takes place. If the USB Flash Drive loss we can use this authentication.

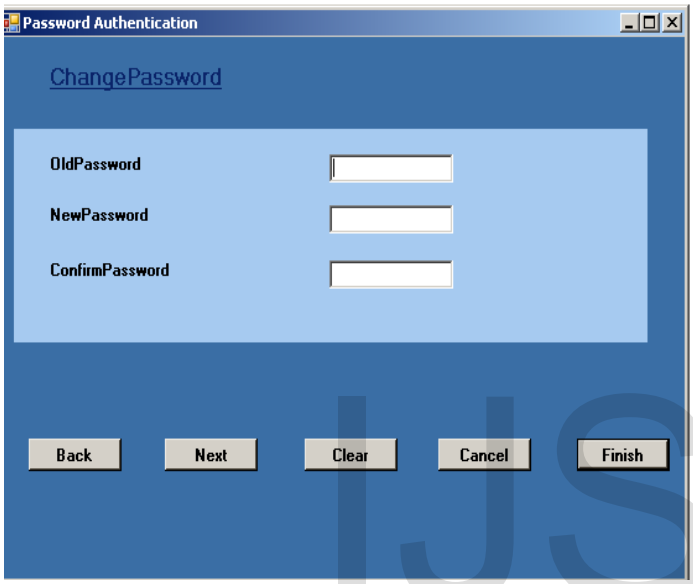

FIG 4: MODULE 3 SCREENSHOT

3.4 Alert Message to Higher Authorities

The user is asked to select an incorrect option if the user selects the above Module. Then it sends an alert message from the user computer to Admin computer when more than the user wrong attempts take place. If any unauthorized action takes place the alert message will be sent.

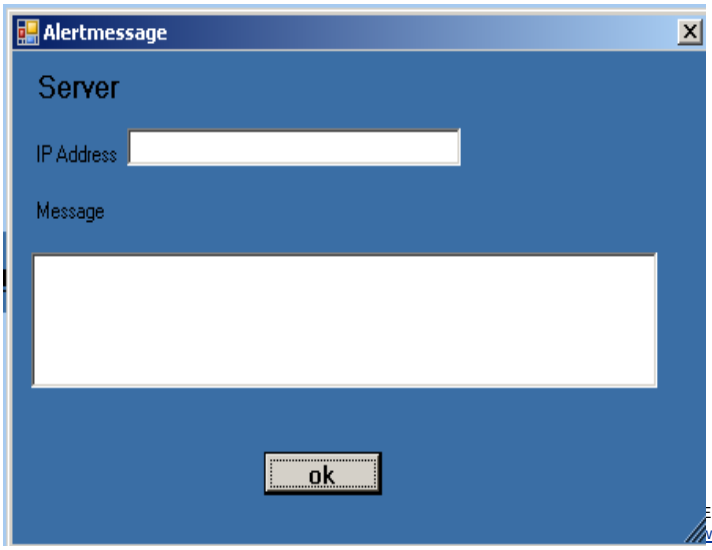

FIG 5: MODULE 4 SCREENSHOT

3.5 Alert Message to Mobile Phone

When the user selects this option it sent the alert message to the user mobile phones exceeds the user login attempts. This option can do in the entire home desktop computer. If any unauthorized action takes place the alert message will be send.

FIG 6: MODULE 5 SCREENSHOT

4 Results And Discussion

This chapter presents the results and discussions of the project carried out. The main objective of this project is to provide security locking to the confidential Desktop computers and also provide user friendly option to select their own authentication settings. Unauthorized person cannot get the confidential data from the computer. The time to login is less. Confidential information is kept with safe locking. Nobody can change the authentication other than the user. The Effective Alert System is kept to catch unauthorized accessing person easily. This software can be used for Government sectors, colleges and Home Computers.

5 Technology Support

The following are the technological challenges in designing of the Authentication

- Selecting the secured USB Flash Drive.
- The Alert message sent to the higher Authorities using
- IP Address at the required time.

- Wi-Fi connection in the Desktop and Mobile send the alert message between them.

6 Benefits Of The Proposed System

Secure the Confidential data from the unauthorized person is proposed for the use of Government sectors. For this purpose following benefits are implemented. They are as follows

- Confidential data is safe and secure.
- Time consuming for login is less.
- Remembering of password is not necessary.
- If Loss of Device it has another option.

7 Conclusion

The Two way Authentication is used for all the Desktop computers. This software makes the data safe and secure. The user can be confident to store the data because of the effective alert system. The software is user-friendly that can be selected by the user itself.

8 Future Work

We can improve the above process with more authentication option like biometrics. The alert system can also further improved by Mobile apps alert message in Video or Audio.

Acknowledgment

This work was done in Aeronautical Development Agency, Bangalore under Mr.G.Ramakrishnan who is the Scientist Engineer G in the ICT Department.

References

[1] Debiao He, Neeraj Kumar, Jong-Hyouk Lee, *Senior Member*, IEEE, and R. Simon Sherratt" Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices" IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014

[2] http://www.makeuseof.com/tag/3-toolsturning-usb-drive-secure-unlock-key-pc/

[3] http://www.predator-usb.com/predator/en/index.php.

[4] http://www.thewindowsclub.com/free-software-lock-windows-using-usb-pen-drive

[5] http://web.deepnetsecurity.com/products2/FlashID.asp

[6] https://helpdesk.lastpass.com/multifactorauthentication-options/sesame-multifactor-authentication-with-a-usb-thumb-drive/

[7] K. -A. Shim, "Security flaws in three password-based remote user authentication schemes with smart cards," *Cryptologia*, Taylor and Francis, vol. 36, no. 1, pp. 62-69, Jan. 2012.

[8] M. Alzarouni, "The reality of risks from consented use of USB devices, "in Proc. 4th in Proc. 4th Australian Information Security Management Conference, pp. 312-317, December 2006.

[9] http://www.rohos.com/products/rohos-logon-key/

[10] Ray Chance President , "Understanding USB Flash Drives As Portable Infrastructure" Browser craft, LLC 2005