ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, April 2013

Security For Portable Data Storage media

Nikita Agwankar[1], Dr. Sunil Surve[2], Prof. Sapna Prabhu[3], Radhika Nayak[4]

Student, Electronics Engineering, Fr.Conceicao Rodrigues College of Engineering & Technology,Mumbai, India [1]

Professor- H.O.D.,Computer Engineering, Fr.Conceicao Rodrigues College of Engineering & Technology,Mumbai, India [2]

Associate Professor, Electronics Engineering, Fr.Conceicao Rodrigues College of Engineering & Technology,Mumbai, India [3]

Student, Electronics Engineering, Fr.Conceicao Rodrigues College of Engineering and Technology,Mumbai, India [4]

Abstract*:* Due to the emergence of smart handheld devices, the portable storage market environment is rapidly changing. With the proliferation of these removable media devices there are many problems where personal identifiable information data and corporate confidential affairs are leaked to the public in case of loss, theft, or capture of the portable device. Various kinds of authentication solutions are developed to protect the confidential information against unauthorized access. But after some research, we found that these solutions which were developed to mitigate these threats; have some serious problems as some of them have insecure environment The main objective of this paper is to present the design of an efficient, real-time system to a secure digital flash memory card via hardware. Accordingly, this paper presents a secure user authentication scheme to bypass authentication; enabling the user to block unauthorized access to an entire SD card by establishing a required user authentication for read/write access. To protect the contents from piracy or misuse we provide an application that will encrypt and decrypt the content according to our encryption scheme. Hardware and software security measures implemented in the system defeats any attempts of unauthorized access and maintains ultimate control to protect data and prevent theft. Considering the pitfalls ofexisting security hardware modules we have proposed easy- steps solution which is suitable for most Oss.

Keywords: SD storage media, information storage, system programming, Encryption & Decryption, Data security, protection, access controls, informationflow, confidentiality, flash memory.

I. INTRODUCTION

Use of portable media cards has increased for data transfer and needs protection from unauthorized access and thus the security requirements for such memory devices has become critical. A secure solution that provides more security and user convenience is needed to avoid direct data loss or compromising the security of that data.The secure data not only requires protection during data transfer but also while handling the data at the end user devices. Vulnerability at the end user device, like easy access to the secret keys that are used to encrypt or decrypt the data, can easily turn down the entire security measure. Thus an embedded device must implement methods or protocols for secure data transfer and also should implement security methods to defeat attempts of unauthorized access of secure data from the device [1,2].

To prevent such incidents, a secure SD card solution that provides access of only authorized users to a secured area has been released. Accordingly, this paper presents a secure user authentication method in which it is hard to bypass authentication even after guessing passwords and enables the user to block unauthorized access to an entire SD card by establishing a required password authentication for read/write access. An important and popular methodology for enforcing information security is encryption, which is itself an element of cryptography [5]. Only data encryption may not be an explicit solution to information security problems. Hence hardware and software security measures are implemented in the system to defeat any attempts of unauthorized access to confidential data. The remainder of this paper is organized as follows.

Section 2 analyzes existing methods. Section 3 shows security requirements of a security solution for portable storage. Section 4 suggests a secure solution that provides security and user convenience. Section 5 presents conclusions and future enhancement.

II. BACKGROUND OVERVIEW

This section reviews existing methods such as a secure area, user authentication methods for portable storage and their shortcomings. [2,3,4].

A. Secure Area

The security technology for portable data storage media can be largely divided into hardware and software methods.

1.Hardware method: Only once the user authentication is successful, flash memory can be powered, as a security chip exists between the SD port and memory. The security chip

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, April 2013

provides stronger security using encryption and decryption functions. However, there are vulnerabilities whereby flash memory in the SD memory can be separated and it is possible to bypass authentication to access plain text.

2. Software method: Security programs stored in the virtual CD area provided in a secure USB are performed in the USB or performed in the computer using the secure USB by downloading security programs from the manufacturer's web page. Most security USBs use this method. This method has risks, because malicious third party softwares can easily damage security area information.

B. User authentication

The two primary user authentication methods use biometric information or a password.

1. User authentication using biometric information: A method in which the portable data storage media is equipped with a fingerprint reader can be generally used for authentication. The biometric reader extracts biometric information and stores it in the memory. A subsequent user is authenticated by comparing the input biometric information characteristics to the users. However, a single biometric reader can read only solitary biometric information, such as a fingerprint. The False Acceptance Rate (FAR) measures the probability of which a malicious user is considered to be an authentic user. The users can bypass the authentication process and directly access to the memory. Hence this method fails to provide secure user authentication.

