

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 will utilize Read and Write access for information in equipment framework then again we additionally can apply approved username/Id and Password for programming framework where our Data will be more verified and shielded from unapproved people or Hackers.

Our point is to grow such a framework, which can utilize both programming and equipment assurance highlights for information stockpiling media.

Main aim is that hide the sensitive data and information from unauthorized users. Unauthorized users cannot have access to get the data because it will be hidden.

While sensitive data will hide unauthorized user or hacker doesn't do anything in the memory.

2. BACKGROUND OVERVIEW

2.1 Existing System

- ▶ Now a days Transferring or taking tied down Data starting with one spot then onto the next is the prime prerequisite of the considerable number of organizations, Industries, Institutes, Laboratories and so forth.
- ▶ Fundamental strategies to do as such are either to encode or Zip the Data by one or other programming and exchange it by Internet or store the Data in any equipment to convey.

2.2 Limitations of Existing System

- ▶ We as a whole know that exchanging the Data through Internet is not full Proof or can be hacked.
- ▶ Information exchange by the methods for regular durable goods like Pen drive, hard circle drives, CDs, DVDs and so on can be gotten too effectively.

3. PROPOSED SYSTEM

In the proposed framework, we can utilize both equipment and programming mix. 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.

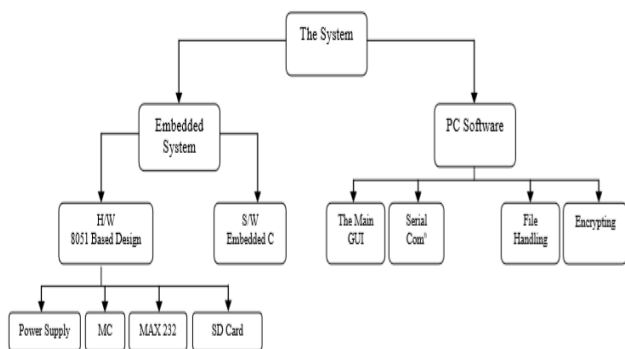


Fig-1: Hardware & Software Flow

3.2 Block Diagram

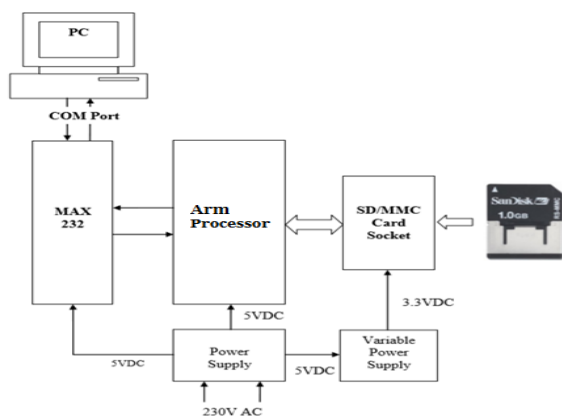


Fig-2: Block Diagram of Proposed System

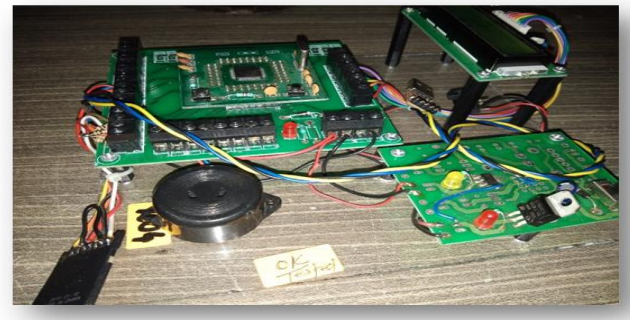


Fig-3: Hardware Design

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 utilize SD/MMC Card attachment for interfacing between memory cards as an outer equipment. Where information is stored 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 out will 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 programming language in Embedded C, run our program. Microcontroller goes about as a controller of the Hardware and Software framework.

