International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 2, Issue 5 (March 2013) PP: 29-35

Smart Card based Robust Security System

K. Eswar Kumar[1], Ashok Kumar Yadav[2], Dr. T. Srinivasulu[3]
[1](Department of Electronics and Communication, Gudlavalleru Engineering College, Gudlavalleru)
[2] (Technical Manager, Electronics Corporation of India Limited, Hyderabad)
[3] (Prof & Principal Guru Nanak Institute of Technology, Hyderabad)

ABSTRACT: *In the up to date electronic planet, authentication of an individual is a vital assignment in numerous territories of everyday existence. Smart Cards are secure compact space gadgets utilized for a few requisitions specifically security identified ones including access to framework's database either connected or disconnected from the net. Smartcard are regularly "secure" movable units. It is an elevated amount outline system for installed informative data frameworks. Normally a smartcard consist a memory or a microprocessor chip. Mainly this paper presents an integrated system for high security objectives. Such as: defense, and nuclear or any critical entering areas. This system is operated with the three factors; they are having a smartcard, password, and any user specific identification components. These may be: fingerprint, or any facial elements. The purpose of this application is to limit the access of the unauthorized person to high security locations, based on access rights of different persons.*

Keywords: *Authentication, Biometric, Chip, fingerprint, PIN, Smartcard.*

I. INTRODUCTION

In this section we have to discuss about the smartcard and types of the smartcards.

1. What is a Smartcard?

Integrated Circuit Cards have conventionally come to be reputed as "Smart cards". A smart card is a card that is installed with either a chip and a memory chip or just a memory chip with non-programmable coherence. If there should be an occurrence of the microprocessor based cards we can include or erase otherwise control the qualified data on the card. While a memory chip card (for instance prepaid SIM card) it will do the predefined functionality.

2. Types of Smartcards:

There are two main distinguish the card types. On one hand it is based on the application/issuer type, on the other hand it is technical features or/and physical characteristics. For example: an ID card approved by the government the card body having the security features. It will focus on "application view". In banks there are the standard credit and debit cards, its having the multi-layer card body with printed design some optional features magnetic strip, a signature panel, a hologram and a hologram with chip. The below figure2 [Fig2] shows the classification of the smart cards, with processors and without such as memory cards. In case processor based again sub divided into three contact, contactless and hybrid.

The International Organization for Standardization (ISO) standard7810 "Identification card-physical Characteristics" define the physical properties such as flexibility, temperature and dimensions. The dimensions three different type format cards they are ID-1, ID-2, and ID-3. These are different types of ID-1 format cards, specified different formats.

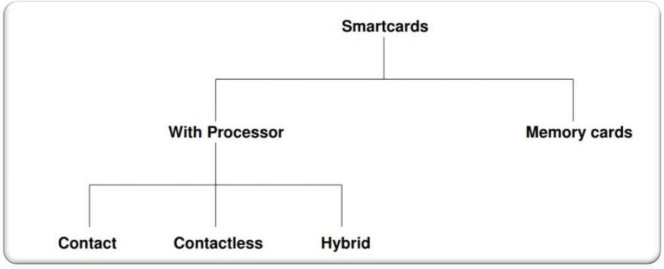

Fig1: Taxonomy of smartcards.

Some of the smartcard types are as follows:
Emboss cards: it allows for textual information and designs on the card.

Magnetic stripe: the magnetic storage capacity is 1000bits and it is consists the user information, anyone with the appropriate device we can read/write or alter the data.

Integrated circuit cards: (Smart cards): these are the cleverest augmentations to ID-1 family. The memory limits are 16Kb, 32Kb, 64Kb, and 128Kb in this usually utilized 32Kb only. Memory roles for example reading, writing and erasing could be interfaced to particular conditions, regulated by both equipment and programming. Furthermore moreover saved information can be secured. An additional point of interest of smartcards over attractive stripe cards is that they are more dependable and have longer needed lifetimes.

Memory cards: Memory cards are regularly a great deal less unreasonable and substantially less practical than microchip cards. They hold EEPROM and ROM memory, and additionally certain address and security consistency

Contactless Smartcards: it is the enhanced version of the contact based smart cards in light of their incessant failure rate. The failure focuses may be soil, wear, and whatnot. In this Cards need never again be embedded into a reader, which might enhance end client reception and which are costlier.

