ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 4, April 2016

Key Based Model to Secure Storage Devices

Mayuri K. Dhole
Department of computer Science and Engineering
G.H. Raisoni College of Engineering
Nagpur, India

Prof. SonaliNimbhorkar
Department of computer Science and Engineering
G.H. Raisoni College of Engineering
Nagpur, India

***Abstract*-USB peripheral devices such as pen drives, printers, scanners, external hard disk have increased in numbers in recent decades. External USB storage devices are considered as popular devices in market. USB can transmit data with high speed. But they are not permitted in institutions that work with confidential file because of security concern. Therefore a technique must be developed to secure the data so that the authorized user can freely use the mass storage devices. This paper proposes a software based technique that secures the files and data stored.**

***Keywords*- peripheral devices, Universal Serial Bus (USB), USB storage devices**

I. INTRODUCTION

Today's world is continuously progressing in different aspects. Be it economically, industrialized or culturally. We are now always trying to develop innovative goods n things for better living of society. Some of these innovations are required to be kept safe. The data related to these innovations should be secured. As these innovations could play an important part for military based and medical based centers and government institutions that have an access to any confidential data. The data stored in these institutions is very confidential. Therefore if it is required to be transferred from one place to another then it should be transferred in a secure way. Here comes the role of mass storage devices that stores the data and transfers it from one machine to another. But if this mass device gets in the hands of any unauthorized person then this confidential data stored in the device is prone to stealing, tampering and misusing. So there is a need to develop a technique or model that can save the data from stealing and tampering. Many different techniques and protocols have been proposed for this purpose. Some techniques are based on passwords. Some are based on biometric keys. Some others are based on smart cards. Some other protocols are combination of the above mentioned parts.

II. DRAWBACKS OF EXISTING SYSTEM

The existing systems are based on passwords. Many other systems are also based on biometric keys. Others are based on smart cards. But using these methods has some drawbacks.

Following are the drawbacks of existing system:

A. The protocols that are based on password depend on the strength of the password. That is, if the password is less strong then more chances are there that they can be cracked and data can be stolen.
B. The protocols that are based on smart cards are less prone to data stealing. But as it is a hardware part it increases the protocol implementation cost as well as is difficult to handle.
C. The third drawback is related to the biometric keys. These are not easy to handle. For example, suppose our technique is based on securing the storage device by using the thumb impression of the user on the machine. If the user has applied some ink or henna on his/her thumb then it becomes next to impossible for the system to detect the thumb impression of the user.
D. Also another drawback related to biometric keys is that it increases the cost of the implementation of the protocol.

Due to the above drawbacks observed in the existing system, there is a need to develop a different technique or protocol that can overcome the drawbacks of existing system.

III. PROPOSED SYSTEM

This proposed system is software based so that the implementation cost is reduced as well the handling of the system becomes easier. This is done by developing a three tier keys based protocol.