3.3 GUI of our Proposed System

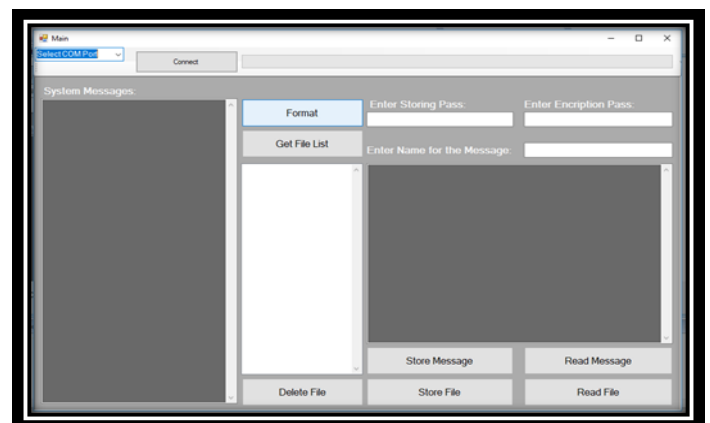


Fig-4: Front End

In this Front end we can Format, Read Message, Store Message, Read File & Store File this functions are most important to edit the our sensitive files.

We can adding encryption password for storing message and file because we can change the memory value which will be hidden and not get original file. It will be encapsulate the original data in the encryption manner.

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

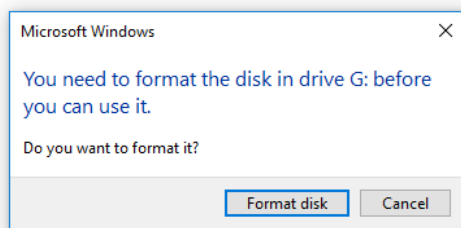


Fig-5: Pop Up Message to Format Disk

4. SYSTEM OVERVIEW DIAGRAM

The following diagram shows the real time working of our Framework/System:

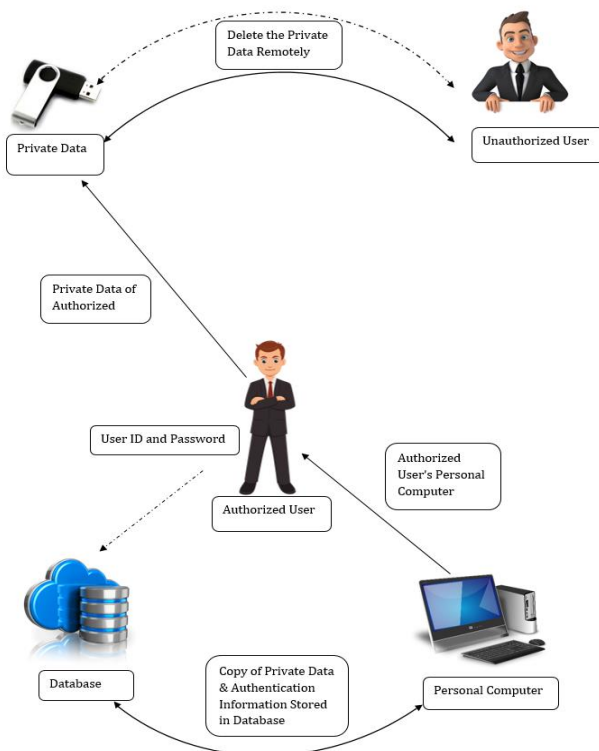


Fig-6: Real Time Overview

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 are used combination of hardware and software both are 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 discover 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
- [2] Adesh Kumar, Piyush Kuchhal, Sonal Singhal, "Secured Network on Chip (NoC) Architecture and Routing with Modified TACIT Cryptographic Technique", 2015
- [3] "Big Data and Database Security", 2017
- [4] "Smart Card based Robust Security System", 2013
- [5] "Security and Privacy –A Big Concern in Big Data A Case Study on Tracking and Monitoring System", 2017
- [6] Venus638FLPx GPS Receiver, SkyTraq Technology, Inc. www.skytraq.com.tw, empower mobility, without uncertainty, Information of GPS
- [1] Sunil Upadhyay "Digital Communication", , <http://students.iitk.ac.in/eclub/assets/lectures/embedded14/comm.pdf>.