THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Smart-Card Cognition

Abhijeet R. Pathak
Student, University of Mumbai, Mumbai, India
Abhishek R. Pathak
Student, University of Maryland, College Park, United States of America

Abstract:
A smart card is a safe and portable device which is employed for several functions, especially security associated ones involving situations such as access to the database of the system, either in an online or offline basis. For the brightness of Smart Card's future, it is imperative to look at a number of aspects and factors that consequence due to the fast advancement in communication technology and information. This paper evaluates the modern trends in the technology of smart cards and brings out probable events to occur in the future. Furthermore, the paper addresses different features in order to discover the core ideas that are of attention to smart card researchers and developers. More emphasis is offered for four key features of smart cards: Memory management, portability, open platform and security, as they are considered to be in the center of numerous smart card applications.

Keywords: *smart card, memory chip, BioAPI, datacard, microprocessor*

1. Introduction

A Smart card is among the largest achievements in the information world skills. Just like plastic payment card that has either a microprocessor or a memory chip embedded in it, a smart card has one too. It makes it able produce power to use in diverse applications when it is installed in a reader. The Smart card also can be employed as an access server on internet. For instance, they can make business and individual information available to the users who need it. They also act as portable data devices which offer convenience and security. Gemplus categorized smart cards into:

Microprocessor and Memory: as a microprocessor, the smart card can delete, alter, or add data to the memory card. The memory card mostly stores information that is used in the minute floppy disk that contains different security options.

Contactless and contact: With contactless, an antenna is embedded in the smart card to enhance communication with no physical contact. With contact, there is physical contact as smart cards are installing in minute card reader that enables the contact. A smart card that has both features that are contact and contactless, is called a combi-card and its level of security is very high. Smart cards assist in the business evolution and expansion of their services and products in the diverse world markets. The range of applications of the smart card has increased annually to include uses in various disciplines and markets. In current years, privacy and security matters introduced by the age of information has called for developed smart card security uses.

The other parts of the paper describe the history of smart card growth, recent as well as future analysis of the market. Another section looks at uses, the advantages and shortcomings of a smart card. There is then the technology future direction of smart card, it mostly emphasis on memory control as well as security considerations. This part as well analysis further studies so as to improve the present smart card state to fit future requirements.

2. Historical Viewpoint

A smart card was discovered in the 1970s by Michel Ugon (Seaward, 2006). The French association of bank cards (Carte Bancaire) CB started in eighties and has permitted the dispersion of 24 million devices (Katsikas, 2006). For the Physical features, the initial draft proposal was recorded in 1983. A prolonged dialogue resulted in the equalization of the contact setting. Subsequent was the equalization of protocols and signals which resulted in 7816/1-4 ISO/IEC international standards. Logical security was next in line, as it was crystal clear from the start that there was a need for cryptographic competencies, though it was a little hard due to the restricted computing power and limited bytes of RAM offered at that time (Tilborg, 2011). Today, smart cards are employed in several functions. A survey conducted by the Card-Technology magazine (www.cardtechnology.com) indicated that the companies had distributed a total of 1.5 billion smart cards globally in 1999. In the coming five to ten years, the companies will experience stable growth, specifically in devices and cards to conduct electronic trade and to enable safe access to computer networks. A study conducted by Dataquest in the month of March, 2000, predicts approximately twenty-eight million smart card distributions (Memory and Microprocessor) in America. According to this prediction, a yearly growth rate of sixty percent is supposed for America smart card distribution between 1998 and 2003. Smart card forum Client Research, published untimely in 1999, gives an additional insight into the client attitudes towards functionality and employment of smart cards. A market growth of smart cards is rising fast due to its broad range of services. The global smart cards market prediction in millions of units and millions of dollars as indicated in the figure below:

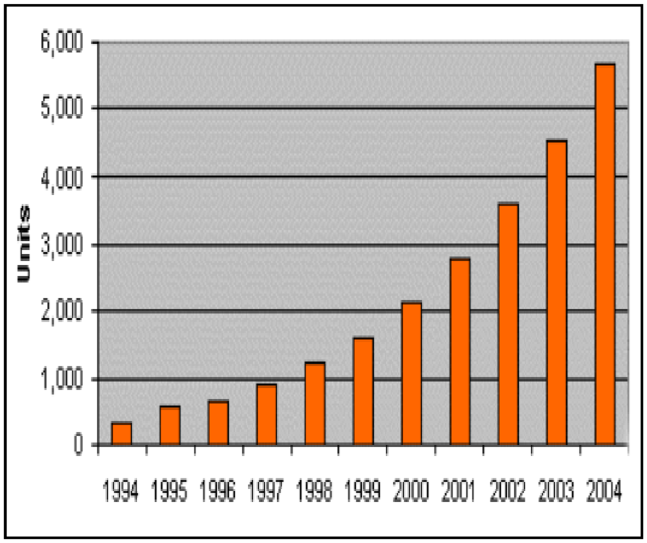

Figure 1: Global Market for smart cards
Smartcard market retrieved from (smartcardcentral.com)

