Thesis for the Degree of Doctor of Philosophy

A Study on the Biometric Sensors-chip Identification Pattern for Smart Card Frameworks

by

Sang Thawng

Department of IT Convergence and Application Engineering

The Graduate School

Pukyong National University

August 2016

A Study on the Biometric Sensors-chip Identification Pattern for Smart Card Frameworks

스마트 카드 프레임 워크를 위한 생체 센서 칩의 식별에 관한 연구

Advisor: Prof. Man-Gon Park

by

Sang Thawng

A thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Department of IT Convergence and Application Engineering,
The Graduate School,
Pukyong National University

August 2016

A Study on the Biometric Sensors-chip Identification Pattern for Smart Card Frameworks

A dissertation

by

Sang Thawng

Approved by:

(Chairman) ***Chang Soo Kim***

(Member) ***Kyung-Hyune Rhee***

(Member) ***Yong-Soo Pyo***

(Member) ***Am Suk Oh***

(Member) ***Man-Gon Park***

August 26, 2016

Contents

Chapter 3. Biometric Sensors-chip Card Architecture and Cryptographic Documentation Prototype

Chapter 4. Identification and Authentication System

Chapter 5. System Monitoring and Administration

Chapter 6. Biometric Software Infrastructure

Chapter 7. Infrastructural Strategies and Identification Methodologies

Chapter 8. Authentication Methodologies Models

Chapter 9. Biometric Privacy, Implementation, and Legislation

Chapter 10. Conclusions and Further Study

List of Tables

List of Figures

스마트 카드 프레임 워크를 위한 생체 센서 칩의 식별에 관한 연구

상 탕 (Sang Thawng)

부경대학교 대학원 IT 융합응용공학과

요약

21 세기에 들어서 스마트카드 프레임 구조를 하는 생체 패턴 인식이 급격히 주목을 받고 있는 이유로는, 첫 번째 보안과 인증 그리고 이들의 편리한 관리 도구로서 사용된다는 것이고, 두 번째는 지역 혹은 글로벌 여행자들의 관리 차원에서 범죄와 테러를 예방하기 위한 효율적인 제어 방법이 될 수 있다는 점이다. 세 번째 이유로서는 다음 세대를 위한 기술적인 진보와 발전을 시키기 위해서 일 것이다. 스마트 카드 어플리케이션을 기반으로 한 생체인식이 인간의 정보 인식을 위한 적절성과 편리함으로 자리잡음에 따라 그것을 정보 신뢰성과 인증이라는 관점에서 신뢰할 만한 암호 작성 기술과의 교류 부분이라고 할 수 있다. 센서 칩과 스마트카드 시스템을 기반으로 한 생체인식은 편리한 관리와 더 나은 환경 그리고 안전한 작동을 구축하기 위하여 인간의 중요 생체 정보를 인식하고 인지하기 위하여 고안되었다. 스마트 카드는 인증절차를 위한 스마트 칩에서 이전에 설치된 데이터가 사라지지 않거나 혹은 도난 및 복제되지 않기 때문에 훨씬 강한 인증시스템이 될 것이다. 스마트카드는 오늘날 접근 제어와 여행자들의 신원 보장 그리고 인간의 사회적 서비스의 동일성을 탐지할 뿐만 아니라 과학적 및 기술적인 사회에서 수많은 비즈니스 기회를 제공할 것이다. 이러한 장점과 혜택으로 인하여, 우리는 실 세계에서 이를 구현하기 위하여 생체 인식을 통한 스마트 카드 시스템 개발에 주목해야 할 것이다.

본 논문에서는 데이터 구성에 의한 유일한 특성들 또는 행태적인 요소평가를 가진 생체 스마트 카드 검출 시스템을 위한 패턴 인프라 프레임워크들의 프로세스가 사용자의 실제 정보 신원확인과 어떤 특별한 위조 정보 체격 검출 사이에 훨씬 더 근사한 관계를 수립하는 것이 가능함을 보이고 시큐리티 행정과 제어 지역을 관리하고 이를 구현하기 위한 참신하고 편리한 형태의 스마트 카드를 사용하는 생체 인식 시스템을 위한 패턴 인식 및 식별 인프라에 관한 기술들을 제안하였다.

Chapter 1.

