A Review on Smart Card

Viraj Deokar[1] Prof. Prathibha Adkar[2]
[1,2]Department of MCA
[1,2]Savitribai Phule Pune University/Modern College of Engineering Pune-05, India

Abstract— Smart card is a secure portable storage device used in several applications. It is important to look into various aspects and factors those related in information and communication technology. This paper gives details about what is smart card, architecture of smart card, need of using the smart card, survey on the smart card, component of the smart card, its interaction and applications, comparison with other system.

Key words: Architecture, Components, Interaction, Types, Application's

I. INTRODUCTION

A smart card, typically a type of chip card, is a plastic card that contains an embedded computer chip–either a memory or microprocessor type–that stores and transacts data. This data is usually associated with either value, information, or both and is stored and processed within the card's chip. The card data is transacted via a reader that is part of a computing system. Systems that are enhanced with smart cards are in use today throughout several key applications, including healthcare, banking, entertainment, and transportation. All applications can benefit from the added features and security that smart cards provide. Markets that have been traditionally served by other machine readable card technologies, such as barcode and magnetic stripe, are converting to smart cards as the calculated return on investment is revisited by each card issuer year after year.

Smart card is called 'smart' because it contains a computer chip. Indeed, smart card is often referred to as 'chip card' or 'integrated circuit card'. The smart card looks like a credit card but acts like a computer. Without realizing it, smart cards have become a very important part of human's life. Smart cards are secure devices that enable positive user identification and they are multi-functional, cost effective devices that can be easily adapted for both physical and logical access. Logical access control concerns such familiar principles as password checking or the more sophisticated cryptographic mechanisms for authentication such as windows logon, virtual private network (VPN) access, network authentication, biometric storage and others. Physical access control relates to ID badges and building access control. Importantly, smart cards technology includes a wide range of applications and additional physical forms, than just plastic cards.

A. Why Smart Cards

Smart cards improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart card systems have proven to be more reliable than other machine-readable cards, like magnetic stripe and barcode, with many studies showing card read life and reader life improvements demonstrating much lower cost of system maintenance. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. The costs to manage password resets for an organization or enterprise are very high, thus making smart cards a cost-effective solution in these environments. Multifunction cards can also be used to manage network system access and store value and other data.

Smart cards can also act as keys to machine settings for sensitive laboratory equipment and dispensers for drugs, tools, library cards, health club equipment etc. In some environments, smart card enabled- SD and microSD cards are protecting digital content as it is being delivered to the mobile hand-sets/phones.

Security is very crucial issue in smart card especially due to the various independent parties involve throughout the card's life cycle leading to what is now called "splits" in trust. There is need to develop a method in which even without trust none of the parties can cheat one another. Further, to overcome the lack of security provided by passwords or PINs for authentication and access control, some researchers believe that biometric is the best genuine means of authentication. However, due to the significant amount of processing and memory capacity required by this approach, implementing it in smart card remains difficult. Hence, this area needs to be further evaluated to make it suitable for built-in smart card applications. Other important security issues involve further investigation of elliptic curve and quantum cryptography on smart cards.

II. LITERATURE SURVEY

A survey completed by Card Technology Magazine (http://www. cardtechnology.com) indicated that the industry had shipped more than 1.5 billion smart cards worldwide in 1999. Over the next five years, the industry will experience steady growth, particularly in cards and devices to conduct electronic commerce and to enable secure access to computer networks. A study by Dataquest in March, 2000, predicts almost 28 million smart card shipments (microprocessor and memory) in the U.S. According to this study, an annual growth rate of 60% is expected for U.S. smart card shipments between 1998 and 2003. Smart Card Forum Consumer Research, published in early 1999, provides additional insights into consumer attitudes towards application and use of smart cards. The market of smart card is growing rapidly due to its wide range of applications.

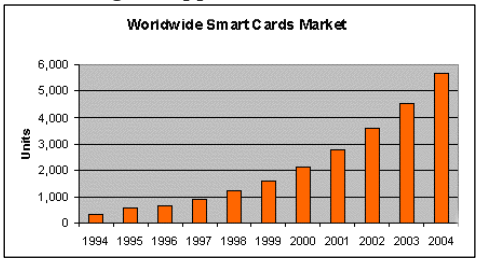

Fig. 1: Smart card Market

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 (the size of the switch that turns transistors on and off), must be taken into consideration. This idea not only improves the performances of chips but also lowers their manufacturing cost and power consumption per switching event. Recently, IBM have built a working transistor at 6 nanometres in length which is per beyond the projection of The Consortium of International Semiconductor Companies that transistors have to be smaller than 9 nanometres by 2016 in order to continue the performance trend.