Optical memory cards: ISO/IEC standards 11693 and 1169 [5] define standards for optical memory cards. These cards having the piece of CD glued on-top. For today technology these cards does not have processors. This type cards carry megabytes of memory but read/write devices are expensive.

3. Essence of Smartcard:
- Authentication, Data storage, Validation, Self-lock mechanism these are the basic actions of the smartcard.

1.4 Smartcard Architecture

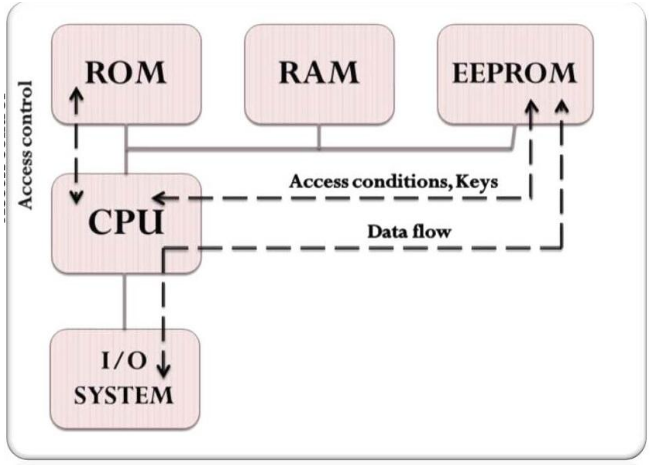

Fig1: Secure smartcard Architecture

Architecture of a typical smartcard are shown in Figure1. The smartcard processor is typically a 8-bit microcontroller-based, however, there are numerous exertions to update it to a 16-or 32-digit processor in additional later smartcards. The memory in a smartcard comprises of three distinctive memory sorts: ROM, RAM and EEPROM. The ROM is utilized for the smartcard working framework and is ordinarily installed throughout production. The RAM memory is utilized by the working framework as transitory space zone. The client accessible information fragments are distributed in the EEPROM memory portions. The predominant two sorts of memory are not ready for client access. A few levels of right to gain entrance security are backed in the EEPROM. The strategies for relegating access security could be regulated by way of utilization of a watchword or a biometrics or utilizing cryptography. Additionally while setting off to the estimations of the sharp cards it might as well go hand in hand with the some sort of ISO guidelines like 7810 and 7816, the reason for why accordingly of the previously stated measures are according to the smartcards we need to generate the bibliophiles so if our card is standard degree we can use the Universal book fans elsewise we may defy the differing inconveniences. The figure [Fig2] shows ISO models.

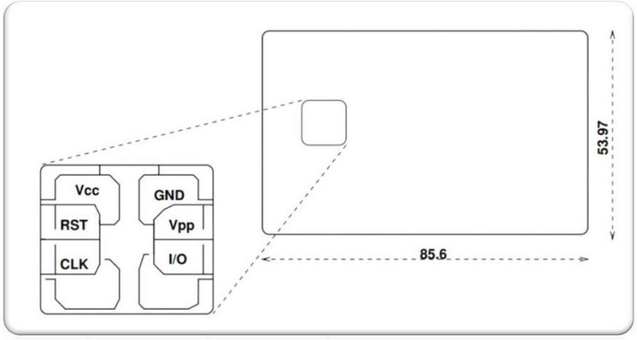

Fig2: physical dimensions of smartcard according to the ISO standards

4. Security Issues in Smartcard:

The most attractive quality of a smartcard is the assortment of security functions that it can back. At the card level, it could be ensured by numerous passwords. At the document level, we portrayed diverse sorts of right to gain entrance assurance routines in the past segment. The information substance in the card get reset if there should be an occurrence of conceivable fittings ambushes on the card. Notwithstanding the aforementioned, cryptographic confirmation can additionally be backed on numerous smartcards. Cryptographic contrivances are utilized to encode and decode contents. There are two sorts of cryptographic functional processes.