Introduction

Biometric Sensors-chip Identification systems denote the structural design and systematically building the platform of pattern infrastructure for information data management structure for a person via a functional investigation with bio-measuring methods. Biometric pattern recognition infrastructure (BPRI) refers to the advanced capability of verification by a pre-installed program on software's system. This infrastructure system is linking to authentication one's personal identity with smart-cards and its credential information for security, business and safety reasons.

Biometrics Identification (BI) provides identification of the person by both acquiring an internal body image, who must cooperate in a way that would be difficult to counterfeit and external elements which are un-fake-able information infrastructure pattern glory. The installed base is a testament to the confidence in its accuracy and invulnerability. The aim of this research is to design a system of the infrastructure within software and hardware for both bio-traits and physical traits such as retina identification system using neural sensors framework and DNA authentication. The theory of such pattern design for such systems will allow automating the personal identification using biometric sensors-chip, smart card. Biometrics sensors-chip identification on smart-card methods on pattern recognition for verifying, authentication and tracking someone's identity are increasingly crucial part of security management system that essential to advance. The monograph describes biometric pattern recognition infrastructure that allows creating efficient individual's characteristics of a person by

using sensors measuring different physical properties and information. The process of authentication a person's trait, verifying identity, plays an essential part in several areas of the task to perform by securing a person in a claimed identity with biometrics trait for society and national. Any situation, by advancing to capture a person's information with a smart-card, with the user's interaction when authentication is required, so as to confirm the claimed personal information, which is logical access control with computer pattern recognition systems via sensors network.

The process of pattern infrastructure frameworks for biometrics smart-card detection system, its unique features or behavioral elements evaluation by data configuration, is capable of establishing a much closer relationship between the user's real information identity and a particular counterfeit information physique detection. While, the growth of global counterfeit technological issues, fake information or data being uneasy to eliminate, and from the future to come to these issues will be managed and verified by the use of the biometric sensor-chip smart card. Therefore, this thesis aims to develop a pattern recognition infrastructure for biometrics system within the smart-card which is a novel type of comfortable to manage and implement to security administration control zones.

1.1 Research Background and Objectives

1.1.1 Background

The existing models and systems for smart card and convenient e-card and ID had been introduced decade ago. The limitation sufficient uses and implement are being developed and still in an impossible situation. It is proposed that the design of an

efficient and secure authentication structure can deliver individuals with trusted identifications for the bio-traits management of applications, such as qualifying contact to services and its secure networks, proving a privacy's rights to amenities and directing by the use of Biometric sensor chip technology. Biometric based smart card technologies are employed with a well-designed authentication frameworks and management system that can allow for the means to guarantee an individual presenting a protected identification credential. On other hands, biometric sensor-chip card has the exclusive capability to store huge amounts of data, capable of high data and volume to carry out functions, and interact logically with a biometric data's reader within its purposes' realm. Secure authentication systems have the challenging task to achieve a maximum degree of information security and therefore increasingly implementing both smart card and biometric technology. The need for reliable authentication systems, the use of biometric identity verification systems and its pattern recognition is because of biometric-chip has become increasingly important for today global society. Biometric products are currently used in some several areas such as airports, in log-on devices for networked via PCs, in e-commerce, e-banking and health monitoring. Face recognition and fingerprint systems are among the top choices because these recognitions are friendly, non-invasive and fairly accurate. However, there are a number of practical issues that still need to be developed and integrated such systems. Once designing face confirmation systems one has to compact with unsolved problems that arise from each component of the overall system such as data collection, transmission, data storage in which signal processing via sensor or network and a final decision making correctly. The problem becomes more complicated when the target platform and matching, in

which a suitable algorithm has to be ported, imposes severe engineering constraints. Therefore, in dealing with the restrictions of both aspects and verifications via biometric-based smart card technologies are a very challenging task with many key factors to consider in the biometric-based authentication system.

