Smart Cards: The Future Gate

S.A.M. Rizvi , Halima Sadia Rizvi,Zaid Al-Baghdadi

***Abstract* -** Smart Cards are one of the latest applications of Information Technology whose use is growing with each passing day. Like computers today, it is presumed that smart cards, which in fact contain tiny computers, will be used extensively in future for a variety of purposes. In Europe, US and many developed countries smart cards are being extensively used by commercial organizations as well as the Government. In future they are expected to replace every thing that a person carries in a purse, like cash, credit cards, driving license cards, identification documents etc. Smart cards can be used for a wide variety of applications in many areas ranging from personal identification to e-commerce transactions. One of the important purposes for which smart card technology was developed is for dealing with card fraud in e-commerce. This article covers the history and origin of cards, weaknesses of the traditional plastic cards, development of smart cards, their design, different types, how they work, their applications in e-commerce and other areas, advantages and disadvantages. This article also examines how this technology can be used as a potent weapon in the fight against cyber crime.

Keywords: smart cards, chip card, or integrated circuit card (ICC)

1. Introduction

A smart card, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits which can process data. This implies that it can receive input which is processed by way of the ICC applications and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic.

Microprocessor cards contain volatile memory and microprocessor components.

The card is made of plastic, generally PVC, but sometimes ABS or polycarbonate. The card may embed a hologram to avoid counterfeiting. Using smart cards is also a form of strong security authentication for single sign-on within large companies and organizations.

2. History of Smart Cards

Diners Club was the first to introduce all plastic cards for payment applications. Till 1950 the cards in use were paper based cards and during early 1950 Diners Club introduced PVC based cards for longer life. The card became very popular as one could pay with it at select restaurants. What really appealed to the customers is convenience, there was no need to carry the money and it also identified them with an elite group in the society. VISA and MasterCard entered the market. These cards were prone to fraud, tampering. Soon the realization came that the solution to these problems may lie in development of machine readable cards. That led to the introduction of Magnetic stripe card, which permitted storage of data on it in a machine readable format. Magnetic stripe card is a major weakness and that is anyone with access to appropriate device could read, re-write and delete data. Thus, magnetic card was not secure enough for sensitive data and also needed complex back end infrastructure for verification, The necessary back end information was available in US but not in Europe. So Europe solved this problem by transferring some of the back end work to an Integrated Circuit Card (ICC) on the client side of client/server architecture. First ICC patent was registered by German inventors Jurgen Dethoff and Helmet Gotrupp during 1968. Japan developed its card in 1970 and France 1974. Initial commercial applications of this card were as telephone cards. With developments in cryptography, France introduced the first chip incorporated banking card in 1984. Germans followed suit in 1997 and they also issued 70 million Smart cards with insurance information. Magnetic stripe cards could store 1000 bits of data, whereas Integrated Circuit Cards came to be known as Smart Cards could store up to 20 Kilo Bytes of data, cards fall into the last category, where the transactions are carried out with the understanding that the payment would be made sometime in the future. The credit cards account for one third of all sales in US, Europe and Australia.

3. The Alternative: Smart Cards

Plastic cards offer little security and are prone to frauds. Magnetic stripe cards are easiest to manipulate or fabricate. These vulnerabilities of plastic cards created a necessity for more secure cards. The developments in the area of IT offered a solution by the way of Smart cards. Smart cards look similar to the present-day plastic payment cards and are of the same size. It has a memory chip or a micro processor embedded on the card. This chip -is a kind of miniature computer which can store data or perform computations. It can receive information, process and make decisions. Smart cards are convenient,

Dr. S.A.M. is with Rizvi Dept. of Computer Sc., J.M.I., New Delhi, India (email: samsam_rizvi@yahoo.com)
Dr. Halima Sadia Rizvi is with Dept. of Economics, J.M.I., New Delhi, India (email: halima_rizvi@yahoo.co.in)
Zaid Al-Baghdadi is with Dept. of Computer Sc., J.M.I., New Delhi, India (email: zaid1983@ymail.com)

secure and provide data portability. The chip also contains the information about the cardholder.

