BSC: A Novel Scheme for Providing Security using Biometric Smart Card

S. Mahaboob Hussain
Dept. of CSE
UCEV, JNTU Kakinada
Vizianagaram

A. S. N. Chakravarthy, Ph.D
Associate Professor
Dept. of CSE
UCEV, JNTU Kakinada
Vizianagaram

G. S. Sarma
Assistant Professor
Dept. of E C M
K L University

ABSTRACT
Technology advances day by day and the new things are being developed. There are many new technologies being introduced and developed in any discipline. Data Security plays a vital role and Biometric security systems is one of the new trends to be developed, which has its advantages for controlling access, protecting sensitive data, tracking on-line systems, etc.,. Biometric technologies such as fingerprint, face and iris recognition have seen an increasing interest throughout the past decades to increase the security, convenience, accountability. Such interest has been intensified with various large-scale initiatives from governments that seek to incorporate biometric technologies for the purposes of identification, verification and for fraud detection and deterrence. Being purely ad hoc technological implementations, biometric devices are now seen as being of strategic value and consequently of strategic importance. With the perception of better efficiency and effectiveness, governments are beginning to embrace biometric technologies. Industry is also geared up to sell the products, and all over the world businesses are looking to incorporate biometrics for many different uses ranging from access-control to e-commerce and entertainment. Biometrics and smart cards are two of the most powerful security solutions available today. This paper introduces a new mechanism to provide better security and services with Biometric Smart Card technology including hybrid biometric security, i.e., with the combination of security for fingerprint pattern and for the smart card.

General Terms
BSC, NFC, PIN, X.509, Authentication, Security Mechanism, RSA Algorithm, Cyber Forensics.

Keywords
Biometrics, Biometric Security, Fingerprint patterns, Smart Cards, Biometric Smart Cards, Certification Authority.

1. INTRODUCTION
The word biometrics comes from the Greek language and is derived from the words *bio* and *metric* which means *life, to measure* respectively, which refers to the automatic identification or identity verification of living persons using their enduring physical or behavioral characteristics. In general, biometrics offers a more secure and friendly way of identity authentication [1, 2]. The two main classes of the biometrics characteristics in the modern approach are *Physiological* and *Behavioral.*

- Physiological are related to the shape of the body and thus it differs from person to person finger prints, face recognition, hand geometry and iris recognition are some examples of this type of biometric.
- Behavioral are related to the behavior of a person. Some instances for this case are signature, key stroke dynamics and voice. Sometimes voice is also considered to be a physiological biometric as it differs from person to person.

Biometrics is the automated approach to authenticate the identity of a person using individual's unique physiological or behavioral characteristics. Biometrics is based on a unique trait which is part of our human body. So, no need to worry about forgetting it, losing it or leaving it at some place. Since it is unique, it is more difficult for others to copy, duplicate or steal it. i.e., these biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. These characteristics can uniquely identify a person, replacing or supplementing traditional security methods by providing two major improvements: personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes.

The two general uses of biometrics are identification and verification which both require the existence of reference data that the person's measured traits will be compared with reference templates or raw data.

A biometric data sample is compared against the respective biometric data of every person enrolled in the database or against a single reference template of a particular enrolled individual in order to confirm the identity of that person respectively. When a biometric system correctly identifies a person, then the result of the identification process is a true positive, whereas if the system correctly rejects a person as not matching the respective enrolled template, the result is a true negative. Similarly, when the system incorrectly identifies or rejects a person then we speak about a false positive or a false negative, the security aspects of which will be discussed in a subsequent section.

This paper mainly discuss about the new approach for identifying and verifying an individual identity using finger print and smart card security on BSC (Biometric Smart Card). The subsequent sections analyses the principles of biometrics, different types of finger scans, and the applications of finger scans. Lastly, we discuss about Biometric Smart Card design, implementation and working.

2. PRINCIPLES OF BIOMETRICS
Biometrics is also a science of measuring which is used to distinguishing physical characteristics. Biometric technology works on basic principles called Verification and Identification [4]. Verification is the process of determining

the identity of a person and confirming his or her identity and it verifies that you are the one you say you are. Identification means collecting your information and finding out who you are. Verification requires a one-to-one comparison between the biometric sample just acquired and the reference template stored. Identification requires comparing the biometric sample against every reference template contained within the database. It involves one-to-many comparisons. Biometric verification shows better performance when the number of biometric references is very high and it is faster than identification.

In general, there are lot of technologies like Finger scan, Facial scan, Iris scan, Retina scan, voice scan, Signature scan, Keystroke scan and Hand scan and etc. Among them, a Finger scan technology is the oldest of the biometric sciences and utilizes distinctive features of the fingerprint to identify or verify the identity of individuals. Finger scan technology is the most commonly deployed biometric technology, used in a broad range of physical access and logical access applications [5].

Dermatoglyphics is the scientific study of fingerprints. It is the ridged skin covering our palms and sole, are not only found on human beings but also be found on the paws of certain mammals and on the tails of some monkey species [9]. The drag against the ridges when feeling the texture of a surface heightens the intensity of stimulation of the nerve endings.