- Symmetric secret key algorithms
- Asymmetric secret key algorithms

In the symmetric algorithms the same secret key is utilized within encryption and decryption. Subsequently, it is needed that the secret key be known to both sender and receiver. In the asymmetric technique, the message is encoded utilizing public key and decrypted utilizing a private keys. The general public key is distinctive from the private key. As the name demonstrates, public key in general could be known to numerous parties. The private key is simply known to the decryption module which can decrypt the message. public key functional processes are dependent upon relating key sets comprising of a secret private key and an public key. The private secret key is administered by the possessor although general public key is known to a lot of people. This nature of public key requested systems gets ready them to work with modernized imprints. Cryptographic qualified informative content made with the secret key of the sender is called an “digital signature”. The general public key might be used to verify the signature associated with the substance without the constraint to know the secret key.

II. Historical Perspective

Smart card was invented at the close of the seventies by Michel Ugon (Guillou, 1992). The French aggregation of bankcards CB (Carte Bancaire) was made in 1985 and has permitted the dissemination of 24 million units (Fancher, 1997). For the physical qualities the first draft suggestion was enrolled in 1983. A long exchange brought about the standardization of the contact area. Afterward was the standardization of signs and methodologies which brought about norms ISO/IEC 7816/1-4. Consistent security came afterward, as it was clear from the starting that there was a need for cryptographic capacities, however this was a digit troublesome because of the confined registering force and the few bytes of RAM accessible around then (Quisquater, 1997). These days, keen cards are utilized as a part of numerous requisitions.

A study finalized via Card Technology Magazine (http://www.cardtechnology.com) exhibited that the industry had transported more than 1.5 billion sharp cards worldwide in 1999. Over the emulating five years, the industry will experience continuing improvement, in particular in cards and units to regulate electronic business and to get ready secure access to PC systems. A study by Dataquest in March, 2000, predicts very nearly 28 million smart card shipments (chip and memory) in the U.S. As per this study, a yearly development rate of 60% is wanted for U.S. sharp card shipments between 1998 and 2003. Keen Card Forum Consumer Research, circulated in right on time 1999, gives extra experiences into shopper disposition towards provision and utilization of smart cards. The business of smart card is developing quickly because of it extensive variety of provisions.

III. Biometric Authentications

Users personalities are verified utilizing one or a greater amount of several bland routines (sorts): something they know (PINs, passwords, memory phrases, and whatnot.), something they have (a physical token for example an attractive stripe card, a physical nexus, a smartcard, and whatnot.), or something they are (biometric verification). Assuming that this informative content is accumulated by a trusted technique, verified, and after that marked by a trusted authority, it could be acknowledged as trusted confirmation authentication information (AI).

Numerous distinctive sort of biometric ascribes to recognize clients. They may be based upon fingerprints, hand or facial geometry, iris patterns, or even address distinguishment. Every of these advances might be acquired from various origins, with distinctive functional processes and procedures for archiving a distinct qualities or investigating "lives can" of a distinct headlines to the formerly saved record. This record commonly pointed to as the "Biometric Template". Biometrics might be best described as a rising engineering.

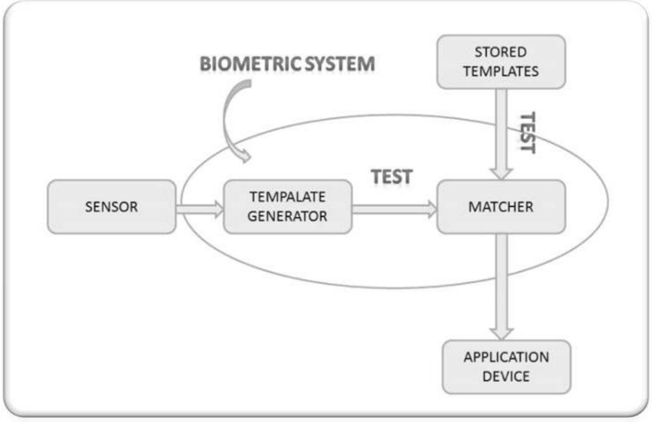

Fig4: Biometric Authentication system

Consistent with the Biometric validation framework [Fig4] the sensor block produces the either the nexus facial component or the unique finger impression of the user then extractor create the template given to the generator it create the test plan and sent to the matcher then an additional data of the matcher is the saved as template, the matcher basically checks the two templates and given to the relating provision mechanism.