This card is used along with a card-reader meant for this purpose and is capable of receiving data from the card's chip, analyzing and responding to the data. Smart cards can be used not only for e-commerce but also for a wide variety of applications ranging from e-commerce to physical access control.

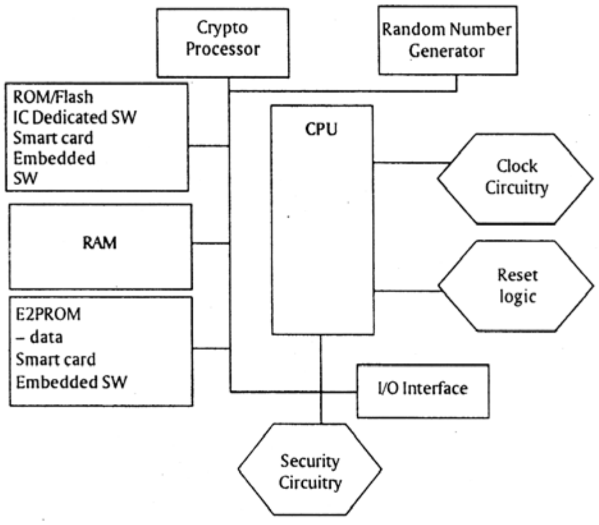

Figure 1: Typical Smart Card IC

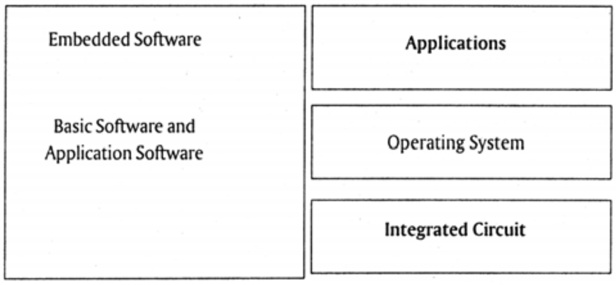

Figure 2: Smart Card Architecture

4. Types of Smart Cards

A. Memory and Microprocessor Cards

Based on the type of chip present, the smart cards can be of two types. They are 'Memory cards' and 'Microprocessor cards'. Memory cards contain some special type of memory chips on them like, Electronically Erasable Programmable Read Only Memory (EEPROM) and Read Only Memory (ROM) and can store large amounts of data. They can be compared to floppy disks. Additionally, they have some security features. Some of them are capable of carrying out limited mathematical functions like addition and subtraction. The logic prevents writing of the data and allows memory read access. They are typically used for applications like prepaid telephone cards and health insurance cards. Microprocessor cards, on the other hand, are cards with a miniature computer on them. This computer has an operating system, input/output ports and can carry out complicated functions. Unlike the normal personal computer operating systems, the operating system on smart cards is only a few thousand bytes of code. The tasks it can handle include data transmission over the bi-directional, serial interface, loading, operating and management of applications, instruction processing and execution control, protected access to data, memory management, file management and most importantly management and execution of cryptographic algorithms. They have built-in security features but do not have the user interfaces or the ability to access external peripherals or storage media. For Hardware architecture of smart cards refer to Figure I and smart card architecture, Figure 2.

B. Contact and Contact Less Cards

Another way these cards are classified are 'Contact cards' and 'Contact less cards' based on the interface used. In case of contact smart cards these cards have to be inserted into the reader in order to read from or write to them. In contact less cards the embedded chip also contains a tiny antenna, and a radio frequency signal is used for communication between the card and the reader. The physical contact is not necessary. Contact less cards are more efficient, saves time, and also prolong the life of card reader. The chip is sealed between a number of layers of the card and hence the data is protected throughout the life of the card. Contact less cards produce a higher throughput. Maintenance of readers is minimized and as a result the life of this equipment goes up. Contact less cards are suitable for applications like attendance records, electronic cash, health information, access privileges. They can be used for multiple applications and also in combination with biometrics thus making them very secure.