A. *Flowchart Of Proposed System*

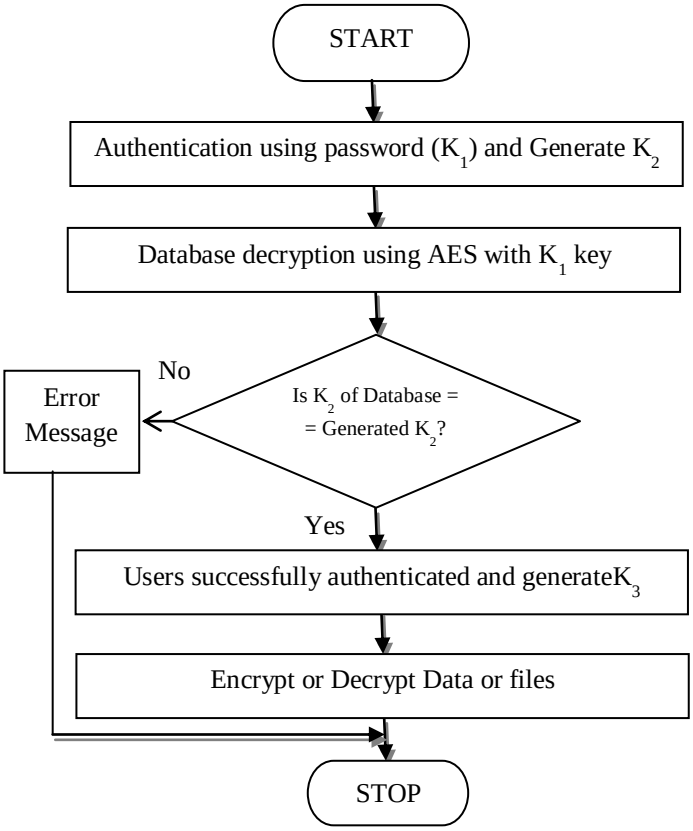

Fig.1. Flowchart of proposed system

The proposed system works in the following way. (Fig.1.) when the authorized user enters the username and password (K_1), this password is converted into hash function (K_2). The database is decrypted using password K_1 and the hash function stored in database is compared with the generated hash function. If the two hash functions are same then the user is authenticated. The user is now able to store the data or files into the storage device and is able to transfer and carry in a secured way. The files stored in this device are stored in an encrypted format. That is why an unauthorized user cannot steal or tamper the data stored in this device.

B. *Soft wares Used*

The soft wares that are used for developing a system that strongly secures the storage devices are .net framework 4.0 and Visual Studio 2010 Express edition as platform, Windows as operating system and C# as language.

C. *MODULES*

The project consists of modules such as:

- Authentication of authorized user using key K_1
- Generation of key K_2
- Decryption of database and comparison of key K_2
- Generation of key K_3
- Encryption and decryption of data or files

1. **Authentication of authorized user using key K_1** . The authorized user enters his/her username and password K_1.

2. **Generation of key K_2-** The key K_1 is converted into hash function i.e. key K_2. This hash function is generated using windows in build function.

3. **Decryption of database and comparison of key K_2** . The generated key K_2 is compared with the key K_2stored in the database. If the keys are same then database is decrypted and user is successfully log-in.

4. **Generation of key K_3** . The key K_3 is generated by using ECDH (Elliptic Curve Diffie-Hellman) algorithm. This is a protocol used for exchanging or sharing a secret key through a non-secure channel. This shared key is taken as the key K_3.

5. **Encryption and decryption of data or files -** The key K_3 is used for encryption and decryption of files using asymmetric encryption and decryption algorithm.

IV. RESULTS

A. GUI of user log-in, file encryption and decryption

The GUI (Fig.2.) consists of username and password text box for entering username and password. It contains the 'Authenticate Data' button which is clicked after entering the username and password. It consists of box named 'List of Files' for listing the encrypted files that are stored in the storage device such as flash drives, SD cards etc. It also consists of buttons for encrypting and decrypting the data.

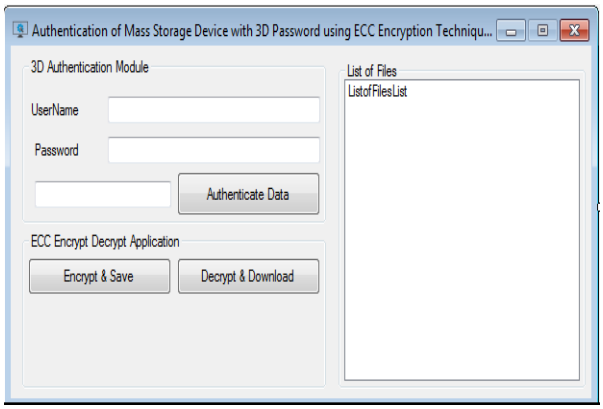

Fig.2. GUI of user log-in, files encryption and decryption

B. User authentication

Enter the name of user and the user's password to do authentication. User is authorized or not is checked. If the user is an authorized user then message is generated for successful login (Fig.3.). The database is encrypted back after the comparison of two keys for authentication.

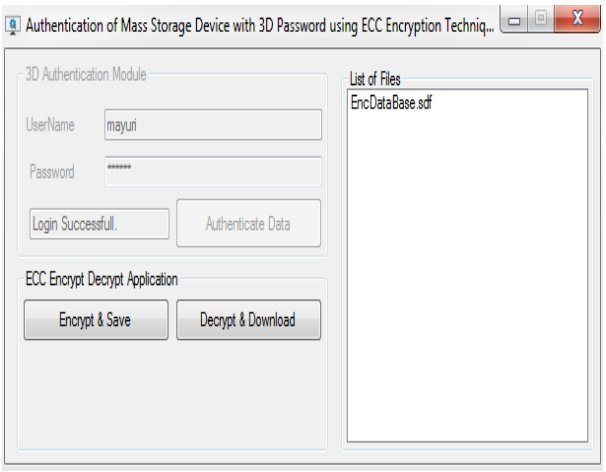

Fig.3. Login Successful

C. Encrypt and save the selected document

For the purpose of encrypting a file click on 'Encrypt & Save' button (Fig.4.). Select the file which is to be encrypted and open it. This selected file is encrypted using ECC encryption algorithm.