1.1.2 Objectives

The objectives of this research are to develop how the system on a smart-card pattern recognition implementing biometric sensors-chip into the ID card which will address identified security issues, the component, installation, and elements for its software and hardware's models. This research puts concern toward the question in which need to be solved by the use of biometric sensors-chip card. How does the pattern of biometrics card play a role in security within the security zone to help protect not just the travelers and workers but also public security and international security management? This research aims to discuss the issue and privacy of a person, community, and public:

- User's endorsement
- Confidentiality of travelers' privacy
- System security for Public Key Infrastructure (PKI) management
- Internet confirmation services
- Data mining, storage, and recovery management
- Fishing, fraud, leak, and attacks

Despite its usefulness, the implementation of biometric sensors-chip card (BSCC) raises several political and social concerns. These emerge both from the exceptionally large scale of deployment and from the need to protect collected data from

abuse. One of the major concerns in the existing conventional biometric systems is the security-privacy dilemma. However, sensor chip based smart card authentication is the ideal tool to overcome this problem. A (BSCC) can offer the necessary technology to keep both citizen's rights and foreigners satisfied providing with a very attractive security application as well. Identity solutions will deter and reduce fraud by Biometric sensors-chip card authentication in security and convenient for the users and administrators: It will also reduce identity fraud, improves security management and protects citizens and foreigners' privacy:

- Preventing card or information sharing and others' identity theft by authenticating the anonymous by fishing to the provider's fake information.
- Verifying pre-installed data and stored database "encounter data" services from card holders so that administration can rely on this accurate data transmission and authentication within biometric sensors-chip card's information.
- Creating the "audit trail" at a check in & check out for comparisons fake and genuine information as an indicator for the possible scam, called "up coding".

Bio-traits pattern recognition system correspondingly generates functioning competences design for smart cards procedure, also provides the developments to risk management programs by ensuring the accurate verifications that require a unique key for criminal management and to be matched to biometric data for each individual personal smart ID card. It also offers for what most needed a card and the idea of a common documentation number that delivers confident identification of a person's identity by using a biometric-based sensors-chip card secured to information uniquely.

And lastly, the overall quality of infrastructure system is improved through a precise research on the frameworks of advanced identity authentication and infrastructure pattern system.

1.2 Problem Formulation and Scope

This research describes a biometric sensor-chip ID card verification system which is smart-card-based authentication of a person genuine or fake identity. The scope is set to identify or authenticate a person from the key bio-traits parameters. Such an effect for the design of the system, to study the universal optimization complications and tests' heftiness when each of every keys parameter is optimized. Some of these parameters are indelicately investigated in the works in the framework of the overall recognition problems. However, this study only partly fulfilled the requests of smart-card-based frameworks, in which the unembellished production constrictions and confines imposed by biometric cards that have to be taken into the overall design frameworks and requirements.

To address the problems on the projected effusively contained architecture of the smart card verification systems of BSCC, the study aims to start with the collection of the client detailed rectilinear criminated analysis procedure, seemly to be ported to the boarding podium in which the biometric sensors process can be run. The focal efficient parts of the frameworks are obtainable: biometrics duplicate symmetrical alignment, photometric normalization and extraction, and confirmation. Each part involves sequences of rudimentary steps, where each part of the phase is fixed. Conversely, the procedure is methodically wide-ranging in some steps to explore the consequence and results on system performance, and a system intricacy in terms of

speed, memory and its capability of volumes' management. Therefore, algorithm proves will not be discussed, though, which is one of the most crucial parts for BSCC.

Two major problems have been considered. The first problems are the limitations of both BSCC's corroboration and biometrics technology execute and the second is the extreme convolution of the structure in which the number of processing platforms and structural designing constraints. In the simplified search procedure adopted, a number of parameters have been designated to that of the comprehensive structure set elaborate in general BSCC. This set was recommended, this research avoids, by previous mainframe-based studies, and deemed to provide acceptable performance.

System optimization in the context of smart card implementation has been conducted starting from those parameters involved in the pre-processing phase pattern, then those involved in the remaining stages. A combined optimization frameworks conclusive key parameters are also implemented, presumptuous that the result is autonomous. Experimental results obtained on a number of publicly available face databases (used to evaluate the system performance) show the significant benefits of this design both in terms of performance and system speed. The different results achieved on different databases indicate that optimum parameters of the system are, to a certain extent, training database dependent.

1.3 Contributions and Frameworks

In this research it is proposed a biometric remote authentication system, which only requires the biometric data of the user in the authentication process, discarding the need for the use of passwords. This solution overcomes all the issues regarding the security of the fake and false information within that data template of the user, and the

confidence in a remote biometric information data matches accordingly. Then, two kinds of biometrics: public and non-public while experts proposed biometric is public.