Present contact less cards use micro controller or wired logic technology. Wired logic cards can only support pre-defined functions, whereas Micro controller based cards have the capability of PCs. They are far superior to wired logic technology. For applications which do not need high security and cost is a factor, wired logic technology is the answer. Further contact and contact less cards are equally secure, as both use advance cryptographic techniques. In case of contact less technologies it is technically possible for someone to intercept communication between a card and t e reader. Further, when the card passes near the reader there is a chance of card getting activated without the knowledge of the owner. This is controlled by making user authentication necessary for activating the cards. Currently contact cards are being extensively used in financial sector and contact less cards in transport sector and access control. With the costs of contact less cards coming down and the security levels going up, future will certainly belong to contact less cards.

C. Multiple Applications Cards

Smart cards can be used for multiple applications obviating the need to carry number of cards, each designed for a specific application. A trial program in multi-application cards was conducted at Florida State University, where 40000 smart cards were issued to students catering for applications like personal identification, dormitory security, banking, food, pay phone, photo copying, transportation and vending. This trial was a success. However, the biggest benefits of smart cards can be reaped in commercial arena. These cards can be used for storing the money, information and hence are suitable in both B2B and B2C commerce. The applications here include banking, payment, loyalty programs and promotions, access control, stored value, ticketing, parking and tax collection etc. Further multiple applications can be stored on a single card, which is not possible with the conventional cards.

The first payment smart card in the US was introduced during 1999 by American Express. Though 'American Express Blue' had only limited functionality, the customer could use it as credit cards, it had extra security for online shopping and also offered electronic wallet. It had become quite popular. During 2000, Visa came out with 'smartVisa, a multi application smart card. 'SmartVisa incorporated EMV (EuroPay, Master card, Visa) standards and payment applications. The applications included Internet access, secure Internet purchases and reward services. 'SmartVisa has become the *de facto* industry standard. Visa's multiple application offering, open-platform technology, uses firewalls on chips for added security, and also allowed downloading of applications eliminating the need for new cards for new applications. It was largely successful. Mastercard launched its 'OneSMART' during 2002. 'OneSMART' offered basic services and a variety of applications such as chip-based credit/debit, stored value, e-couponing, Internet payment, security, loyalty, e-ticketing etc. The experiences of these organizations and studies indicate that smart cards are attracting customers and are a success. According to industry estimates, at the end of 2003 in the US alone 30 million smart cards are in use.

D. Hybrid and Combi Cards

It has become very common to use different terminologies while referring to cards that support plurality of technologies. There are smart cards that serve both contact and contact less operations. Similarly smart cards can be combined with magnetic stripe cards. When different technologies reside on the same chip do not communicate with each other, for example, contact less technology and magnetic stripe technology, they are called hybrid cards. Normally hybrid card has two chips. These chips are not connected. When a single micro processor can be used for both contact less and contact readers it is called a 'dual interface card' or 'Combi card'. A Combi card is a single integrated platform for multiple contact and contact less applications. Theoretically it is possible to combine any number of applications on a smart card. However, with too many applications, the complexity of the card goes up. Further, it is more important that the card reader should be able to support all the applications on the card.

E. Cryptographic Capabilities of Smart Cards

Present-day smart cards have all the necessary cryptographic capabilities and can support many security applications. The smart cards make use of asymmetric, Public Key Infrastructure cryptography, which uses Private and Public Key combination. The EEPROM contains the Private Key of the cardholder and it is so designed that the key can never leave the EEPROM. To that extent even the cardholder himself cannot access the key. As additional layer of security, the private key is also protected by user's PIN. Hence, mere possession of the card is of no use in the absence of the PIN. Multiple PINs for different purposes can also be used like one for access to information, other for using electronic purse etc. One PIN called Security Officer can be configured to block or reinitialize the card after specific number of bad attempts. Further, biometrics is also being added to the cards making them absolutely safe. Smart cards support RSA signatures and verifications for different key lengths such as 512 or 1024 bits. Digital Security Algorithm (DSA) is also used but less widely than RSA algorithms. Further many methods of hardware security monitoring are added. To avoid card cloning an unalterable serial number is burned into the memory. The cards are also designed to rest themselves when they experience power fluctuations. Random number generation uses pseudo random technique and also hard wire based generation. Further security protocols are built into communication protocols. They allow the smart card itself to authenticate to the terminal or card reader and vice versa. What is noted, however, is that cryptographic algorithms are application or terminal specific.