2. User authentication using passwords: A preset password is compared to an entered password for user authentication. The value of the user authentication, which is to be compared to the password that the user enters, is stored as a plain text password in the secure memory, hence the password can be exposed causing the vulnerabilities and the user authentication password can be acquired through attacks.

III SECURITY REQUIREMENTS

Enduring personal information may include name, social security number, code or a character. Such sensitive information must be protected. Personal information may be easily leaked when portable storage, such as SD memory, if lost and stolen. A secure solution for portable storage must meet the following security requirements [3,4,6].

A. Confidentiality

Only a legitimate entity should verify the communication data between PC and SD memory. An attacker must be prevented from learning the nature of the data.

B. Authentication

Only a legitimate user should be allowed to access the secure area of SD memory. User authentication bypass should be impossible.

C. Access Control

Unauthorized entity attempts to access must be preblocked by clearly distinguishing the authorization to read or change information resources in the secure region of SD memory.

D. Efficiency

Service implementation should be facilitated. The implementation cost should be considered for cost effectiveness.

The Aim of this work is to develop a system which will maintain security of the data meeting the above security requirements and to maintain ultimate control to protect data and prevent theft. Achieving a cost effective yet foolproof method to protect the secure data within the device will be a boon to the owner of the contents that needs security.

IV THE PROPOSED SYSTEM

The system is designed to provide a secure authentication such that the Hardware and software security measures implemented in the system defeats any attempts of unauthorized access to retrieve the data and to maintain ultimate control to protect data and prevent theft, by taking care of design metrics as well. For our purposes, an implementation consists of a software, processor with an accompanying program, a connection of processor, or some combination thereof. The system is divided into two units viz. Hardware & Software as shown below (see Figure 1) .

A. Block Diagram

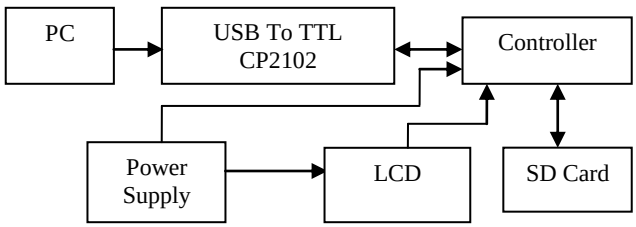

Fig. 1 Block Diagram Representation

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, April 2013

Power supply unit will supply the various voltage requirements of each unit. This unit consists of transformer, rectifier, filter and a voltage regulator. Microcontroller is actually responsible for all the processes being executed. It will monitor & control all the peripheral devices or components connected in the system. The complete intelligence of the project resides in the software code embedded in the Microcontroller. USB To TTL CP2102 is serial converter, connects MCU easily to the computer. This is stable and reliable chipset. It handles handshaking and interfacing signals. The normalSD/ MMC (Data Storage) card is used to store the data. This unit works on SPI (Standard Peripheral Interface) protocol for its communication. It will be interfaced with microcontroller using 4 wire interface. This unit will provide huge amount of non-volatile memory the embedded system.Generalized flow chart of an algorithm is shown here (see Chart 1).The proposed system operates under a different premise. Data must be rendered unreadable if the storage devices are removed from the systems for which they were intended. In the system, the host must maintain ultimate control over security algorithms to protect data. Considering the deployment of various encryption algorithms, this developed algorithm can be as simple as ensuring that the correct storage product is in the host, or as intricate as tying the software and application data directly to the storage device. User will insert the card and will enter two passwords; storing password and encryption password. From our research it has been found that some systems are restricted to the messages/ files stored in their databases. But in our system the user can select any file to be stored or just type the desired message on the screen. From storing password base address is calculated. By Ex-oring the encryption password with message/ file contents; the plain text will be converted into encrypted text (see Chart 2). We can allow each letter of the alphabet to shift independently by defining shift values in the function. This encrypted data will be sent to the hardware which will store the information in the Standard Capacity Memory SD card. Hence the data is secured and no one will be able to retrieve it without the same hardware & software combination along with the passwords. In addition to this the information or file will not be visible by any operating system or card reader, so the erasure or modification of the data is prevented. The basic transfer scheme used here is a communication used by the application that carry out the device's purpose which occurs when the host exchanges the data that performs the function the device is designed for.