In the future, smart cards could handle multiple tasks for their owners, from providing access to company networks, enabling electronic commerce, storing health care information, providing ticketless airline travel and car rentals, and offering electronic identification for accessing government services such as benefit payments and drivers licenses etc. Smart cards of the future may even stop resembling "cards" as smart card technology is embedded into rings, watches, badges, and other forms and factors that will make them remarkably convenient to use. In the near future, we believe all PC's and Network Computers will be integrated with smart card readers. These can be implemented either as part of the keyboard or occupying one of drives or perhaps as an external units. It is hoped that the smart card of the future will be a PC in pocket size with sensors for biometric features and a human interface.

Information and entertainment is being delivered via satellite or cable to the home DVR player or cable box or cable-enabled PC. Home delivery of service is encrypted and decrypted via the smart card per subscriber access. Digital video broadcast systems have already adopted smart cards as electronic keys for protection. Smart cards can also act as keys to machine settings for sensitive laboratory equipment and dispensers for drugs, tools, library cards, health club equipment etc. In some environments, smart card enabled-SD and micro SD cards are protecting digital content as it is being delivered to the mobile hand-sets/phones.

Security is very crucial issue in smart card especially due to the various independent parties involve throughout the card's life cycle leading to what is now called "splits" in trust. There is need to develop a method in which even without trust none of the parties can cheat one another. Further, to overcome the lack of security provided by passwords or PINs for authentication and access control, some researchers believe that biometric is the best genuine means of authentication. However, due to the significant amount of processing and memory capacity required by this approach, implementing it in smart card remains difficult. Hence, this area needs to be further evaluated to make it suitable for built-in smart card applications. Other important security issues involve further investigation of elliptic curve and quantum cryptography on smart cards.

III. SMART CARD ARCHITECTURE

Smart Cards are thin cards with an embedded chip, and this automatically poses its own unique challenges of architectural design. However, it turns out that the solutions tend to be a scaling down of conventional chips rather than inventing an all-new chip.

A. Central Processing Unit

Traditionally this is an 8-bit microcontroller but increasingly more powerful 16 and 32-bit chips are being used. However, none have multi-threading and other powerful features that are common in standard computers. Smart Card CPUs execute machine instructions at a speed of approximately 1 MIPS. A coprocessor is often included to improve the speed of encryption computations.

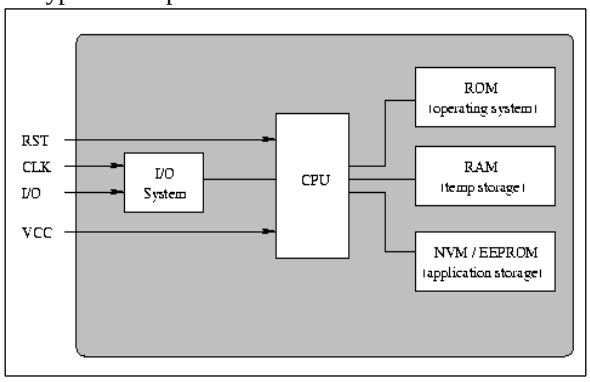

Fig. 2: Architecture of Smart Card

B. Memory System

There are three main types of memory on cards:

1) 1.RAM. 1K.This is needed for fast computation and response. Only a tiny amount is available.
2) 2.EEPROM (Electrically Erasable PROM).Between 1 to 24K. Unlike RAM, its contents are not lost when power is. Applications can run off and write to it, but it is very slow and one can only read/write to it so many (100 000) times.
3) 3. ROM. Between 8 to 24K. The Operating System and other basic software like encryption algorithms are stored here.

C. Input and Output

This is via a single I/O port that is controlled by the processor to ensure that communications are standardized, in the form of APDUs (A Protocol Data Unit).

D. Interface Devices (IFDs)

Smart Cards need power and a clock signal to run programs, but carry neither. Instead, these are supplied by the Interface Device - usually a Smart Card Reader - in contact with the card. This obviously means that a Smart Card is nothing more than a storage device while being warmed in your pocket. In addition to providing the power and clock signals, the reader is responsible for opening a communication channel between application software on the computer and the operating system on the card. Nearly all Smart Card readers are actually reader/writers, that is, they allow an application to write to the card as well as read from it.

The communication channel to a Smart Card is half-duplex. This means that data can either flow from the IFD to the card or from the card to the IFD but data cannot flow in both directions at the same time. The receiver is required to sample the signal on the serial line at the same rate as the transmitter sends it in order for the correct data to be received.