Ridges are extremely narrow in infants and gradually broaden with age. Despite this fact, there are no changes in the ridge patterns themselves, which is why fingerprints are used for identification [9]. The patterns such as the stripes of zebras, the arrangement of hair on the body, sand whipped by wind or waves, and magnetic field patterns are also called Dermatoglyphics.

Generally there are three basic fingerprint patterns, which are classified by Galton, are the whorl, the arch and the loop. A number of other fingerprint patterns, which are generally variations of these basic three, have been recognized such as the twin loop and the central pocket loop as shown in the below Figure 1.

Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger [19].

Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side [19].

Whorl: Ridges form circularly around a central point on the finger [19].

Fig 1: Basic finger prints patterns Arch, Loop, Whorl

The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint.

Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical [7, 19]. Worldwide, fingerprints harvested from crime scenes lead to more suspects and generate more evidence in court than all other forensic laboratory techniques combined [13].

2.1 Finger Scan Verification and Identification

According to the author [15], there are five stages involved in finger-scan verification and identification.

- Fingerprint image acquisition
- Image processing
- Location of distinctive characteristics,
- Template creation
- Template matching

Generally, a scanner takes a mathematical snapshot of a user's unique biological traits. All these collected snapshots were saved in a fingerprint database as a minutiae file. The main challenge task of a finger scanning system is to acquire high-quality image of a fingerprint. The quality of the image of a finger print is measured in dots per inch (DPI), more dots per inch means a higher resolution image. Generally as per in the market, the Lower DPI found is in the 300-350 DPI, but the standard for forensic quality fingerprinting is images of 500 DPI [5]. Image acquisition can be a major challenge for finger scan developers, since the quality of print differs from person to person and from finger to finger. Some populations are more likely than others to have faint or difficult-to-acquire fingerprints, whether due to wear or tear or physiological traits. Some of the reasons are that affect the quality is to taking an image in the cold weather. One of the techniques to putting oils in the finger helps to produce a better print but in cold weather, these oils naturally dry up.

2.2 Characteristics of Fingerprint Patterns

Friction ridges are the basic bio metric patterns measures which are begin forming during the 12^{th} week of gestation. These fingerprint patterns remains permanent for the life of the individual until the body decomposes after death. As per the huge survey, authors found that no two fingerprints have ever been found to be alike. Nearly 100 years of evidence and practical experience of various researchers has supported the uniqueness and permanence of fingerprint arrangements. In twins, each of the twenty fingerprints will be unique which are cannot be easily differentiate by the modern DNA technology. Each fingerprint contains minutiae, or ridge characteristics [18]. To justify whether the unit relationship between the two individuals are matched and the characteristics occupy the same relative area and position, fingerprints impressions of the individuals will be identified by examining and comparing the ridges [18].

All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization [6].

These unique fingerprint traits are termed *minutiae* and all the required comparisons are made based on these traits. On average, a typical live scan produces 40 "minutiae". The Federal Bureau of Investigation has reported that no more

than eight common minutiae can be shared by two individuals.

Image processing is the process of converting the finger image into a usable format. This results in a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys. At this stage, image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat and dry skin.

3. CLASSIFICATION OF FINGER PRINTS AND BASIC PATTERNS

Fingerprints are classified by general shape, positions like arch, loop, or whorl within the finger, and relative size [10, 18]. Classification of fingerprints provides for an orderly placing of fingerprint cards in a file [18]. Classification of the fingerprints will be done in two methods, they are: Henry Classification and NCIC Classification.

Fingerprints offer a completely trustworthy and sure means of personal identification. There is an essential explanation for fingerprints by the author [12], having replaced other methods of establishing the identities of criminals reluctant to admit previous arrests. Fingerprint patterns are basically classified into three types that are: loop, whorl and arch patterns which are discussed below [11, 17].

3.1 Loop Patterns

In a Loop pattern, the ridges will flow in one side, re-curve, (loop around) touch or pass through an imaginary line drawn which is in between delta and the core, and exit the pattern on the same side from which it entered. A loop pattern has only one delta. There are two types of loop patterns: (1) Ulnar loop (2) Radial loop shown in the below Figure 2.

Fig 2: Ulnar loop (left), Radial loop (right)

Nearly about 60-70% of the fingerprints patterns will be occur in the Loop. In this pattern some of the ridges will enter through any side of the impression it may touches or crosses or re curve the line which running between delta and the core. It terminates on the line or in the way where the ridge or the ridges entered direction. With at least one core and one delta in the loop pattern fingerprints gives the ridge count. The name radial loops are named after the radius [17, 20].

In the radial loops the flow of the pattern runs in the direction of the thumb i.e., towards radius. Most of the time radial loops will be found on the index fingers because radial loops are not very common as other loops.

3.2 Whorl Patterns

A whorl pattern consists of a series of almost concentric circles and it has two deltas. These patterns are of four types: Plain whorl, Central Pocket Loop whorl, Double Loop whorl, Accidental whorl.

Fig 3: Pocket Loop whorl, Double Loop whorl, Accidental whorl

In the above Figure 3, one can observe that whorls encountered nearly 25-35 % of fingerprint patterns. In this type of patterns, some of the ridges in the fingerprints pass through at least one circuit. Any whorl fingerprint pattern contains two or more deltas.

