Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Smart Card for Smatter Access

Bhimani Kaushal[1], Hingrajiya Milan[2], Kamaliya Vishal[3], Kaneriya Jay[4]

Students, CSE, SLTIET, Rajkot, Gujarat, India

[1]Computer Science & Engineering, SLTIET

[2]Computer Science & Engineering, SLTIET

[3]Computer Science & Engineering, SLTIET

[4]Computer Science & Engineering, SLTIET

Abstract—*today, smart cards are widely used in variety of applications of human life. We demonstrate how 1-of-n encoded speed-independent circuits provide a good framework for constructing smart card functions that are resistant to side channel attacks and fault injection. A novel alarm propagation technique is also introduced. Smart Cards are secure portable storage devices used for several applications especially security related ones involving access to system's database either online or offline. Moving from special-purpose operating systems with single application into multi-purpose operating systems with open architecture, is proof of claim. A smart card is a card with a microchip embedded in it. The evolution of smart card technology provides an interesting case study of the relationship and interactions between securities. For the future of smart card to be bright, it is important to look into several aspects and factors especially those resulted due to the rapid advancement in information and communication technology. The embedded chip, however, empowers the card to be useful in a variety of environments.*

***Keywords*— Smart Cards Operating System and they Application, File Management System, Hardware Architecture, Security, Smart Card Reader**

I. INTRODUCTION

Smart Card is a fully functioning computer system built on a single chip (integrated circuit). This computer system has important similarities and differences from other kinds of traditional. The big question is what type of smart cards the banks will issue. Will they require Smart cards are far more secure than traditional credit cards, which store account information? These cards take the form of either "contact" cards that require a card reader or "contactless" cards which use Digital signals to operate. Smart card is a plastic card with size of credit cards (about 5/5 on 8/5 cm) that has embedded memory chips and processor for data storage and processing [1]. Ability to provide security and ease of use are the most important reason for extension of smart card usages in different domains, these cards can processing and storing significant volumes of data. Smart cards and secure elements are the basis for many secure systems and play a decisive role in ID management [2].

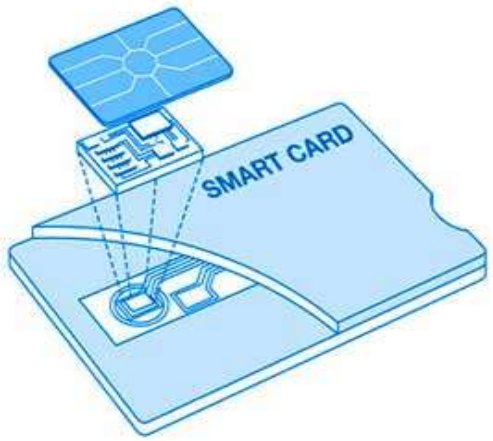

Fig. 1 A sample chip displayed [4]

Smart card operating system is a set of codes which are executed on the card processor and is responsible for memory Management, data exchange, instruction execution and cryptographic algorithms management [3]. Smart cards, also known as IC cards, are portable information media, having the size of about a credit card. They comprise an integrated card controller, or at least an integrated memory, for a data exchange with a respective appliance. Smart card provide data portability, security, convenience and the like

Memory and microprocessor- Memory cards simply store data and can be viewed as a small floppy disk with optional security. A microprocessor card, on the other hand, can add, delete and manipulate information in its memory on the card. A range of private and governmental organisations have played an important role in the development, promotion, and wide-scale deployment of smart cards.

II. Related Work

Smart card implementations are typically based on the set of international standards. Although these standards are elaborate and address every aspect of smart card implementations, it was considered necessary to specify some of the finer details more elaborately and do away with any ambiguity before any smart card application was undertaken by the Government of India. IIT Kanpur also developed the first SCOSTA compliant OS in 2001 for smart cards which was used for the National transport application [5]. This OS was, however, limited in its functionality to the requirements of contact smart cards. The SMART CARD compliant OS was subsequently enhanced for compliance to contactless smart cards with support for secure messaging to avoid the possibility of eavesdropping.