One of the goals of the proposed solution is to use existing technologies, thereby ensuring low development costs and a high compatibility with existing remote authentication systems. This solution is therefore designed to be considered as a reliable possibility, small, flexible, secure and convenient to integrate the future authentication mechanisms in already existent remote scenarios. The proposed solution is based on the use of biometric sensors-chip cards, in which the private key and biometric template of the user are stored. The smart card of the user is afterward deployed in a Public Key Infrastructure (PKI).

There are similar solutions in which the smart card is deployed limitedly without a biometric system in a PKI, being able to perform the remote authentication, authenticating the user with his PIN. The smart card possesses the private key of the user, as well as a public digital certificate signed by a trusted Certification Authority (CA). The remote authentication process is based on a challenge response, in which the response corresponds to the digital signature of the challenge, retained with the remote key of the user performed by the smart card. Not even the user has access to this private key, ensuring that only the biometric sensors-chip smart card knows it. The user authentication is performed ubiquitously in the smart card via sensors-chip.

One of the real applications using this remote authentication approach are the Electronic Identity cards. These cards are responsible for the cryptographic computations required for the identification and authentication of a person. An example of

this solution is the Portuguese citizen card, where a Java Card stores the user information, fingerprint templates, PIN, private keys and public certificates signed by a CA. However, this research is more reliable, secure and convenient for the user and administrator. Meanwhile, the applet installed to perform remote authentications follows the Identification-Authentication Signature - European Citizen Card. S m art cards also possess the capability to manage biometric templates, and to perform Match-On-Card (MOC) operations.

The solution herein offered entails replacing the local PIN authentication, in systems o f information detection via the ID card, with a ubiquitously managed biometric authentication. This is achieved by only allowing a remote authentication after a biometric authentication is also performed. In this solution, an applet implementing the Automatic Identification System (IAS) standard is responsible for the remote authentication of the user. The IAS only has the private key released to sign the challenges from the remote server, after a successful user biometric authentication in the MOC applet. The obtained results show that it is possible to use biometric authentication in remote scenarios, taking advantages of their potential as a more secure and easy to use authentication mechanism. It also eliminates the need for users to have different passwords in different systems. The smart card technology is used in the proposed solution, enabling the secure use of the biometric authentication in remote scenarios. In the proposed system, smart cards are possible for storing the user biometric template, and for computing the match-on-card (MOC) operation system. This section describes the importance of these devices in current days and the main benefits that make them implement. It is shown how biometric sensors-chip cards are a

very useful instrument in people lives, protecting against attacks on information security, being at the same time flexible, small, portable, trustworthy, and secure electronic devices need to be developed and deployed by using biometric sensors-chip card.

In general, biometrics smart cards can be separated into two types of card, and cards without biometric sensor chips such as the magnetic cards. The Integrated Circuit Card (ICC) can be considered memory cards or processor cards, depending on their chip structure and features. The processor cards have the ability to store information, and also to process it. This type of biometrics smart cards can be additional subdivided into two types of card called "with processor card" or "without coprocessor". The coprocessors are responsible for the execution of the asymmetric cryptographic algorithms. The cards with a chip usually communicate through the use of contact pads. However, these cards can contain an embedded antenna to perform the communication with the host side, instead of using the contact pads attached to the chip. The cards with antenna and contact pads can be called by combined or hybrid cards, depending on the amount of chips that they have. The combined cards contain one chip that can be read through either exchange pads, or a fixed antenna, while fusion cards two or more embedded chips, such that some communicate through the antenna and others through its contact pads.

The improvement and functionality of the biometric cards are sturdily driven by standards demands. Therefore, the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) is the standard for contact Smart Cards, defining the physical characteristics of the integrated circuit cards, their dimensions and the location of the contact pads, as well as specifying the electronic

signals and transmission protocols used in the communication with the host side. Likewise, the ISO/IEC 14443 [1] is the standard for contactless smart cards, specifying their physical characteristics, the radio-frequency power and signal interface used for the communication with the host side, as well as defining the initialization requirements, the anti-collision mechanisms, and the transmission protocol specifications.