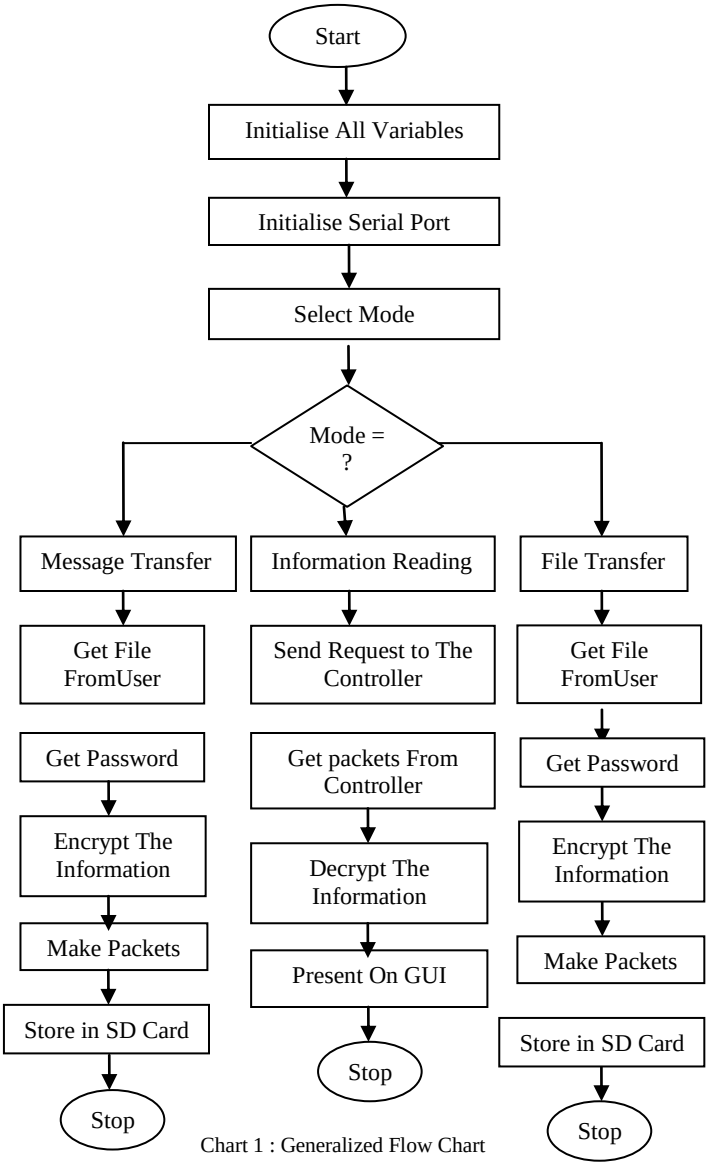

Chart 1 : Generalized Flow Chart

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, April 2013

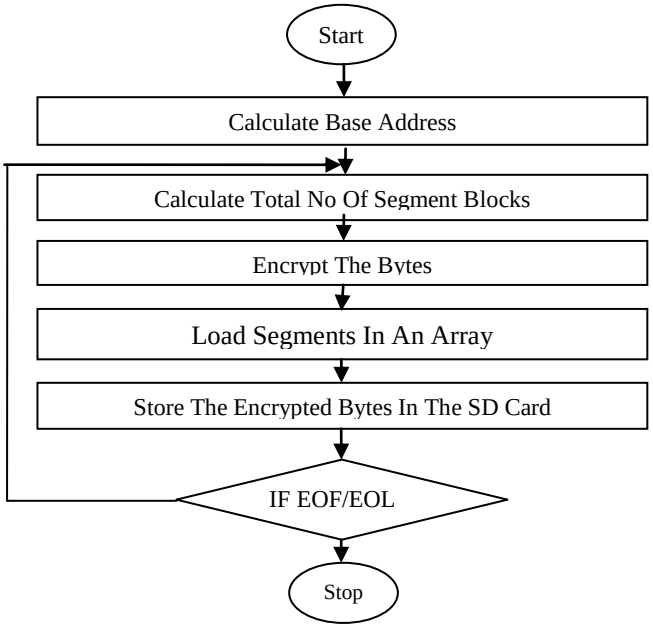

Chart 2 : Flow Chart For Information Storing

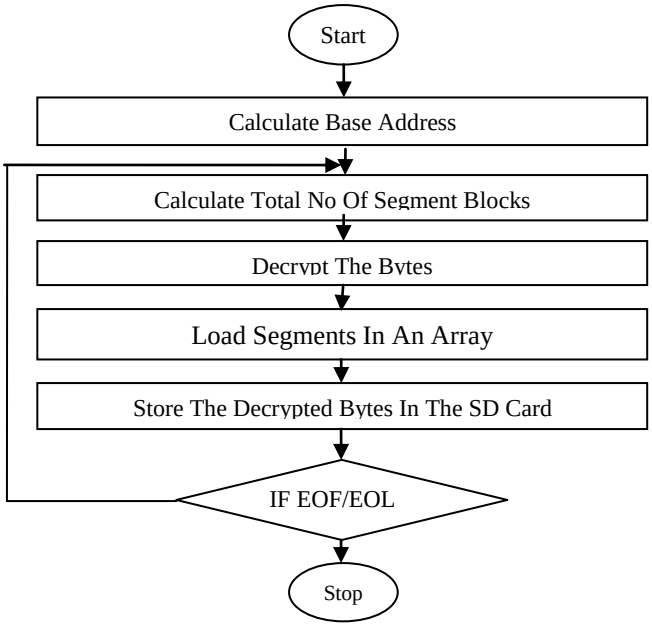

Chart 3 : Flow Chart For Information Reading

V CONCLUSIONS

The objective of this work is to prevent a malicious third party leaking personal information when portable storage such as SD card is robbed or lost. This proposed method can overcome the existing method's weakness. The method meets the security requirements in section 3. A login GUI is designed to prevent unauthorized user from invading. Security Levels are increased. The values of parameters are set by user, which means that the passwords are only known by the user himself. Most importantly; it is hard to bypass authentication even after guessing passwords. The proposed easy- steps solution is suitable for most Oss. Future improvements can be done in following mentioned ways.

- Instead of SD Card USB can be used,
- Any type of files can be stored,
- Large file support can be integrated,
- Data transfer rate can be increased.

REFERENCES

[1] "Security needs in embedded systems", Anoop MS Tata Elxsi Ltd. India.

[2] Marwan AlZarouni School of Computer and Information Science Edith Cowan University,"The Reality of Risks from Consented use of USB Devices", Australian Information Security Management Conference Security Research Centre Conference 2006.

[3] Sun-Ho Lee, Kang-Bin Yim, Im-Yeong Lee, "A Secure Solution for USB Flash Drives Using FAT File System Structure", IEEE 2010 13th International Conference on Network-Based Information Systems.

[4] Srivaths Ravi and AnandRaghunathan NEC Laboratories America Paul Kocher Cryptography Research and Sunil Hattangady Texas Instruments Inc, "Security in Embedded Systems: Design Challenges," *ACM Transactions on Embedded Computing Systems*, Vol.3, No.3, August 2004

[5] "Essential security requirements on USB storage" , KISA, 2007.

[6] Adedayo M. Balogun, Shao Ying Zhu, School of Computing and Mathematics, University of Derby, Derby, United Kingdom, "Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.5, 2013