5. Smart Cards Eliminate Security Risks Associated with Magnetic Stripe Cards

Smart cards are primarily being used in financial (payment) applications. There are a number of other areas also, where smart cards are being used effectively. As far as the financial applications are concerned, smart cards available in the market from Visa, Master Card, American Express support multiple applications. For any financial or other application the important considerations are security, speed, convenience and customer satisfaction. Though the Internet commerce is growing, many potential customers are staying away due to the ever growing number of reported credit card fraud incidents on the Internet. Many people are scared of disclosing their credit card number due to the frauds. Smart cards are quite, secure. Smart cards use cryptography and carry a private key in a secure manner. Nobody other than the rightful owner of the card can have access to this private key. Because of this security, payments using smart cards are safe. This safety can help in removing the inhibitions from the minds of potential customers about the risk aspect. Further smart cards are also incorporating biometric technology for making authentication fool proof. During the process of authentication the biometric comparison eliminates the possibility of somebody else making use of the card. The issuing authorities can authenticate the card and the owner before the retailer concludes the transaction with the customer. While using plastic cards like magnetic stripe cards this facility is not available and the transaction is treated as 'card not present' transaction and the retailer is solely responsible. Using smart cards shifts the responsibility from the retailer to the issuer authorizing it. Smart cards could be used at physical retail outlets or for Internet commerce.

Secure identification systems vastly improve the confidence level of all parties involved in e-commerce. Biometric technologies involve identification of a living person, by using unique physiological characteristics. Biometrics could be finger prints, retina, ear lobes, etc. Smart cards ':ire capable of storing large amounts of data on them, and the biometrics of any person can be stored on the smart card in addition to the other programs and data. Smart cards with biometrics are presently being employed wherever there is a need for a very high degree of privacy and security. The identity of individual is verified by capturing the biometric of an individual at the place of contact and the same is compared to the biometric which was captured when the smart card was issued to that person. Smart cards compare stored biometric image with the live biometric. This system provides enhanced security by eliminating the need for access of central database during verification process, enhanced security, improved 10 system performance.

6. Smart Card Infrastructure for Physical Retail Payments

To use smart cards at any physical retail outlets, the following infrastructure is needed. The first is smart cards and smart card applications. These applications which are of interest to customer, issuer and the merchant are loaded onto the card at the time of issue or added later through a smart card terminal or ATM or Internet. At the retailers end smart card reader or integrated P S hardware is needed. Smart card payment applications are generally loaded onto these terminals or Integrated P S terminals. The next component is retailer host system where additional data from smart card transaction can be updated. Then, Acquiring and Processing Systems that collects the data from P S terminal when it goes online are needed, and is meant for authorization and settlement services for the retailer. Issuing, life cycle management and fulfillment systems is another important component. The aim is to manage issuance, activation, post issuance support, for updating card data and applications. Further, as the smart cards are moving towards multiple applications, there is a need to implement new terminals and applications that can support these activities at the retailer end.

7. Smart Card Payment Process at Physical Outlet

After scanning the purchased items P S prompts the customer to insert smart card. The terminal asks the customer for payment mode like credit or debit. The application on EMV terminal reads the information and begins the credit checks necessary for approval of transaction online/offline. Offline risk checks are carried out as per the reestablished rules on the card and the reader. If the risk is low, offline authorization is approved. If the risk is higher the request is sent for online approval. The P S then informs the customer of the approval or otherwise and complete the transaction.

8. Smart Card Infrastructure for Internet Payments

When compared to physical transactions, security and cardholder authentication is very important in online transactions. Unlike physical transactions evidence like signed sales receipt is not available with online transactions. In the absence of such evidence it is very difficult to prove, if the customer denies the transaction. The infrastructure needed for Internet smart card transactions must also cater for such issues. The Internet retail payment smart card infrastructure include consumer smart cards and smart card applications, smart card reader for the consumer's personal computer, PC client software to support smart card applications, Internet retailer server support for smart card applications, Acquired processor infrastructure for authorization and settlement of smart card transactions. It also needs the issuer systems supporting the authentication and transaction process and managing the issue card base. Merchant service provider infrastructure includes the Web server, authentication server that provides the service that allows access to a secure site and the loyalty servers and 24x7 help desk.