Despite the existence of various types of cards, to be considered sufficient and convenient smart card, as such Javacard, have to respect some important requirements, such as those defined in based on a bio-measuring card system. By definition, a smart card is an electronic device that can participate in an automated electronic transaction, with security, and is not easily forged, stolen copied. In this sense, a smart card must have high memory and a microprocessor, to be able to store and compute data, and to assure the execution of some security algorithms and protocols. A smart card has also to be a tamper-resistant system, in order to resist to the physical attacks made directly to the chip. Smart card must contain many security functions for users and high capacity for secure storage of information and key generation. This definition makes impossible for the magnetic stripe cards to be considered smart cards, once they do not have the processing power, and they can be easily copied or forged. Even some chip cards cannot be considered smart cards if they are only memory cards without a microprocessor to ensure the requirements defined.

1.4 Literature Review

Since biometric sensors-chip with smart-card deployments in security have traditionally been extremely difficult and problematic, which have been under the process of development, this research will be focusing on the identification frameworks system of

its hypothesis statement for the security system to develop pattern recognition. Hypothesis: by implementing biometrics it can increase the security for workers, travelers, administrators, and managers. How does pattern recognition is infrastructure for security management and controlled by the use a biometrics smart-card system? What kind of issues is there with the security by using biometrics? What was done to fix those issues?

The benefits will be gained from using biometric sensors-chip card. After a careful reading of today's criminal threats, the rise of terrors, security administration field and having several teething troubles that work in the check-gates; implementing biometrics in check-gates is critical to help reduce the risk and cause of fault results and criminal clearance. Most predictable schemes nosedive to function dependably in the punitive atmospheres and circumstances found in several places. Persistent washing and cleaning, heavy use of the crowded situation, the using of rubber gloves and that of a wide range of using demographic production make biometric-chip card implementation, registration and substantiation give problematic and challenging. Although those systems are a convenient module for access control system, the security they acquire is usually overvalued, as if they were dreamlike tools whose modest use will inevitably stop each and every type of violence, attack, error management and identifying fake information. Biometrics-traits are actually not protected except it is embedded in a resilient cryptographic protocol, whose enterprise wages extraordinary consideration to its specificities in all aspects. In specific, cryptographic protocol resilient reveals that a beneficial and sufficient partner of biometrics for such a protocol. This research discusses to develop the utmost significant subjects elevated by biometric pattern

recognition administration with smart-card and introduces a unique authentication protocol skeleton of its infrastructure system for the smart card.

Biometric technologies are well-defined as computerized approaches for recognizing and authenticating the uniqueness of a live person information based on exclusive behavioral characteristics. Biometric sensors-chip based card provides actual protected and appropriate proof or identification and authentication of a person's identity since biometrics elements cannot be lost, stolen, forgotten and are impossible to forge. At the same time, four major contraptions are commonly presented in a biometric system:

- Mechanisms: to examine and detect an arithmetical copy of a live person's biometrics installed characteristics.
- Software: to procedure biometrics data to a design that can be used for packing and corresponding.
- Matching: to relate a pre-installed warehoused data within biometric pattern from a live biometric sample.
- The interface in the request process phase is to interconnect with the unique matching results.

Two dissimilar points are intricate to the biometric data process processing acceptance and corresponding. During the enrollment stage, the biometric images of the individual are captured using biometric data reader, a microprocessor for voice recognition, a camera for facial and appearance and iris recognition and so on. The inimitable

features are extracted from the biometrics sensors-chip data to create the holder's biometric data template. This biometric data template is securely warehoused into the database on a legible element composed card for the use of a matching process periods.

During the Matching stage the installed and updated biometrics data sample is over again captured, these sole sorts are mined from the sample of a biometric taster to manage alive biometric data template of users again to renew information. This reinstalled template is matched with the template pre-stored and the result of a matching score is created according to a resolve of the collective element within the two templates. System designer determines the threshold values for authentication score based on its safety and suitability necessities of the systems. The assortment of the suitable biometric technology depends on number applications in detailed features, plus the settings in terms of the identification or confirmation progression is being carried out requirements for matching correctness and amount, the general scheme and competencies, and so some concerns that might touch user's recognition. High, medium, and low are denoted. Standards dispensed for how biometric sensors identifiers meet the numerous potentials are particular conclusions according to the proficient outcome.

After implementing, the efficiency of smart cards is mostly determined by the microcontroller and the performance of the system. The microcontroller's chips are particularly modified for each smart card, in terms of somatic constraints in which the all-out up-to-date ingesting, the variety of permissible chronometer regularities, and the permissible temperature assortment. Smart card microcontrollers are specially hard-

ened against attacks, including the detection of under voltage and over voltage conditions, and the detection of chronometer rates external the stated choice. Therefore, the microcontroller usually incorporates with temperature sensors, in order to identify the attack, and respond accordingly. That microcontroller device pattern recognition infrastructure system is to be adapted, however, different models in term of devices and its development is proposed herein.