[7] Koh Chan, Park Youn, "Enhancement of Secourity Function on USB Memory Driver by Reserved Sector Storage Structure Technique", Journal of the Korean Society for Industrial and Applied Mathematics, 2005, vol.9, pp. 1-14

[8] MajidSarrafzadeh, FoadDabiri, RoozbehJafari, Tammara Massey, AniNahapetan , "Low Power Light-weight Embedded Systems", ISLPED'06, October 4–6, 2006, Tegernsee, Germany.

[9] Book Embedded System Design - A Unified HardwareSoftware Approach.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 1, April 2013

[10] "USB Complete: Everything You Need to Develop USB Peripherals", Third Edition by Jan Axelson Copyright 1999-2005 by Janet L. Axelson.

[11] "Designing Robust Security Options For Embedded Systems", White paper SliliconAdvanced Storage Technology System.

[12] HanjaeJeong, Younsung Choi, WoongryelJeon, Fei Yang, Yunho Lee, Seungjoo Kim, Dongho Won Information Security Group, Sungkyunkwan University 300 Cheoncheon-dong, Jangan-gu, Suwon, Gyeonggi-do, 440-746, Korea, "Vulnerability Analysis of Secure USB Flash Drives", 978-1-4244-1656-1/07/$25.00 ©2007 IEEE.

[13] Abu Asaduzzaman, Muhammad F. Mridh, M. NazimUddin, "An Inexpensive Plug-and-Play Hardware SecurityModule to Restore Systems from Malware Attacks" ,978-1-4799-0400-6/13/$31.00 ©2013 IEEE

[14] Chunlei Wang, Guangyi Wang, Yue Sun and Wei Chen,"ARM Realization of Storage Device Encryption Based on Chaos and AES Algorithm", 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications.

[15] Faith M.HeikkilaPivot Group Security Consultant "Encryption: Security Considerations for Portable Media Devices", IEEE SECURITY & PRIVACY.

[16] Annette Tetmeyer, HosseinSaiedian, IEEE Technology And Society Magazine Winter 2010, 1932-4529/10/$26.00©2010IEEE.

[17] Cheng-Wei Peh, Vee-Khee Wong, and Ying-Khai The, "Development of an Indoor Environment Monitoring System with Secure Digital (SD) Card Storage",Proceedings of the 2010 [EEE Conference on Sustainable Utilization and Development in Engineering and Technology UniversitiTunku Abdul Rahman 20 & 21 November 2010, Faculty of Engineering, Kuala Lumpur, Malaysia.