9. Smart Cards Payment Process on Internet

For carrying out online transactions, user must be connected to the Internet and the browser must be ready. The smart card reader is connected to the user's PC and the necessary smart card client software is already installed on the user's PC. The authentication process is as follows. User enters the URL of the merchant website and the Web server sends the home page to the user. This home page has a link to the users protected information like account information or the checkout page. If this link is selected by the user the card reader software is started by the Web server, which prompts the user to insert the card into PC's card reader and enter the password. The smart card validates the password. A unique transaction certificate is routed to the merchant's authentication server that authenticates the cardholder/smart card combination. The certificate is created by the card, making it unique for each attempt. If the authentication server approves the transaction, the merchant can be satisfied that cardholder is valid one.

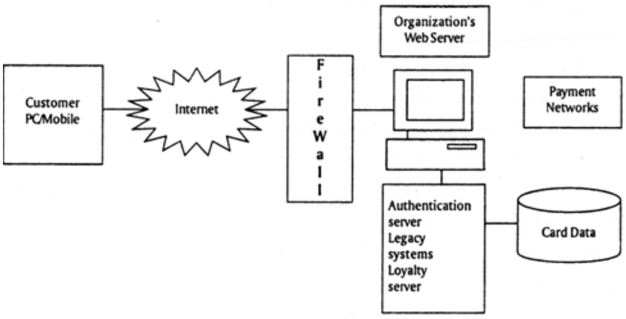
Organization's Web Server
Customer PC/Mobile
Internet
F i r e W a l l
Payment Networks
Authentication server Legacy systems Loyalty server
Card Data

Figure 3: Smart Card Enabled Internet System

A session is created after the authentication is received allowing the user to access protected resources until the user exits or timed out. The payment process then is carried out. User fills the shopping cart. Once the user decides to check out, website order form

starts the card reader software. User may also be given the choice to redeem the loyalty points, if he chooses to. Software then prompts the user to insert the smart card in to the reader and enter the password. Smart card validates the password and launches the e-wallet, which stores the credit card information, along with billing and shipping information. The e-wallet fills the order form with cardholder's information from the smart card. Once the user confirms the purchase, the information is routed to the issuer to authenticate the cardholder/smart card combination. Each card creates a unique digital certificate. This certificate is sent to the issuer through the merchant site if the issuer approves the liability shifts from the merchant for fraudulent transactions and non repudiation. On receipt of authorization, merchant requests an authorization through credit card network. The transaction then follows like a card not present transaction. If merchant participates in any loyalty program, points are added to user's loyalty account. For the diagrammatic representation of the above process refer to Figure 3.

10. Other Smart Card Applications

Initially the smart cards were used as telephone cards and bank cards. At present the other applications include Electronic purse, Telephone calling card, Health care card, Government card, Social security card, Group cards like cards issued by clubs and so on. According to Smart Card Alliance, Internet commerce, General retail, Mobile Commerce, Transit, Contact less Payment, Campuses and government are the seven key markets adding momentum to the growth of smart card use. Both Governments and businesses are using IT and computer networks, intranets, Internet extensively for storing and moving the data. The primary aim here is to make the data available to the persons needing it. But at the same time ensuring the privacy of people is protected and also safeguarding the information assets of the organization. In this context smart cards find many uses. They include secure logging in onto the organizational networks, secure B2B commerce, storing of digital certificates, credentials and passwords, Encryption of sensitive data. Smart cards are the most secure place to carry-out public key, private key encryption which the user wants to hide from others. Smart cards are very secure and the security could be further improved by including biometrics onto the smart cards. Whereas in the traditional cards the security is limited to PIN verification, smart cards can combine PIN with Biometrics, which results in a very high-level of security. Smart cards can also be used in mobile commerce. With the growth in wireless communications systems, the mobile commerce is also growing. Wireless providers are now relying on smart cards for security mechanisms to protect their services. Smart card technology can be used with 'Global System for Mobile communications' (GSM), by inserting the card into the handset. The smart cards here enable secure user authentication, roaming and secure value-added services. The SIM cards will provide easier payment mechanism for mobile commerce.