2.1. Management of the Memory

A Smart card is a gadget with significant hardware limits: low information rate, low-power CPU, limited memory and many more. Nowadays, card technology uses 8 bit processors (largely of the 8051 or 6805 family) whose memory space is about few tens of kbps (Seaward, 2006), typically 1-4 kb RAM (Random Access Memory), ROM (Read only Memory) of 32-128 kb, PEEROM (Programmable Electrically Erasable Read Only Memory) at least, with alternatives on FRAM and FLASH. Also the requirement for smart cards development, the standard memory (64 Kbytes or 32) can demonstrate a severe constraint. The key to this is checking for various design techniques and issues to incorporate many memory chips in a solo smart card. Katsikas had already manufactured a twin card, including two separate chips in a solo card. Other approaches comprise the use of Computers in Connection to smart cards. Seaward (2006) proposes the employing of a powerful Computer in conjunction with a smart card for encryption of symmetric key since the computer gives a higher bandwidth encryption. Table drawn below demonstrates storage capacity required for various communication rates.

	Transmission Rate	**Storage Capacity**
Computer (Pentium 4)	129.5000Mbps	11GBytes
Smart card (Standard)	9600bps	64Kbytes
Several chip card	20Mbps	224Mbytes

Table 1: Transmission rate and capacity of storage

According to Tilborg Et Al, (2011), the smart card chips built in 0.13- micron PEEROM employed in recent smart cards is beyond technology. For the same motive, reaching its scalability confines, particularly for corporations like Philips, concur on the requirement for an optional non-volatile smart card memory future. Presently, Philips is leaning on the side of magnetic RAM as a substitute to PEEROM.

Another imperative application that involves management of the memory is the application of biometrics.The employment of biometrics inside the smart card will mean that features of biometrics (voice, fingerprints and retina) can reliably recognize an individual. With enrichment in memory structure, it will shortly be possible to approve the employment of electronic data in smart card by a spoken word. The employing of some of these characteristics has already been executed in many applications. National ID of Malaysia, for example, is a multipurpose card with a biometric fingerprint. The smart card is a first of its kind in the globe as it combines lots of applications such as healthcare, driving license, passport and non-governmental applications (e.g. e-purse). Table drawn below demonstrates the requisite bytes for diverse biometrics (jpn.gov.my).Additional data on biometric standards and technology can be gotten from the following corporations: The Biometric Consortium (biometrics.org), International Biometric Company Association (ibia.org) or BioApi Consortium (iapi.com).

Biometric	Bytes Requisite
Finger scan	Three hundred to twelve hundred
Finger geometry	fourteen
Hand geometry	nine
Iris recognition	Five hundred and twelve
Voice verification	Fifteen hundred
Face recognition	Five hundred to one thousand
Signature verification	Five hundred to one thousand
Retina recognition	Ninety-six

Table 2: Requisite Biometrics Bytes
(Retrieved from Smartcard Alliance)

2.2. Safety Issues

Safety is at all times a significant distress for smart cards functions. It naturally gives rise to the requirement for efficient, reliable cryptographic algorithms. We require providing identification and authentication in online systems like computer networks and bank machine, access control, and many more. Presently, such facilities permit access employing a token; though, it is imperative that the token controller be the legitimate user or possessor of the token. The smart card is highly restricted or handicapped in their input/output (unable to interrelate with the globe without outside interruptions). This points to the participation of many groups in its applications. Various groups involve Card Issuer, Data Owner, Cardholder, software manufacturer, card manufacturer, and Terminal user. (Imai, 2000). It is, therefore, necessary to ensure that nothing of the above stated groups is a threat. To get to this, there is the requirement for further research on the analysis and design of smart card identification and authentication protocols. For these grounds, Imai, (2000) suggests that the cards be fitted “additional I/O channels” like buttons to lessen these shortcomings. Additionally, there are numerous interruption techniques able to interfere with smart cards plus other alike temper-resistant gadgets as presented in (Tilborg, 2011). It also shows the need for effective interference prevention/detection techniques.

2.3. Open Architecture

Subsisting smart card principles leave merchants with too much space for interpretation. To attain wider accomplishment, there is the requirement for the free policy that offers the inter-operable cards solutions across numerous software and hardware platforms. Open platform, as interpreted by Global Platform (GlobalPlatform.org), is an all-inclusive system architecture that permits the easy and fast development of worldwide interoperable smart card structures. It comprises three essentials; systems, terminal, and card, each of which might include specifications, software or chip card expertise. Together these components interpret a flexible, secure, and easy to use card atmosphere.