3.2.1 Plain whorl patterns

These types of Plain whorls consists more than one ridge which can make or helps to make a complete circuit with two deltas, between which an imaginary line is drawn and at least one re-curving ridge within the inner pattern area is cut or touched [17].

3.2.2 Central pocket loop whorls patterns

Central pocket loop whorls consist of at least one re-curving ridge or an obstruction at right angles to the line of flow, with two deltas, between which when an imaginary line is drawn, no re-curving ridge within the pattern area is cut or touched. Central pocket loop whorl ridges make one complete circuit which may be spiral, oval, circular or any variant of a circle [20].

3.2.3 Double loop whorls patterns

Double loop whorls consist of two separate and distinct loop formations with two separate and distinct shoulders for each core, two deltas and one or more ridges which make, a complete circuit. Between the two at least one re-curving ridge within the inner pattern area is cut or touched when an imaginary line is drawn [17, 20].

3.2.4 Accidental whorls patterns

There are two different types of patterns in accidental whorls which does not consists arch and having two or more deltas or a pattern which possess some of the requirements for two or more different types or a pattern [20].

3.3 Arch Patterns

The ridges in an arch fingerprint pattern flows in one side and flows out the opposite side and it consists of no deltas in fingerprint patterns. Arch patterns are classified into two types: Plain Arch, Tented Arch.

Fig 4: Plain Arch (Left), Tented Arch (Right)

In the above Figure 4, comparing to the other patterns, about 5% of arches are found in fingerprint patterns. The ridges in these patterns don't make any backward turns and they run from one side to the other of the patterns. Mostly there will be no formation of deltas in an arch pattern, but if any delta exists, there will be no re-curving ridge involved and changed between the core and delta points. Basically arch patterns are classified into: plain arches, radial arches, ulnar arches and tented arches. Plain arches have an even flow of ridges from

one side to the other of the pattern; no significant up thrusts and the ridges enter on one side of the impression, and flow out the other with a rise or wave in the center [17] as shown in the Figure 4. The ridges of radial arches consists one delta with no re-curves and they slope towards the thumb. Ulnar arches patterns consists of one delta with no re-curve ridges with slope towards the little finger. Tented arches have an angle, an up thrust, or two of the three basic characteristics of the loop [17]. They don't have the similar flow that plain arches do and particularly near the middle they have significant up thrusts in the ridges that arrange themselves on both sides of a spine [20]. The two innermost ridges which start parallel, diverge, and surround or tend to surround the pattern area. If there any definite break exists in a type line of the pattern, the ridge which is immediately outside of it is considered as its continuation of the braked line [18].

Table 1 Frequency of occurrence of different pattern types on each finger

Galton types:		**Whorls**				**Loops**		**Arches**		
Digit	**Side**	**Whorls**	**Lat.pockets +twin loops**	**Central pocket**	**Acciden-tals**	**Ulnar**	**Radial**	**Tented**	**Other**	**Indeter-minable (nr)**
1sThumb	R	31.86	8.79	0.74	0.04	55.89	0.22	0.02	2.45	15
	L	19.19	9.84	0.36	0	65.9	0.2	0	4.51	12
	R+L	25.52	9.32	0.55	0.02	60.89	0.21	0.01	3.48	
2 Index	R	25.03	2.94	2.4	0.42	32.3	26.03	2.3	8.57	41
	L	22.02	3.5	2.01	0.62	38.1	23.37	1.95	8.41	32
	R+L	23.52	3.22	2.21	0.52	35.2	24.7	2.13	8.49	
3 Middle	R	13.98	1.39	1.15	0.04	74.81	2.53	0.6	5.49	29
	L	13.21	2.11	0.8	0.06	73.32	2.51	0.86	7.12	26
	R+L	13.59	1.75	0.98	0.05	74.07	2.52	0.73	6.3	
4 Ring	R	34.85	0.64	5.5	0.08	55.61	1.47	0.02	1.83	21
	L	22.11	1.07	4.64	0	68.92	0.5	0.08	2.67	25
	R+L	28.48	0.85	5.07	0.04	62.27	0.98	0.05	2.25	
5 Little	R	11.41	0.38	2.01	0	85.46	0.2	0	0.54	22
	L	6.86	0.62	1.53	0.02	89.79	0.02	0.02	1.15	26
	R+L	9.13	0.5	1.77	0.01	87.62	0.11	0.01	0.84	
all digits	R	23.43	2.83	2.36	0.12	60.83	6.08	0.59	3.77	128
	L	16.68	3.43	1.87	0.14	67.21	5.31	0.58	4.77	121
	R+L	20.05	3.13	2.11	0.13	64.02	5.69	0.58	4.27	249
Galton types:	R	**28.74**				**66.91**		**4.36**		
	L	**22.12**				**72.53**		**5.35**		
	R+L	**25.43**				**69.72**		**4.86**		

The above Table 1 shows the fingerprint pattern distribution for a total of 5000 individuals [9]. It gives an indication of the frequency of occurrence of different pattern types on each finger from 1-5 i.e., thumb to pinky. Some of the scientists have found that family members often share the same general fingerprint patterns leading to the belief that these patterns are inherited [8, 19].