11. Standards

For any technology to become popular the important requirements are business case and availability of standards. The security needed for e-commerce and multiple application facility provides the impetus for the business case, whereas the standards are very important for inter-operability and open-platforms. Standards are needed for covering areas like interfaces between cards, terminals and slots. Standards are the key to the growth of any technology. ISO has developed standards for the smart cards. For contact cards the standards are covered through parts 1 to 10 of ISO/IEC 7816 to 7825. 7816 covers physical characteristics and 7825 covers electronic signals and answer to reset for synchronous cards. International standards for contact less cards are ISO/IEC 14443 (1-4). The other prominent smart card specifications and standards are PC/SC standard created by RSA in 1994, PC/SC standard developed by a work group comprising of HP, IBM, Microsoft among others in 1997, Open card standard developed by IBM, Netscape and Sun in 1997, Java card, Common Data Security architecture in 1997 and Microsoft Cryptographic API. Out of all the standards Java card standard has been adopted by 95% of the smart card manufacturers.

12. The Benefits of Smart Cards

Users can easily carry smart cards wherever they go. When smart cards are not present confidential information like private keys of PKI technology had to be stored on hard disks of computers. This information is prone to problems like data thefts, loss or corruption of data during transmission, failure of hardware. Smart cards being tamper proof, eliminates most of these problems, by providing long-term secure storage. Smart cards improve portability. In absence of smart cards people have to make use of laptops by storing the access keys to networks on the hard disks. Smart cards eliminated this need of carrying laptops by storing access permissions with the help of which, the user can work from any node on the network. Smart cards can also store multiple certificates required to access different services. Smart card chip can incorporate magnetic stripe technology and hence can support legacy applications. The card is tamper resistant and can be of no use to anyone other than the owner, even if it is lost and found by somebody, or stolen by somebody. Smart cards have long life period and a single smart card can be used for more than ten years. The cost of smart cards is around $3.79 at present and the costs are coming down. A single smart card can replace a number of cards meant for different applications. For example a customer's smart card can have his photo ID, network access, and physical access permissions on the same card eliminating need for three different cards. Smart card can store biometric information of the user, like retina, finger prints, ear lobes and thus can eliminate the use of PIN and still provide much higher security. Operating systems like MS windows 2000 and XP are smart card ready. The smart cards have the capability to store and execute the Java code.

13. Plastic Card Fraud

According to the FBI/CSI annual survey for the year 2003 and other reports, theft of credit card information accounts for 30 to 40% of the data theft. Credit card frauds are one of the rampant crimes on the Internet. Plastic card payment systems came into existence during the early 1950s and are in use for quite sometime now and have become very popular world over. The prime reason behind the development and success of plastic payment cards is to eliminate the risks associated with carrying large amounts of cash. If the extensive use and wide popularity of these cards is any indication, the primary objective has been achieved. However, the irony is that use of plastic cards has opened up doors for new risks with grave consequences. The cards that are in use today in commercial arena could be broadly divided into three types, cards used to pay before transaction, at the time of the transaction and after the transaction. Prepaid telecom cards are the example of the first type. These are the stored value cards. Second category is represented by ATM and debit cards. The use of these cards permits the concerned transaction. According to Australian Institute of Criminology, these cards registered a growth rate of 919% from 1989. Credit

