Highly Secure Data Chip for Highly Sensitive Data

Bhushan Kumawat¹, Shreya Turbadkar², Jay Mhatre³, Asst. Prof. Pratap Nair⁴

¹,²,³ Student, K.C. College Of Engineering, Management Studies & Research, Thane-400603, Mumbai
⁴ Assistant Professor, Dept. of Computer Engineering, K.C. College Of Engineering, Management Studies & Research, Maharashtra, India

Abstract - Secure capacity of information and the present accessibility of information and data are the most vital parts of any ICT (Information and Communications Technology) framework. Information stockpiling frameworks are compulsory segments of present day data frameworks. It is a Smart chip, while concentrating on security guarantees that ensuring individual and corporate information. We will utilize both Hardware and Software mix security for information putting away.

Key Words: MMC Storage Media, Data Security, Information Storage, System programming, Arm processor.

1. INTRODUCTION

In the software security, we can utilize Data Encryption and Decryption Phases. The greater part of the general population can utilize Internet while exchanging imperative information over the Net. Starting with one spot then onto the next spot, we can exchange the information utilizing Encryption and Decryption process. In any case, there are some unapproved and malevolent software engineer; Hacker can follow your imperative information or message from another side.

In this way, we utilize both Hardware and Software Combination where we utilizes Hardware as Memory Card for secure information putting away and furthermore utilizes Software as the Encryption and Decryption stage. In reality, we will build up a framework where critical information, message or data can be escaped unapproved clients. Which implies where we use memory card as a verified information, which will be covered up inside this card. In the past framework, information was seen by everybody and just uses username and secret word. Nevertheless, we will concealed this data by tossing the information inside the memory card.

In the memory card, there are number of Fact tables where information is store successively. In any case, we utilizes implanted C as a programming language to change the capacity of putting away data in the memory card. We will build up our own Fact tables where information will not store as consecutive way. In this manner, while figuring the data of “The amount Memory is full?” it will dependably demonstrates that no information and envelope is vacant.
Just those are approved clients they can alter the records utilizing gave username and secret key.

The proposed framework will utilize SD/MMC cards for verified information stockpiling. The framework will be separated into two units’ viz. Equipment and Software. The Hardware will have an attachment for embedding the SD/MMC card. It will be associated with the PC utilizing sequential port. The product will have the UI for document or message putting away. Client will embed the card and will simply enter the "Putting away Password" and "Encryption Password". At that point, he/she can choose a record to be put away or simply type the ideal message on the screen. In the wake of squeezing the transfer catch, it will be sent to the equipment, which will store the data in the card. Now the information is verified and no one will most likely recover it without a similar equipment and programming mix alongside both the passwords. Again, the data or document will not be noticeable by any working framework or card reader.

3.1 System Overview

The following diagram shows the overall working of the proposed system.

3.2 Block Diagram

3.3 Explanation of System

Efficiently technique or Overview of the proposed framework we will create is appeared above diagram:

- In the framework, we will utilizes SD/MMC Card attachment for interfacing between memory cards as an outer equipment. Where information is store by utilizing Fact table where we build up our own Fact tables for putting away information. We will toss our information data anywhere in the memory card as not in consecutive way. Due to that information figuring going to fall flat.

- Microcontroller will use as the primary arrangement of our significant undertaking. In that, we can say it is a primary program of our framework. Where we can compose our programing language in Embedded C, run our program. Microcontroller go about as a controller of the Hardware and Software framework.

3.3 GUI of our Proposed System

Fig-3: Hardware Design

Fig-4: Front End
In this front end, we can format, read messages, store messages, read files, and store files. These functions are most important to edit our sensitive files.

We can add encryption passwords for storing messages and files because we can change the memory value which will be hidden and not get the original file. It will be encapsulated in the encryption manner.

Suppose an unauthorized user tries to open your data, then it shows format disk as shown in the following figure:

![Pop Up Message to Format Disk](image)

**Fig-5: Pop Up Message to Format Disk**

### 4. SYSTEM OVERVIEW DIAGRAM

The following diagram shows the real-time working of our framework/system:

![Real Time Overview](image)

**Fig-6: Real Time Overview**

### 4.1 Features of the System

- **Username and Password Provided for Authorized Client as an Authentication stage.**
- **Both Hardware and Software Blend Function as a Noteworthy Job of the Framework.**
- **Memory Card Where Information is Covered Up.**
- **Memory Demonstrating Empty Folder for Unapproved Clients.**
- **Arm-Processor Use as an Interfacing Among Hardware and Software Frameworks.**

### 4.2 Technologies Used

We used a combination of hardware and software both as follows:

- **For Hardware System**
  - Arm-Processor
  - SD/MMC Card Socket
  - Memory Card

- **For Software System**
  - .net Programming Language
  - Visualization of Interfacing in .net
  - Embedded C for Hardware Programming

### 4.3 Future Scope & Its Applications

- **This System is Especially Valuable in Future Extension.**
- **Military Important Data**
- **Secure Correspondence Between Big Companies**
- **Private Information of Industries**
- **As a Major Future Upgrade Is That, Where We Will Endeavor to Conceal Our Critical From Our PDA**

We will endeavor to build up a framework for future extension as a protected correspondence and exchanging information starting with one spot then onto the next as a safe way. This framework will be security based on account of undetectable of information no one discovers our covered up secure information and track our information at whatever point it loses or hack by anybody.
5. CONCLUSION

By the acknowledgment of the above-proposed framework, one can learn numerous parts of an advanced hardware circuit. This will give the total knowledge of planning arm-processor based system and creating implanted programming. We will likewise get familiar with the product advancement methodologies and different programming strategies for PC based applications.

REFERENCES

[1] "Development of Secured Military Data Storage Media", 2012-2013 July