4. DESCRIPTION AND WORKING OF BIOMETRIC SMART CARD

Generally a smart card is a type of chip card which is made up of a plastic card that contains an embedded computer chip which stores and transacts data like a memory or microprocessor type. This data is stored and processed in cards chip that are usually associated with either value, information, or both. A reader is used to transfer the card data which is part of a computing system. Several key applications like healthcare, banking, entertainment, security and

transportation systems that are using today are enhanced with smart cards. In this paper authors introduce security and features that can provide more benefit to the BSC which are used in various applications. The present markets which are traditionally served by other machine readable card technologies, such as magnetic stripes and barcodes, are converting to smart cards for the better security and for easy access of the applications [14].

By using Biometric Smart cards one can improve the convenience and security of any transaction and can provide tamper proof storage of user and account identity. By using these smart card systems it is to be more reliable than other machine readable cards, like magnetic stripe and barcode and also it provides vital components of system security for the exchange of data throughout virtually any type of network. Worldwide, people are now using smart cards for a wide variety of daily tasks [14].

In this paper authors introduced a new mechanism for the security and authentication of a smart card using dual security techniques i.e., for fingerprint pattern and chip of the smart card and for BSC.

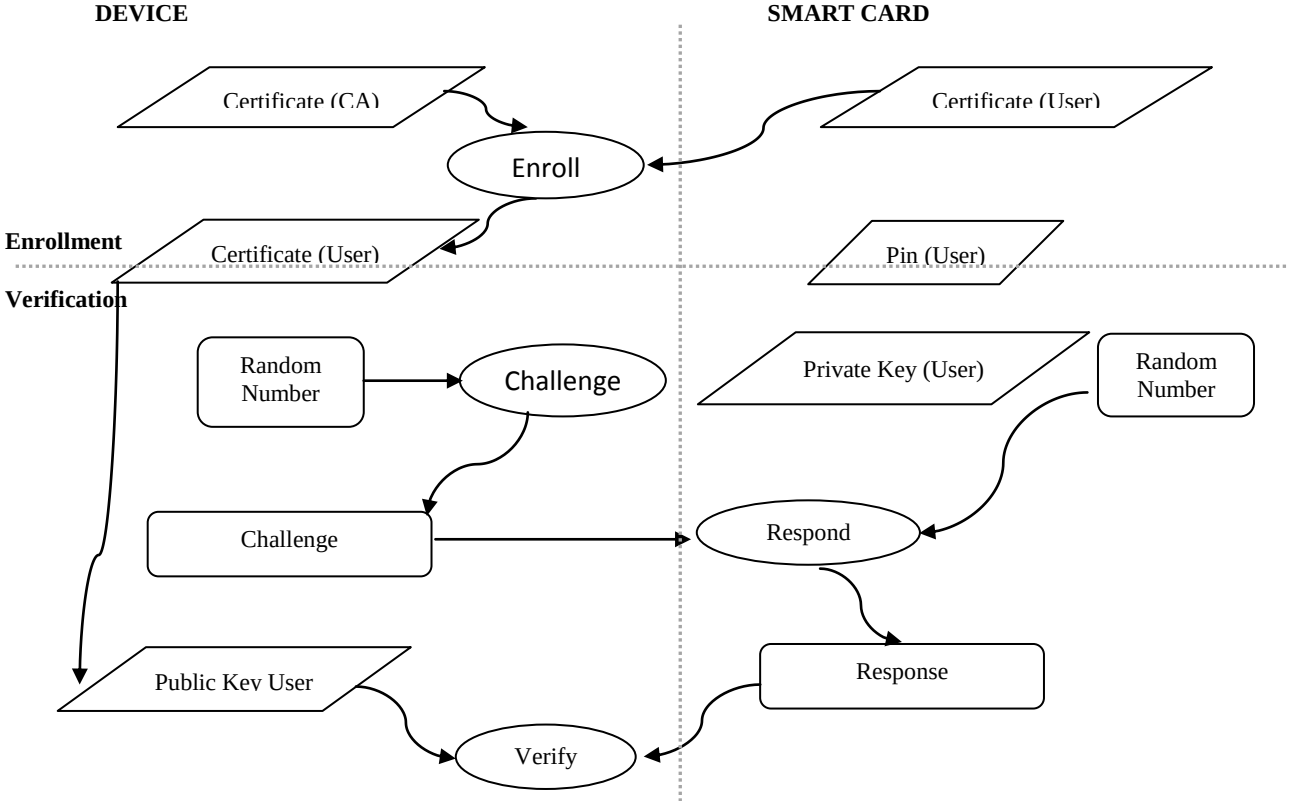

Fig 5: Authentication mechanism

The biometric identity smart card authentication modes are finger prints and password for the chip inserted in to the card. The biometric application stores and verifies users' fingerprint information directly on the smart card for added security. The fingerprint information never leaves the card and is never stored in a database, thus it protects users' digital identities.

For a smart card to allow access, it typically requires the user to input a PIN (Personal Identity Number) first, to verify that the individual in possession of the card is the person to whom the card was issued. Incorrect PINs keep the card from functioning and eventually cause it to lock. Once the PIN is successfully entered, a dialogue between the PDA and smart card occurs, by which the PDA confirms that the card and the credentials of the user on the card are valid and correspond to that of the PDA owner.