This rate is known as the bit rate or baud rate. Data received by and transmitted from a Smart Card is stored in a buffer in the Smart Card's RAM. As there isn't very much RAM, relatively small packets (10 - 100 bytes) of data are moved in each message. Here is a selection of parameters from some of the smart cards on the market today. They are neither the biggest nor the fastest; that is reserved for Java cards. The reason for this is price --- smart cards like these are programmed in assembly language and do not need much in the way of resources. To keep down costs, they don't get resources.

Smart Card	Word size	ROM	EEPROM	RAM	Voltage	Clock	Write/erase cycles	Transmission rate
Infineon SLE 44C10S	8-bit	9K	1K	256b	2.7 - 5.5V	5 MHz	500 000	9600 baud
Orga ICC4	8-bit	6K	3K	128b	4.7 - 5.3V		10 000	
GemCombi	8-bit		5K		4.5 - 5.5V	13.6 MHz	100 000	106 kbaud
DNP Risona	8-bit		1K		5V	3.5 MHz		9600 baud
AmaTech Contactless	8-bit		1K		5V	13.6 MHz	100 000 cycles	
Schlumberger Cyberflex	8/16-bit	8K	16K	256b	5V	1-5 MHz	100 000 cycles	9600 baud

Table 1: Selection of Parameters

E. Operating Systems

The operating system found on the majority of Smart Cards implements a standard set of commands (usually 20 - 30) to which the Smart Card responds. Smart Card standards such as ISO 7816 and CEN 726 describe a range of commands that Smart Cards can implement. Most Smart Card manufacturers offer cards with operating systems that implement some or all of these standard commands (and possibly extensions and additions). The relationship between the Smart Card reader and the Smart Card is a master/slave relationship. The reader sends a command to the Smart Card, the card executes the command and returns the result (if any) to the reader and waits for another command.

Microsoft released a miniaturized version of Windows for Smart Cards in late 1998, and early versions of a Gnu O/S have been released.

F. File Systems

Most operating systems also support a simple file system based on the ISO 7816 standard. A Smart Card file is actually just a contiguous block. Files are organized in a hierarchical tree format. Once a file is allocated, it cannot be extended and so files must be created to be the maximum size that they are expected to be. Each file has a list of which parties are authorized to perform which operations on it. There are different types of files: linear, cyclic, transparent, SIM, etc. The usual create, delete, read, write and update file operations can be performed on all of them. Certain other operations are supported only on particular types of files.

Type	Special Operations	Example
Linear	Seek	credit card account table
Cyclic	read next, read previous	transaction log
Transparent	read and write binary	Picture
SIM file	encrypt, decrypt	cellular telephone

Table 2: File System

G. Software

Smart Cards are either Soft-Mask or Hard-Mask, depending on whether most of the application is in EEPROM or ROM. Hard-Mask cards are more expensive. Some application-specific data/instructions always needs to be stored on EEPROM. Cards do not as a rule run anything off RAM.

When programming a Smart Card, it is standard practice to get the program running on a simulator first for debugging, since EEPROM can only be written to a finite number of times in its lifetime.

Test-running also happens on a different level: banks commonly use a soft mask card for pilot testing new applications and then to move on to more customer-resistant hard mask cards for larger deployments. However, some applications have limited deployments that are never taken to hard mask, as hard masking is expensive in both time and money. Hard masks also may not be justified for some applications, such as an employee identification card for small companies.

H. Programming Languages

Most SmartCards are currently programmed in low-level languages based on proprietary SmartCard operating systems. Some of the programming has been done in the chip's native instruction set (generally Motorola 6805, Intel 8051, or Hitachi H8). Not many programmers are capable of this.

IV. THE COMPONENTS OF SMART CARD

A. Smart Card Memory and chip

Smart card chips contain a microprocessor and/or memory. They are embedded in smart cards and in portable devices that resemble credit cards but are used in applications such as banking and health care. Although the term “smart card” is used to describe any card that can relate information to an application, passive devices such as magnetic stripe cards, optical cards, and memory cards can only store information or complete predefined operations. By contrast, smart cards with embedded microprocessors contain all of the information and functions needed to complete transactions. Known as “chip cards," these microprocessor-based devices do not require access to remote databases and they can perform a dynamic series of complex calculations. Although smart card chips that include both a microprocessor and

memory offer the greatest degree of versatility, the majority of smart cards are memory-only devices

Fig. 3 Smart Card with Memory Chips

Smart Cards based on their Functionalities and Configuration

B. Memory Cards

Memory cards consist of memory circuits. It can perform the following operations: store, read and write data to a particular location. These are cards which only consist of memory circuits. It can only store, read and write data to a particular location. The data cannot be manipulated or processed. It can also be used as a disposable or rechargeable card which contains memory units that can be used only once. It is a straight memory card used only to store and write the data and protected from restricted access.