IV. Fingerprint Identification

In unique finger impression distinguishing proof there are some angles that must be taken in attention, for example: finger impression matching, representation value, FAR/FRR or template space.

1. Fingerprint matching:

Finger impression matching figures out if two fingerprints are from the same finger or not. Numerous finger impression verification systems have showed up in written works over the years. As a rule, the two most conspicuous headlines utilized within finger impression matching are edge finishing and edge bifurcation called particulars. The equation utilized within particulars correlation needs a particular mode of archiving qualities, utilizing polar coordinates, which moreover carries the playing point of lessening the memory space required.

The parameters are:

- The minutia point of X and Y coordinates
- Orientation, defined as the local ridge orientation of the
- Associated ridge.

2. Image Quality:

Quality is exceptionally critical to realize elevated operational exhibition. Some of requisitions have progressed input dialog memos which furnish convenient informative data about downtrodden value outputs, of the finger impression. There ought to be great equalize between the programming and selecting officer.

3. False Acceptance/False Rejection:

The False Acceptance Rate (FAR) is the rate at which the gadget might be distinguish a good client, numerous outlets are quote their mechanisms as a false reception rate, it ought to be exceptional the same as level. Yet it paramount to recollect that throughout client verification (a balanced match), false reception is dependent upon faker tries, not on the aggregate number of tries by bona fide clients. In the event that the FAR is 1 percent, that means one out of 100 clients attempting to break into the framework can be efficacious.

The False Reject Rate (FRR) is the rate at which a substantial client is dismissed by the framework. m. A 1% FRR might infer the normal client might flop each hundredth time. On the other hand, it is more probable that just a couple people might slip up a ton more regularly. The aforementioned single may be channels for an optional verification instrument. Numerous frameworks, for example the unique mark-distinguishment units, may be tuned to do less strict checking at the expenditure of opening the framework.

V. About application

By using the smartcard and fingerprint we propose the development of authentication system. The motto of the application is the identifying the user PIN and fingerprint for corresponding card holder. The below figure [Fig5] shows the smartcard configuration means the enrollment the fingerprint until the good image will be captured. Then that should be loaded into the card.

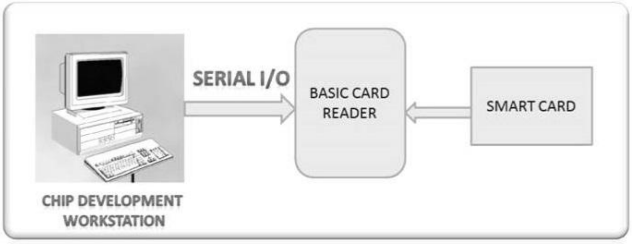

Fig5: Basic smartcard configuration.

The below flow diagram [Fig6] shows the complete flow of the application. Firstly prepare the hardware corresponding to our application. Then after power up the reader waits for the smartcard when we are inserted into it asks the PASSWORD or PIN number then card extracts the user details and fingerprints. At that time the fingerprint scanner waits for the minutia, if both the stored template and the generated template is matched , access granted otherwise it should be access denied again its go to the start otherwise the process go to the end.