This paper introduces the biometric authentication solution enhanced the end-user experience by providing added convenience and flexibility for secure network access. Fingerprint biometric credentials are stored on the smart card that they are uniquely portable and can be used with any hardware system that has a smart card reader and fingerprint sensor.

The underlying mechanism used to authenticate users via smart cards relies on a challenge response protocol between the device and the smart card. The PDA challenges the smart card for an appropriate and correct response that can be used to verify that the card is the one originally enrolled by the device owner [3]. The PDA relies on user credential information, obtained earlier from the smart card when the PDA owner initially enrolled the card with the device.

The above Figure 5 describes the authentication mechanisms to authenticate a user to the PDA [3]. It illustrates a typical exchange, omitting the requisite PIN satisfaction step that occurs.

The first part of the diagram shows the enrollment information exchange used to register a card (at right) with the PDA (at left), while the remainder show the exchanges used to verify the claimed identity.

Before the smart card can be enrolled at the device, it must first be personalized for the user. The personalization step is essentially another enrollment process whereby a security administrator enrolls the user on the card (i.e., user enrollment), by populating it with the user's credentials, PIN, and other information. Those credentials are obtained from

the card when it is enrolled with the device (i.e., card enrollment) and validated using the certificate of the Certification Authority (CA) who issued the credentials or is otherwise the point of trust for validation.

Note that, at a minimum, the user name is needed to enroll. The CardEnroller tool first establishes a secure channel of communication with the card, and then performs the following steps in the below Figure 6.

Load the Enroll applet onto the card (deleting possible old applet instances), then asks the user for a PIN (4-8 decimal digits) and set the user PIN. Verifies the user PIN just set (it will ask again the user for the PIN). It generates a pair of RSA keys and a X.509 certificate for the user and stores the private key and the certificate onto the card.

To sign the certificate, the Card Enroller application needs its private key, which was stored in a file encrypted with a password, *Preparing Card Enroller keys and certificate*, one must provide the same password when prompted by Card Enroller.

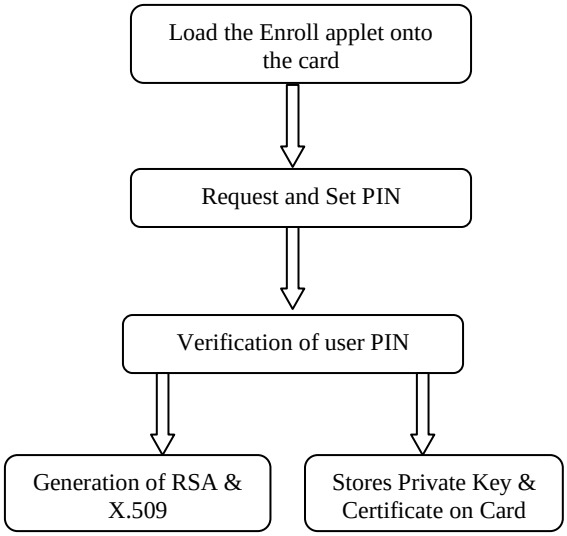

Fig 6: Authentication and verification process

One can also see the steps performed by the Card Enroller's at the bottom of application main window. The other menus of the Card Enroller application can be used to [22]:

- Display the last certificate generated by the Card Enroller tool or read from the smart card i.e., the menu "View/Last Certificate".
- Extract and display the certificate from a XMC card i.e., the menu "View/Card Certificate".
- Generate a new RSA key pair and certificate i.e., the menu "Action/Get Certificate".

Action/Enroll also generates new user keys and certificate so that the old ones will be lost and that will be used to personalize the smart card [22].

- Save the last certificate generated by the Card Enroller tool or read from the smart card to a file in PEM format by using the menu "Action/Save Certificate".

If the certificate was generated by the tool together with the keys and not simply read from the smart card, then the associated private key will also be saved encrypted with a password if you check the menu "Action/Save Private Key".

4.1 Design and Implementation

4.1.1 Card Personalization

In this Biometric Smart Card, the personalization of the card involves populating information such as the user's name and credentials into files maintained on the smart card, before issuing to a user and also include the biometric pattern of the user [22]. In addition, the procedure usually entails recording a PIN on the card, which the user later enters to enable the card to confirm that the holder is the same person who was issued the card.

Figure 7 shows, the processing and templates storing on BSC by the collected finger print patterns.

4.1.2 Token Management

The proposed Enroller applet is designed for use in different types of applications, for example like Rennes's' X-Mobile Cards (XMC) and other Java Card-compliant smart cards [22]. This applet participates both in the personalization of the card and the authentication process.