Most Smart Cards are currently programmed in low-level languages based on proprietary Smart Card operating systems. Some of the programming has been done in the chip's native instruction set (generally Motorola 6805, Intel 8051, or Hitachi H8). Though this results in highly efficient code, it is much more difficult to program than higher-level languages. The number of programmers who could do this type of programming is quite limited [6].

III. Classification

The The SCSA card is very effective. Main advantage of this system is too many card include to only one card. Will they require a Smart cards are far more secure than traditional credit cards, which store account information unencrypted on a magnetic stripe these next-generation cards encrypt and store that data on an embedded microchip that generates a new code for each transaction So even if your credit card number is stolen, it's nearly impossible for a criminal to create a counterfeit card.

Smart Card is a fully functioning computer system built on a single chip. If a program is added in ROM, it must be added when the basic chip is manufactured, and no changes can be made to it. If programs are added to EEPROM. Most Smart Cards are currently programmed in low-level languages based on proprietary Smart Card operating systems. Security generally has a cost, in money, time to market, and Smart Card markets are very price sensitive. The user requirements may be well known and have high security needs, such as those for the Secure Application Module implemented on a Smart Card in some stored value systems it is now managed by Global Platform, a new consortium intended to promote Open Platform beyond banking uses. Open Platform is an architecture and sets standards to define and manage dynamic multi-application Smart Cards. The vision of smart card as an application platform rather than a simple security token is a paradigm shift for smart card operating systems. Performance and speed are very important factors that need to be considered in most smart card application. To achieve this, transistor scaling or the reduction of the gate length must be taken into consideration

VI. Analysis

The user have store many card in pocket. Many card is required more space for store. So we made this smart card. Smart cards have also been the targets of security attacks. These attacks range from physical invasion of the card's electronics, to non-invasive attacks that exploit weaknesses in the card's software or hardware.

VI. Acknowledgment

We would like to extend our gratitude to our respected teacher – Mr. Krunal Vasani, for his constant support and for imparting us with the knowledge and helping us throughout the paper.

VI. Conclusion and Future Works

Smart Card is a fully functioning computer system built on a single chip (integrated circuit). This computer system has important similarities and differences from other kinds of traditional. In day-to-day life we use district cards for providing various services. One day a scientist get idea for smart card which is use as stand for all other cards as well as new features and modified service will also include. Technology: Build allied infrastructure (like reader terminals) and improve its penetration across cities. Work towards educating customers on the extent of application of smart cards across user segments and governing bodies. Main advantage of this system is too many card include to only one card. Will they require a Smart cards are far more secure than traditional credit cards, which store account information unencrypted on a magnetic stripe these next-generation cards encrypt and store that data on an embedded microchip that generates a new code for each transaction?

REFERENCES

[1] G. Selimis, A. Fournaris, G. Kostopoulos, and O. Koufopavlou, "Software and Hardware Issues in Smart Card Technology", COMMUNICATIONS SURVEYS & TUTORIALS, IEEE, Vol. 11 (3), PP. 143-152, 2009.
[2] 13th Smart Card Research and Advanced Application Conference November 5-7, 2014 • Paris, France
[3] W. Rankl, and W. Effing, *Smart Card Handbook*, 4th edition, Wiley Publishing, 2010.
[4] Image:- http://www.observatoriotui.com/images/r5png.png
[5] IIT Kanpur and NIC India, SCOSTA-CL Specications v1.2: Specications for the Smart-Card Operating System with Contact-less Interface, Version 1.2 Available at http://www.scosta.gov.in India, July 2007
[6] IDRBT's Working Paper No. 6 A Framework for Smart Card Payment Systems - Ashutosh Saxena and Aditya Gaiha 1.5 Programming Languages