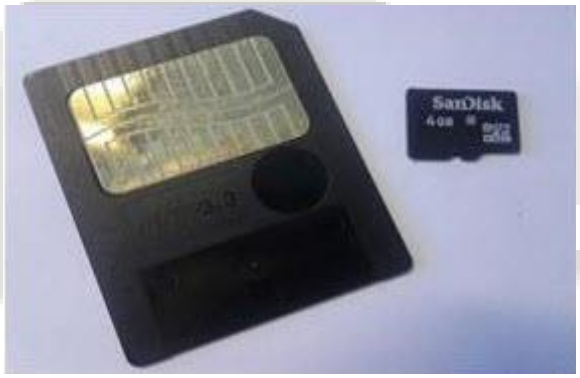

Fig. 4: Memory Smart Card

C. Microprocessor Based Card

These smart cards comprise of microprocessor embedded on to the chip along with the memory blocks. It has specific sections of files which are associated with a particular function. The data in the files are managed either by dynamic operating system or fixed operating system. It also performs the multiple functions and also used for data processing and manipulations.

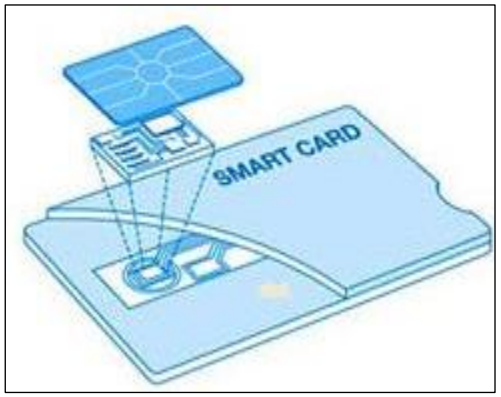

Fig. 5: Microprocessor Based Card

D. Types of smart card chips

1) Contact chips are read by an independent card reader and conform to ISO 7816, the International Standards Organization (ISO) specification for the standardization of smart card systems.
2) Contactless chips are read by radio frequency (RF) signals instead of a card reader. They conform to ISO 14443A and include a magnetic loop antenna that operates at 13.56 MHz.

E. Contact Smart Card

Contact smart card consists of electrical contacts which connect to the card reader where the card is inserted. The electrical contacts are arranged on a conductive gold plated coating on the surface.

Fig. 6: Contact Smart Card

F. Contactless Smart Card

This contact-less smart card communicates with the reader without any physical contact. It consists of an antenna which is used to communicate with the RF band with the antenna on the smart card reader. The antenna receives power from the card reader through the electromagnetic signal.

G. Smart Card Reader System

Smart card reader system including safety and security devices, tools and equipment are supplied by us with assured reliability and durability. Smart card readers system is an electronic device system and also based on data input device system. In this system devices read data from a card shaped storage medium also read plastic cards embedded with either barcode (it is a series of alternating dark and light stripes that are read by an optical scanner) or magnetic stripe(it is a stripe of magnetic oxide tape that is laminated in a card and holds more data than barcode).

Some modern keyboard and personal computer's devices have built in smart card reader. We can see mostly laptop models have built in smart card reader. In this system external devices read cards PIN or other information. Whole model works by supplying the integrated circuit on the smart card. Hiral manufacturer is a well-known provider .He able to consistently manufacturer a product that meets your requirements and allows you to verify claims by visiting or auditing the factory. He focus so much on the product capabilities of a prospective.

Fig. 7: Smart Card Reader

V. SMART CARD INTERACTION

Smart card reader is also called as a card acceptance device, card programmers, or an interface device. There is a minute difference between the card reader and the terminal. The reader is used to determine a unit that interfaces with a computer or microcontroller for all of its processing requirements. Similarly a terminal is also considered as a self-contained processing device. It can be contact type or non-contact type.

Smart card is a portable device (transmits data) which communicates with another device to gain access to a network or a display device. Cards can be operated with radio frequencies; these cards can be plugged into a card reader commonly referred to as a card terminal. When smart card reader and smart card comes closer, it identifies itself to the other by transmitting and receiving information. If the exchanged data doesn't match, further processing will not occur. As compared with ordinary bank cards, these cards able to secure themselves against unauthorized users.