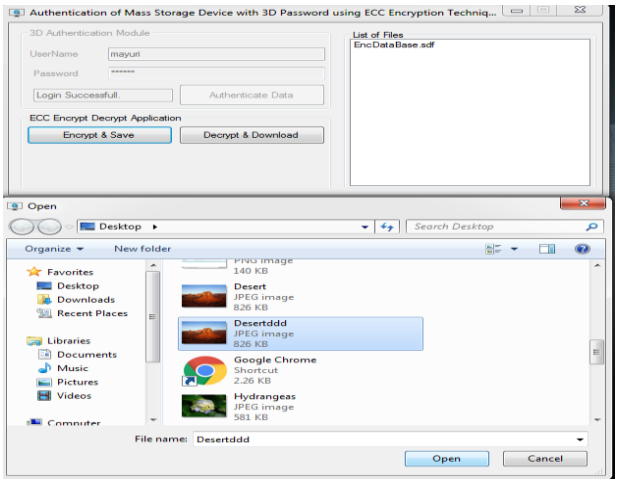

Fig.4. Encrypt and save the selected file 'Desertddd.jpg'

D. Decrypt and download the selectedFile

The file that is stored in the storage device in an encrypted form is decrypted and saved in the other machine. To do so click on 'Decrypt & Download' button(Fig.5.). It will direct to the folder where all the files are stored in an encrypted format inside the mass storage device. Select the file which is to be decrypted and then save it in the desired folder of the machine where the mass storage device is attached. It is necessary to provide the extension to the file. To decrypt ECC decryption algorithm is worked out.

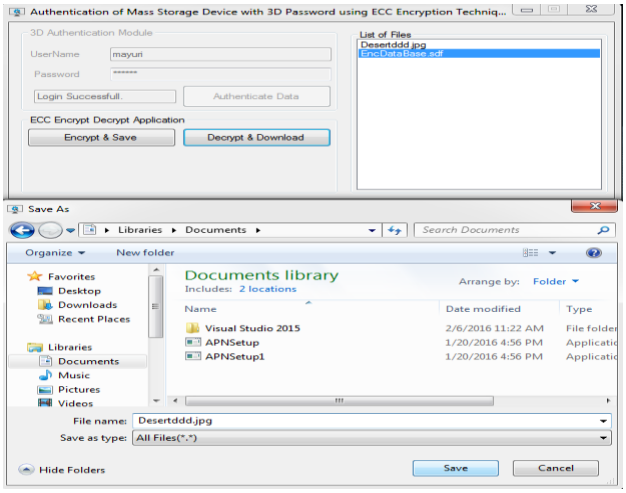

Fig.5. Decrypt and download the selected file 'Desertddd.jpg'

V. CONCLUSION

The proposed system is a software based model. It is a three tier key based model that provides security using three different keys at three different levels. In first level the password is taken as key K_1. This password provides security at a certain level. In second level the database is stored in an encrypted format using key K_2. So that the data stored in the database is not accessed by an unauthorized user. In the third level the files are stored in an encrypted format using the key K_3. Thus the security is tripled. This proposed system is developed for twenty users for a mass storage device.

Future scope for this proposed system is that the users can be increased that is more than twenty.

VI. REFERENCES

[1] Debiao He, Neeraj Kumar, Jong-HyoukLee, 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] A. N. Magdum, Y. M. Patil, "A Secure Data Transfer Algorithm for USB Mass Storage Devices to Protect Documents", International Journal of Emerging Engineering Research and Technology Volume 2, Issue 4, July 2014, PP 78-84.

[3] C. Lee, C. Chen, and P. Wu, "Three-factor control protocol on elliptic curve cryptosystem for universal serial bus mass storage devices," IET Computers and Digital Techniques, vol. 7, no. 1, pp. 48-55, Jan 2013.

[4] Bo CHEN, Chunfang QIN, Ling YU, Ping JIANG, "A Secure Access Authentication Scheme for Removable Storage Media,"Journal of Information and Computational Science, Nov. 2012.

[5] A. K. Das," Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol.5, no. 3,pp. 145-151,Sept. 2011.

[6] Fuw-Yi Yang, Tzung-Da Wu, and Su-Hui Chiu," A Secure Control Protocol For USB Mass Storage Devices", IEEE Transaction on Consumer Electronics, vol.56,no. 4, pp. 2339-2343, Nov. 2010.

[7] D. Hankerson, S. Vanstone, and A. Menezes, "Guide to elliptic curve cryptography," Lecture Notes in Computer Science, 2004.