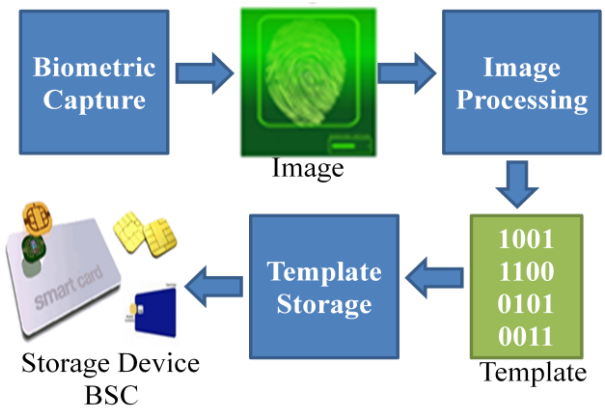

Fig 7: Processing and storing data on BSC

The applet conforms to Java Card 2.1.2 specifications and supports secure channel communications between a host application and itself as specified in Global Platform 2.1. The Enroller applet has the following functionality [22]:

- Supports the optional creation of a secure channel of communication between the host application and the applet.
- Generates an RSA private/public key pair of 4 (1024 bits).
- Stores an RSA public or private key (1024 bits) onto the XMC card.
- Retrieves the RSA public key previously stored on the XMC card.
- Stores an X.509 certificate as a byte array on the XMC card.
- Sets user PIN.
- Verifies user PIN.
- Replies to a host challenge by signing it with the private RSA key previously stored on the XMC card.

4.1.3 Protection

For user authentication the fundamental threat is an attacker impersonating a user and gaining control of the device and its contents. These Smart cards are designed to resist tampering and monitoring of the card, including sophisticated attacks that involve reverse engineering, fault injection, and signal leakage [22]. Presuming those designs are effective, the

following vulnerabilities are the main candidates for exploitation:

- The authentication mechanism can be bypassed.
- Weak authentication algorithms and methods are used.
- The implementation of a correct and effective authentication mechanism design is flawed.
- The confidentiality and integrity of stored authentication information is not preserved.

With all the above working principles of smart cards, this paper describes a process to create highly secured Biometric smart card by providing two tier security systems. As shown in the below Figure 8, initially in Tier-1, Authors provide security with the parameters mentioned in the paper for the chip and as well as for the Biometric patterns separately. In Tier-2, security is provided for the BSC i.e., Biometric and Chip combined by some security mechanisms. Thus Biometric smart card will be provided with high security in two levels by using this two tier mechanism.

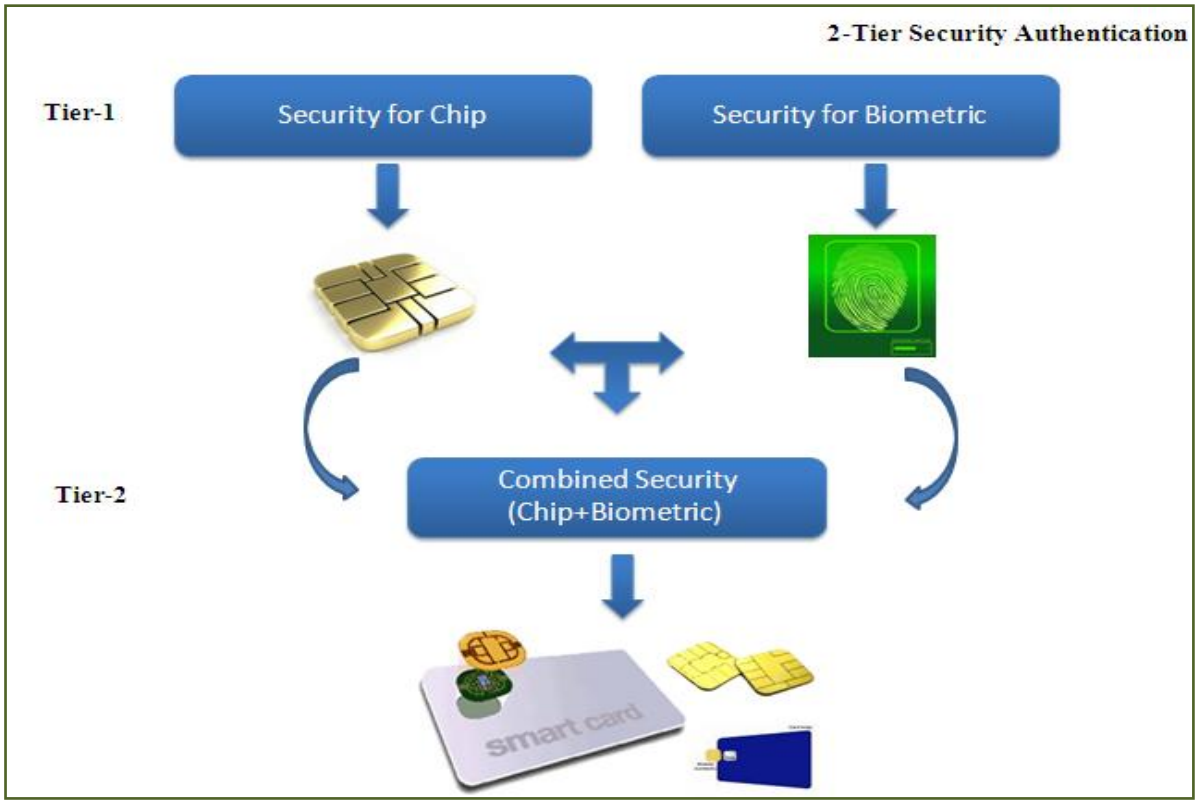

Fig 8: Dual Security mechanism in BSM

The above Figure 8 illustrates the security authentication mechanism for BSC with all the principles of security mechanisms for biometric patterns and smart cards mentioned in this paper.