The development of principles like IATA 791, PC/SC, EMV, ITSO, GSM, and CEPS gives an opportunity for producers to produce products on a profitable scale and offer stability to systems makers. According to an account by Data card Group (Version 1.0 of the White Paper), True ‘open’ cards will contain the following features:

1. The will control a non-proprietary operating structure widely supported and implemented.
2. No single seller will specify principles for the operating structure and the card’s application.
3. The cards will sustain a high-level function programming language (for instance C++, Java) so issuers can support and provide their applications and the applications from many more other sellers.
4. Applications can be jolted and will function on different seller’s multi-application cards with alike API (Application Programming Interface).

To overcome the trouble of lack of equivalence, American organizations have come up with an add-on portion of cards software destined to overcome communication concerns between readers and chips cards from different sellers. They would admire to observe this expertise, which they name “card capabilities container” employed globally, making it an organization standard that would permit American Agencies to purchase readers and cards from many sellers, sure that they will work together (Tilborg, 2011). Another way is the expansion of a new corporation named Smart Card Alliance, structured by Smart Card Organization Association (SCOA) and Smart Card Forum, to play as the sole voice for the American smart card Corporations. Even in biometrics, every seller has its techniques for enrolling persons and later checking somebody’s identity against the kept picture. However, there are progresses underway to produce biometric standards, mainly driven by the American government. In a major way, the U.S National Standards Institute endorsed BioAPI as a principle way for biometric gadgets to exchange information with ID functions. ANSI is suggesting BioAPI to ISO in for adoption as a global Standard (IEEE Spectrum, 2015).

3. Conclusion

Most of the card systems in employment these days serve one motive and are associated with just one procedure or is hardwired in only one function. A smart card may not justify its subsistence in this area. The approach of prospect smart card is therefore to designing multi-application smart cards with individual operating structure bottomed on the open principle that can do a variety of applications. It must be programmable and configurable and it should be able to acclimatize to new requirements and new situations especially in regions such as operating system, memory management, and security.

4. References

i. Jarvis C.R., Beyond the Phone Card : Emerging Smart Card Opportunities, in GEC Review, pp. 131-137, vol. 12, n° 3, 1997.

ii. Fancher C.H., In your pocket : smart cards, in IEEE Spectrum, vol. 34, n° 2, february 1997, pp. 47-53.

iii. Quisquater J.-J., The adolescence of smart cards, in Future Generation Computer Systems, n° 13, 1997, pp. 3-7.

iv. http://www.dice.ucl.ac.be/~dhem/cascade

v. Colinge J.-P., Performances of Low-Voltage, Low-Power SOI CMOS Technology, in Proceedings 21st Int. Conference on Microelectronics, vol. 1, september 1997, pp. 229-235.

vi. Colinge J.-P.,Silicon-on-Insulator Technology: Materials to VLSI, 2nd edition, Kluwer Academic Publishers, 1997.

vii. Guillou L.C., Ugon M., Quisquater J.-J., The Smart Card. A standarized Security Device Dedicated to Public Cryptology, in Contemporary Cryptology, edited by Simmons G.J., IEEE Press, 1992, pp. 561-613.

viii. Motorola, Technical Summary, MSC0501, 8- bit microcontroller with Modular Arithmetic Processor, 1997.

ix. Rankl W., Effing W., Smartcard Handbook, Wiley, 1997.

x. Huang W.M., Papworth K., Racanelli M., John J.P., Foerrstner J., Shin H.C., Park H.,B.Y., Wetteroth, Hong S., Shin H., Wilson S., Cheng S., TFSOI CMOS Technology for sub-1V Microcontroller Circuits, in IEDM, 1995, pp. 59-62.

xi. Mistry K., Grula G., Sleight J., Bair L., Stephany R., Flatley R., Skerry P., A 2.0 V, 0.35 µm Partially Depleted SOI-CMOS Technology, in IEDM, 1997, pp. 583-586.

xii. Kimio U. et al., A CAD-Compatible SOI/CMOS Gate Array having Body Fixed Partially Depleted Transistors, in IEEE International Solide-State Circuits Conference,1997, pp. 288-289

xiii. Masayuki et al., 0.25 mm CMOS/SIMOX Gate Array LSI, in IEEE International Solide-State Circuits Conference, 1996, pp. 86-87.

xiv. Chi M.-H., Bergemont A., Programming and erase with floating-body for high density low voltage Flash EEPROM fabricated on SOI wafers, in Proceeding 1995 IEEE International SOI Conference, oct. 1995, pp. 129-130.

xv. Dickson J.F., On-Chip High Voltage Generator in NMOS Integrated Circuits Using an Improved Voltage Multiplier Technique, in IEEE Journal of Solide-State Circuits, vol. SC-11, n° 3, june 1976, pp. 374-378.