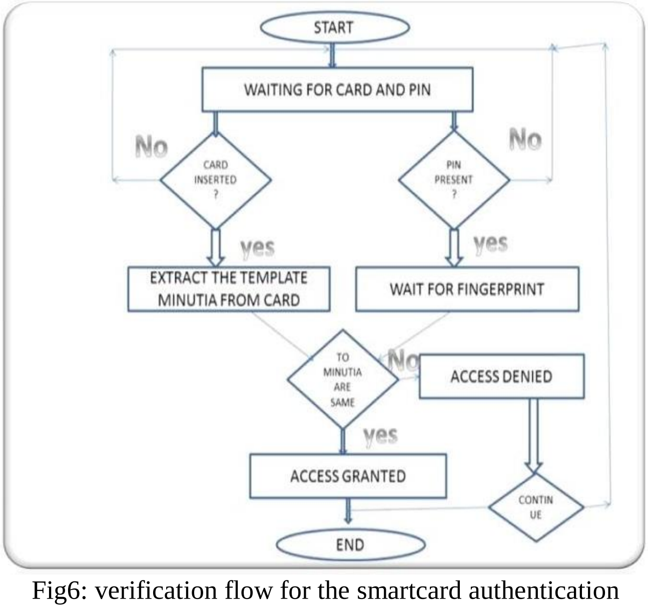

Fig6: verification flow for the smartcard authentication

VI. Benefits of Combining Smart Card Technology, Password and Biometrics

The combination of smart cards, biometrics and password delivers a number of significant benefits to organizations implementing secure identification system.

1. Enhanced Privacy

Utilizing smart card technology essentially improves protection in biometric ID system. The smart card furnishes the single person with a private database, a private firewall and a private terminal. It secures private qualified data on the card with progressed cryptography and digital signatures to avoid change or trade of biometric information and to anticipate cloning of the card. This permits the single person to control access to their biometric qualified information and kills the requirement for mid database access throughout character verification.

A smart card based ID system likewise gives the cardholder control over who can access private informative data saved on the card. Biometric and password further updates this control, ensuring that equitable the honest cardholder can authorize access to personal informative data.

2. Enhanced Security

Biometric advances are utilized with smart card technology for ID system requisitions particularly because of their capacity to distinguish individuals with negligible equivocalness. A biometric-based ID considers the verification of “who you case to be” (qualified data concerning the cardholder printed or saved in the card) dependent upon “who you are” (the biometric qualified information archived in the shrewd card), in place of, or likely notwithstanding, checking “what you know” (for example a PIN). As indicated in Figure [Fig7], this expansions the security of the generally speaking ID system and enhances the correctness, speed, and control of cardholder validation.

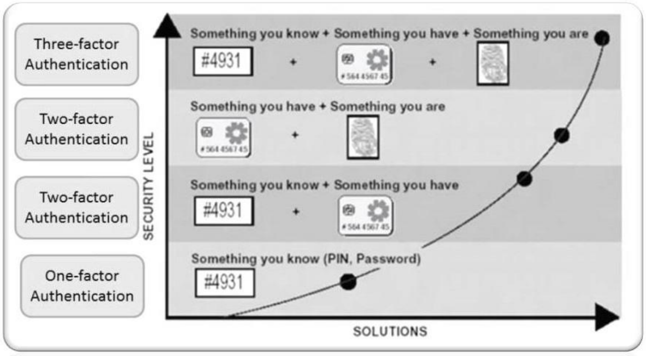
Three-factor Authentication
Two-factor Authentication
Two-factor Authentication
One-factor Authentication
SECURITY LEVEL
SOLUTIONS
Something you know + Something you have + Something you are
#4931
+
#564 4567 45
+
Something you have + Something you are
#564 4567 45
+
Something you know + Something you have
#4931
+
#564 4567 45
Something you know (PIN, Password)
#4931

Fig 7: Impacts of smart cards and Biometrics on Security

3. Improved System Performance and Availability

Saving the biometric template on a smart card increments on the whole system performance and cardholder advantage by permitting neighborhood personality verification.

The character of a distinctive is built and validated around then the smart card is issued and the distinct has demonstrated qualification to accept the identity card. From that focus on, the client's personality is validated by way of the presentation of the smart card to a card reader, without the necessity to perform a pursuit and match opposite a remote database over a system. This neighborhood handling can lessen the chance to validate a single's personality to one second or less, permitting quicker security checks, and decrease the necessity for the card book lovers to be connected with a central system.

The requisitions where snappy and successive utilization is indispensible (e.g., regulating access to buildings and at airports), contactless smart cards can speed the exchange of biometric templates and dispose of the requirement to make a physical connection. Ease, contactless smart cards with elevated conveyance velocities are currently ready that have enough memory to store an interesting unique mark template (fingerprint) or photographic representation. These methods are higher security biometrics-based ID system can utilize contactless smart card technology to attain an extent of security, throughput and cost objectives.

4. Improved Efficiency

Utilizing the mixture of smart card technology with biometrics for distinguishing proof and confirmation of people gives the most productive execution of a secure authentication system.