5. APPLICATIONS OF BSC

BSC plays an important role in various fields with high security and authentication mechanisms for reducing different types of cyber crimes and now-a-days BSC with dual security systems will be efficiently used in various applications. This paper presents some of the applications where the security need is relatively high.

5.1 Citizen Facing Applications

The below defining element of citizen facing applications is that a government body, normally a state or federal agency, provides authentication and enforces compliance with BSC systems match decisions [16]. Citizen Facing Applications include:

- Criminal identification
- Citizen identification
- Surveillance

5.2 Employee Facing Applications

The below defining element of citizen facing applications is that an institution, be it in the public or private sector, provides authentication and enforces compliance with BSC systems match decisions[16]. These are generally closed systems, incorporating a department, a division, or an entire institutions staff. They include:

- PC/Network access
- Physical Access/Time attendance

5.3 Customer Facing Applications

The below defining element of customer facing applications is that a provider of goods or services provides authentication of consumers and enforces compliance with BSC systems match decisions. These are generally open systems, incorporating some percentage of a seller's customer base [16]. The applications are,

- E-Commerce Telephony
- Retail/ATM/Point of sale

5.4 Biometric Vertical Market

A large percentage of biometric deployments occur within five key vertical markets. In these vertical markets, the BSC can serve to increase security and reduce fraud, and it

provides functionality not achievable through other authentication methods [16]. Following are some of the applications:

- Law Enforcement
- Government Sector
- Financial Sector
- Health care
- Travel and Immigration

5.5 Education and Application

BSC is also used in education applications as mentioned below:

- Remote Student Authentication
- Student services
- Security
- Guardian authentication

Thus the proposed Biometric Smart Cards need to be used for the abovementioned applications with high security and authentication mechanisms to avoid vulnerable attacks.

6. COMPARATIVE STUDY AND MARKET ANALYSIS OF SMARTCARDS

Online services are rapidly increasing and the Internet things are coming into existence, there is a very clear increasing demands of security in addition to existed smart card based applications. Based on the several analyses and the history, the industries which providing securities for these types of smart cards are well positioned and they are providing secure and convenient solutions as well as services for the present trend markets.

As per the analysis [21] there is a huge growth in industries with smart card securities in the year 2013 comparing to the previous years by considering the factors of increasing in eID cards, secure e-documents, electronic health cards, EMV migrations, New Field Communications (NFC) and the new technologies like 4G and etc. The deployment of 4G technology and the continuous demands in the SIM markets leads the growth in telecom industry.

The below Table 1 represents the survey data of the various services throughout the world and the number of devices are equipped for the usage of various secure based applications.

Table 2. Worldwide Smart Secure devices equipped in millions of units.

Services/Year	Year 2009	Year 2010	Year 2011	Year 2012	Year 2013
Telecom	3400	4200	4600	5100	5350
Financial Services	750	880	1010	1200	1480
Government-Health Care	160	190	240	310	360
Transport	40	65	80	135	160
Pay TV	100	110	125	135	145
Others	70	75	80	90	100
TOTAL	**4520**	**5520**	**6135**	**6970**	**7595**

The below Figure 9 shows the total number of smart secure devices (in *Million Units*) has been equipped for the various places in the world in including all the services mentioned in above Table 2. As per the records [21], the improvement of the usage of the technology has been increases with the year.

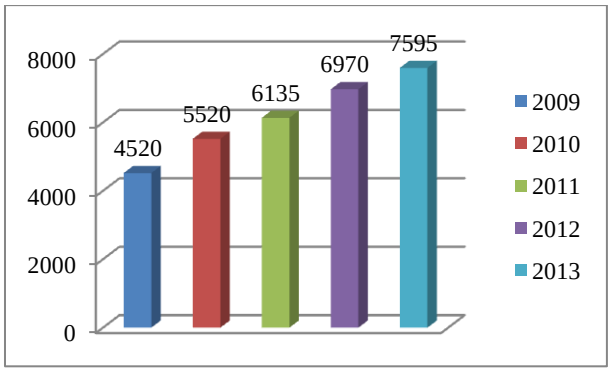

Fig 9: Total number of smart secure devices equipped in last five years

Dual interfaces devices like contact and contactless smartcards for e-payments in various banking sectors also using these smart card technologies. Various services and their shipment details of smart secure contact less devices in millions of units in various years are shown in the below Table 3.

Table 3. Worldwide smart secure contact less devices in millions of units.

Services/Year	Year 2009	Year 2010	Year 2011	Year 2012	Year 2013
Financial Services	120	175	225	295	455
Government-Health Care	75	100	128	170	210
Transport	40	65	80	135	160
Others	30	30	30	60	70
TOTAL	**265**	**370**	**460**	**660**	**895**

The Figure 10 shows the total number of smart secure contactless type of smart cards (in *Million Units*) has been equipped for the various places in the world in including all the services mentioned in above Table 3. As per the survey data records [21], the usage of contactless smart cards have been rapidly increases from the year 2009 to 2013.