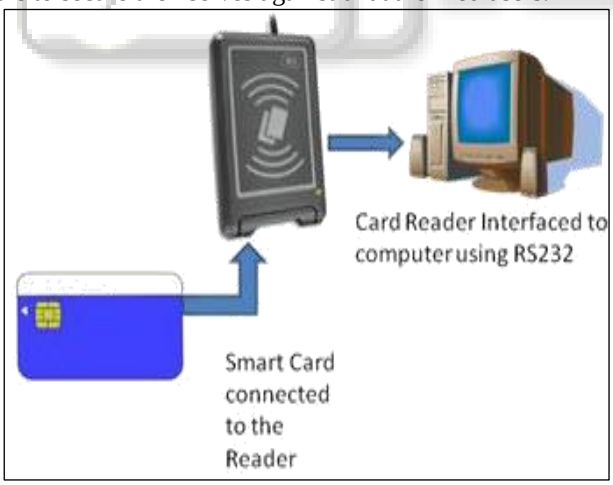

Fig. 8: Smart Card Interaction

VI. APPLICATIONS OF SMART CARD

Smart card is used in a variety of applications over different fields some of these areas are discussed below.

A. Financial Applications

1) Electronic Purse to replace coins for small purchases in automatic vending machines and over the transaction at counters.
2) Debit and Credit accounts, reproducing what is currently placed on the magnetic stripe bank card, in a secure environment
3) Securing payment across the Internet as part of Electronic Commerce.

B. Transportation Purpose

1) Driving licenses
2) Electronic toll gate collection systems
3) Fare collection systems for huge crowd transportation

C. Physical Access Control System

Smart can be used by different public areas such as consumers and business dealers or organizations to provide access to the members (employees of the organization) or other persons to enter the secured areas.

D. Telecommunications

The major and highly prominent use of smart card technology is in the development of Subscriber Identify Module or SIM card. A SIM Card provides network access to the each user or subscribe and manages its authentication. It also provides unique identification to each subscriber.

E. Domestic Purpose

The most commonly used smart cards in domestic field are the DTH card. This DTH smart card provides authorized access about the information coming from the satellites. The card which gets direct access directly to the TV services in the home is nothing but a smart card. The information gets encrypted and decrypted within a smart card.

F. Government Applications

Government of India issue identity cards to individuals by using this smart card technology. These identity cards consist of all the personal and individual details like name, place and date of birth, as an example of this smart card government has issued Aadhar card to all Indians.

VII. CONCLUSIONS

The Smart Card today relay on the fact that code of functions to be performed by operating system. Smart card improve the convenience and security of the transaction. It provide vital components of system security for the exchange of data through any network.

Compared to other cards like credit cards, ATM cards, fuel and phone cards, they can be used to as a one-stop shop for citizens to access multiple services. Smart cards improve service delivery by connecting clients directly with service providers thereby reducing the discretion of public authorities. If implemented well smart cards can improve service delivery systems to cut out middlemen, corruption and bring services to closer to end users and beneficiaries. It is also used in various applications such asFinancial Applications ,Transportation Purpose, Physical Access Control System, Telecommunications, Domestic Purpose,Government Applications.

REFERENCES

[1] Hamed Taherdoost, Shamsul Sahibuddin & Neda Jalaliyoon"Smart Card Security; Technology and

Adoption " in International Journal of Security (IJS), Volume (5) : Issue (2) : 2011.
[2] L. A Mohammed, Abdul Rahman Ramli, V. Prakash, and Mohamed B. Daud ." Literature survey on Smart Card" ,in journal of "International Journal of The Computer, the Internet and Management ", April 2004.
[3] Abhishek Mahajan, Akash Verma, Dhruv Pahuja" Smart Card: Turning Point of Technology"In International Journal of Computer Science and Mobile Computing on 10th, October 2014.
[4] Aditya Bodake , Viraj Baviskar , Ashwini Bodake, Shital Bhoite"Multipurpose Smartcard System" In International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
[5] www.smartcardbasics.com/smart-card-overview.html
[6] www.smartcardbasics.com/smart-card-overview.html
[7] http://people.cs.uchicago.edu/~dinoj/smartcard/arch-1.html
[8] www.smartcardalliance.org/smart-cards-applications/
[9] www.efxkits.com/blog/smart-card-technology-types-working-applications/
[10] http://www.smartcardbasics.com/smart-card-types.html
[11] https://www.elprocus.com/working-of-smart-card/
[12] www.techwalla.com/articles/advantages-disadvantages-of-using-smart-cards