14. Vulnerabilities of Plastic Cards to Fraud

During a study of card fraud by Jackson, a group of 14 fraudsters admitted that they have committed the fraud using more than 100 ways. Cards. are vulnerable to frauds in many ways. Among these vulnerabilities 'Altering and Counterfeiting' is the most prevalent. Normally lost or stolen cards are used for perpetuating fraud. What actually takes place is the details on the card are altered. Most of the cards in use today are in counterfeiting called skimming and buffering. For example, when customers pay their bills at the restaurant or at a supermarket, the waiter or the sales person takes a brief possession of customer's card during which he passes it over magnetic card reader which will capture all the details and then using those details makes a counterfeit copy. This process is known as skimming. Modifying this information is called buffering. The second method of committing the card fraud is through what is known as 'Application fraud'. In this method the con collects the personal details of somebody else and applies for a card in that other person's name. In another variant of this the fraudster may apply for a card with fictitious details. Once the card is issued, after using up the card, up to the limit, he simply disappears. The third major method used in carrying out the fraud involves use of Permanent Identification Number (PIN) issued with the cards. The weakest link is the way the issuer communicates it to the customer. Someone can intercept this communication and can have access to the PIN. Or the user himself might give away the number unwittingly without realizing the implications. In ma1J.y cases users were tricked and in a few cases they were coerced into disclosing PIN. There were instances of physical violence and also use of sophisticated telephoto lenses. With the growth of e-commerce, Internet has become the main source of card data theft. As the card details have to be disclosed for carrying a transaction on the Internet, this has become the main vehicle of theft, by intercepting the traffic on the Internet. In a large number of cases, hackers stole the information from organizational databases. The consequences of the theft of credit card information could be grave for the cardholder.

15. Barriers and Challenges to the Growth of Smart Cards

Notwithstanding the benefits organizations and consumers can derive from smart cards still there are many challenges and barriers to their adoption. The first among them according to many is lack of a business case. These people argue that still non-payment smart card applications have not become mature enough. Then conflicting interests of stakeholders and competing technologies is a major problem. The next issue is the costs involved with back office integration for smart cards are a major hurdle. Lack of universally acceptable standards is also a major hurdle. Though EVM has become a de facto standard, there is a serious problem attached to it. EVM standards are designed for GSM Technologies. In some countries like the US the technology used for mobile communications are COMA based. Hence there is a conflict. Though ISO standards are available they are not covering the entire range of requirements. Then there is the case of loyalty programs. It is well-known that loyalty programs help retain and reward the loyal customers. No standards or industry driven specifications are currently available. Yet another gray area is the lack of standards for smart card readers used with PCs. Work is going on at various levels to address these issues and most of these issues are being addressed.

16. Conclusion

Smart card technology is the latest of IT technologies and addresses the security issues concerning a wide spectrum of areas. Smart cards are not only useful for customers and business organizations but also for the national governments. Smart cards are very popular and latest surveys indicate that there are more than 30 million smart cards in use in US alone and the number is growing. The number of applications smart cards can support is also growing. With this technology identity theft and credit card fraud can be controlled to a great extent. Further it will give a fillip to the Internet commerce. It will be no exaggeration to predict that the future belongs to contact less smart card supporting multiple applications.

References

[1] John Elliott, "Two Fingers to the Smart Card", May 2003, www.chyp.com.

[2] Smart Card Alliance, "Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems", May 2002, www.smartcardalliance.org.

[3] Smart Card Alliance, "Contact Less Technology for Secure Physical Access: Technology and Standards Choices", October 2002, www.smartcardaUiance.org.

[4] Hurgen Bohler, "Advanced Security Functions for Smart Card Chips", 2002, STMicroelecrronics, *www.st.com*.

[5] David Storch, "Smart Cards and Public Key Infrastructure", 2001, www.slb.comidexa.

[6] Laura Joyce Moriarty, "Evolving Smart Card and Biometric Technology", 2000, Emory university, *net.educause.edu/ir/library/pdf/DEC0004.pdf.*

[7] Russel G Smith, "Plastic Card Fraud", July 1997, Australian Institute of Criminology, www.aic.gov.au.

[8] Oliver, Markus G Kuhn, "Design Principles for Tamper Resistant Smart Card Processors", 1999, University of Cambridge, *www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf*

[9] CSI/FBI, "Computer Crime and Security Survey", 2003, www.gocsi.com.

[10] Laminex, "Contact Less Smart Cards", Viewed March 2004, www./aminex.com.

[11] SSP Litronic, "Introduction to Smart Cards", 1999, www.sspsolutions.com.