5. Upgradability and Flexibility

A crux prerequisite for any recognizable proof framework is the capability for the framework to be overhauled without requiring extensive backings in new framework. Case in point, there may be a need to adjust the framework without supplanting the single ID cards if a security plan is traded off or if upgraded proficiencies get ready. On the grounds that smart cards hold rewritable information space, and in certain cases rewritable system space, they permit the most adaptability for upgrades to card information and card-framework communication ordered systems and for secure administration of various requisitions on a specific card.

VII. Conclusion

Biometric ID is inclined toward over the universal systems on the grounds that the individual to be recognized is instructed to be physically showed at the purpose of distinguishing proof and likewise recognizable proof dependent upon biometric systems.

For authenticating yourself, there are basically 3 methods: something you know (a shared secret, or password), something you have (a token/card), or something you are (biometrics). A smartcard is two factors, since it needs both something you know (the PIN) and something you have (the card itself). There are also prototypes of cards with an integrated fingerprint scanner, which constitute a robust three factor authentication.so your security will be that much better compared to two factor smartcards.

References

[1]. Gammel, B.M and Ruping, J. "Smart cards insides" IEEE Spectrum , conference publications, PP 69-74, 12-16 Sept. 2005.

[2]. KUMAR,P.Y GANESH, T.S "INTEGRATION OF SMART CARD AND GABOR FILTER METHOD BASED FINGERPRINT MATCHING FOR FASTER VERIFICATION" IEEE, CONFERENCE PUBLICATIONS, PP 526 - 529 , 11-13 DEC. 2005

[3]. Hsien-HauChen ,Yung-Sheng Chen , Hsia-LingChiang , Chung-Huang Yang "Design and implementation of smartcard-based secure e-mail communication" IEEE Conference Publications, PP 225 – 231, 14-16 Oct. 2003.

[4]. Chang, C.-C, Hwang, R.-J , Buehrer,D. "Using smart cards to authenticate passwords"IEEE Conference Publications, PP 154-156, 13-15 Oct 1993

[5]. CHAN,P.K. CHOY, C.S , CHAN, C.F , PUN, K.P, "PREPARING SMARTCARD FOR THE FUTURE: FROM PASSIVE TO ACTIVE", IEEE, PP 245 – 250, FEB 2004

[6]. LASSUS,M. "SMART-CARDS-A COST-EFFECTIVE SOLUTION AGAINST ELECTRONIC FRAUD" IEEE,PP 81 - 85 , 28-30 APR 1997.

[7]. MEI HONG ,HUI GUO , BIN LUO ." SECURITY DESIGN FOR MULTI-SERVICE SMART CARD SYSTEMS" IEEE,PP 299 - 304 , 13-15 DEC. 2008

[8]. SIMPSON, M.C.S. "SMART POWER; A SMART CARD ELECTRICITY PAYMENT SYSTEM" IEEE,PP 3/1 - 3/4 , 23 JAN 1996

[9]. Selimis,G. Fournaris, A. Kostopoulos, G , Koufopavlou, O. "Software and Hardware Issues in Smart Card Technology" IEEE, PP 143 – 152, 3rd Quarter 2009

[10]. ISO 7810 "Identification cards – Physical characteristics"

[11]. Fancher C. H. (1997), In your Pocket: Smartcards, IEEE Spectrum (February),pp. 47-53.

[12]. Stefano Zanero *"Smart card content security"*(http://home.dei.polimi.it/zanero/papers/scsecurity.pdf).

[13]. W.-S.Juang. Efficient multi-server password authenticated key agreement using smartcards. IEEE Transactions on Consumer Electronics, 50:251–255, 2004.

[14]. BIOMETRIC FEATURES EMBEDDED IN A SMART CARD SYSTEM FOR CONTROL ACCESS 8th international conference on Development and Application system Suceava, Romania, May 25 – 27, 2006

[15]. Guillou L. C., et al. (1992), The smart Card: A Standardized Security Device Dedicated to Public cryptology, in G.J. Simmons (Ed.), Contemporary Crypto- logy. The Science of Information Integrity, IEEE Press, pp. 561-613.