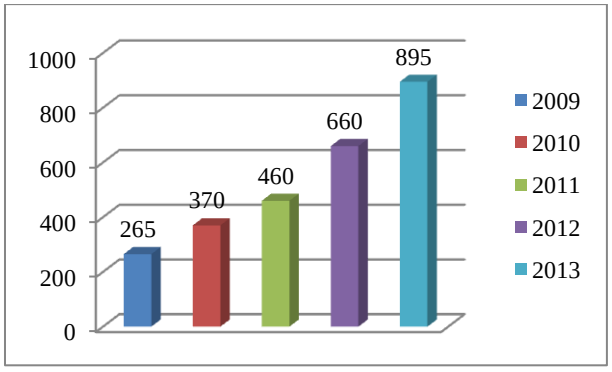

Fig 10: Total number of contactless smart secure devices equipped in last five years

Considering all the above data analysis of smart cards shipments and the developments in the recent years shows the

continuing trend towards secure smart card technologies of all aspects of applications around the world [21]. To develop all the needs of the secure world with these technologies, there is a need of infrastructure and system upgrades, thus there will be a tremendous opportunities for the smart security industries in further developments for a secure world.

7. CONCLUSION AND FUTURE WORK

In this paper authors introduced the novel scheme for providing high authentication and security mechanisms for the proposed biometric smartcards by combining the two levels of security, i.e., for the fingerprint pattern taken as the authentication of the person and the chip on the smart card chip having its PIN as a security. Biometric smart card is the combination of the finger pattern and the chip on the smart card which provides high two tier authentication technique. This BSC will be used in smart card based applications with to provide better secure transactions in all proposed applications. By this mechanism of BSC one can avoid the vulnerable attacks on the cyber world, accessing the databases, tampering the security protections and etc. Currently authors working towards the cyber forensics and the fraud detection mechanisms to avoid tampering of the security protections and cyber crimes. This will be done by various mapping procedures using the database transactions of a particular Biometric Smart Card.

8. REFERENCES

[1] K. Jain, K. Nandakumar, and A. Nagar. "Biometric template security". EUR-ASIP, vol. 8, no. 2, pp. 1–17, 2008.

[2] Jain, A.K., Ross, A., Pankanti, S., Biometrics: a tool for information security. IEEE Trans. on Information Forensics and Security 1, 125–143, 2006.

[3] FIDIS (2005). D3.2: A study on PKI and Biometrics. M. Gasson, M. Meints and K. Warwick: 1-138. BiometricFAQ, "http://www.biometrics.gov/Documents/FAQ.pdf"?

[4] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc.

[5] Wayne Penny, (2002), Biometrics, A Double-Edged Sword,http://www.sans.org/rr/paper.php?id=137.

[6] Thornton, John (May 9, 2000). "Latent Fingerprints, Setting Standards In The Comparison and Identification". 84th Annual Training Conference of the California State Division of IAI. Retrieved 30 August 2010.

[7] Langenburg, Glenn (January 24, 2005). "Are one's fingerprints similar to those of his or her parents in any discernable way?". Scientific American.Retrieved 28 August 2010.

[8] Fingerprints, palms and soles, Cummins, H., 1943, http://www.dse.nl/~frvc/handresearch/derm.htm.

[9] Hueske, Edward. Firearms and Fingerprints.Facts on File/Infobase Publishing, New York. 2009. ISBN 13: 978-0-8160-5512-8.

[10] Engert, Gerald J. (1964). "International Corner". Identification News 14 (1).

[11] Some of the above wording is credited to the writing of Greg Moore, from his previous fingerprint history page at http://www.brawleyonline.com/consult/history.htm (no longer there). Also, David L. von Minden, Ph.D helped correct typos his students kept cutting and pasting into their homework.

[12] Interpol, "General Position on Fingerprint Evidence," by the Interpol European Expert Group on Fingerprint Identification, at www.interpol.int/public/Forensic/fingerprints/WorkingParties/IEEGFI/ieegfi.asp#val

[13] FingerprintPatterns,http://www.odec.ca/projects/2004/fren4j0/public_html/fingerprint_patterns.htm

[14] Smart card basics, http://www.smartcardbasics.com/smart-card-overview.html

[15] Biometric Scanning Technologies: Finger, Facialand Retinal Scanning, http://www.sans.org/reading-room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning-1177.

[16] Samir nanavati, Michael Thieme, Raj Nanavati, Biometrics: Identity Verification in a Network World. Willey India edition, 2002.

[17] The history of finger prints. Finger pak. http://www.fingerpak.com/thofingerprint.html

[18] Crime Scene Forensics. http://www.crimescene-forensics.com/Fingerprints.html

[19] Fingerprint recognition, http://en.wikipedia.org/wiki/Fingerprint_recognition

[20] Clue: Fingerprint patterns, http://www.odec.ca/projects/2004/fren4j0/public_html/fingerprint_patterns.htm

[21] Eurosmart, the voice of the smart security industry, http://www.eurosmart.com/index.php/publications/3-publications/204-figures-may-2012.html

[22] Wayne Jansen, Serban Gavrila, Clément Séveillac, Vlad Korolev. Computer Security. Smart Cards and Mobile Handheld Devices: An Overview and Implementation. July 2005.