1.5 Thesis Outline

The first chapter of this study is the introduction, covering the important of the field to the intersection on this dissertation. I represent the basic traditional card and the state of the element for a different tool, yet concentrating to detail in the interior scopes of the biometric-based smart card as global demands. The first proposal presents biometrics: the different techniques, the system building, evaluation criteria, and design and management system and request instructions.

The second chapter highlights the smart cards frameworks and its related technologies, System architectures, operating systems, and fraud management and duplications authentication. Then, this chapter devoted to so-called multicomponent smart cards and effort on this development and modeling. The section presents how the communication of card and biometrics will work on a smart card.

The third chapter presents components: general concepts, purposes, primitives, smart card architecture system (SCAS) and symmetric. The study briefly introduces the interface in cryptography and an installation and framework labeled biometrics technology, smart cards, and biometrics. This second part is fanatical to comparisons of two methods with biometric presentations and the uses for the authentication system.

The fourth chapter describes overall authentication and identification issues in frameworks and structural design, which defines different uses of biometrics data in smart cards, comparing biometric-chip card's factor concepts.

The fifth chapter presents monitoring and administration management; dimensioning, characteristic and certification issues, classification, discriminant data, and representative templates. Thus, it involves theories and models as well.

The sixth chapter presents the infrastructure equipment: flexible modeling tool and technologies, a different form of recognition framework and its factor and acquisition in the management.

The seventh chapter aims to strategies and methodologies and also requirements on sensors: copy techniques, materials, evaluation of sensors network and security framework. This is the infrastructure strategies of identification.

The eight chapter generally presents the artificial generation of pattern and image, recovering original-duplicate information from biometrics template. I highlight biometrics sensor chip based smart modulation implementation on tests and result.

In the last chapter, I sum up with the previous work of the eight chapters, and how it is evaluated on consistency and correctness in real-time and to real world applications with challenges, scope, and a research limitation. So, for a person information authentication and global terror management with a target of cost effectiveness system and "low-end smart card chips" based identification development.

This research in briefly to state that the Private Key Identity (PKI) and Personal Identity Verification (PIV) smart card used by travelers for domestic or international for authentication for the security of the government and civilians within the

secure Biometric models called Match-on-Card (MOC), (SOC) and (TOC) initiative. These methodologies are a testing program by the existing theories, thus, I remodel by combining models and modified theories, to the achievability of convenient smart cards with the biometric smart cards, and its robust cryptography in compromising convenient and security.

1.6 Results Overview

This research presented regarding biometrics sensors – chip, its component on pattern recognition for smart cards system and its technology tendencies in information communication, Micro-Electro-Mechanical System (MEMS) integration available based on a journal published "From smart cards to smart objects: the road to new smart technologies [2]." This research on security issues with pattern recognition framework systems presented has distributed technical reports.

In this methodology, Match-on-Card (MOC) systems, labeled in the brief search of this dissertation, as a basis system infrastructure at the annual challenge conducted expert option. In this delivery, in a significant of the assessment on frameworks, for a match-on-card (MOC) and the result obtained with proposed are considered expert interagency reports. Thus, there is still more for progress to be concerned. This study reflects the attitude to building security authentication system with biometric sensor chip-embedded smart cards.

Chapter 2.

Informatics Recognition Design and Requirements

The concepts of the informatics recognition and requirements are where the physical characteristic being used for identification that presented to the system within informatics recognition pattern. It is to state that the concept of this design and requirements compose of a complex theory. Multiple models of the informatics recognition design are taken in which requirements will be made from in the adapted models of existing standard. The calculated average of these requirements and design are assigned informatics recognition score for authentication. Each requirement may have different necessities for this measurement informatics system. Therefore, this score is calculated by dividing the number of unsuccessful enrollments by the number of designs and requirement attempting to develop informatics.

2.1 Sensors-chip Specification Design

In a specification in designing a system are classical petroglyphs found in prehistoric caves which cannot trace adequately for sources because the limitation of tools and a long period of time ago trace, while being used to investigate? Moreover, these petroglyphs are found in various regions: then, prints and traces were used on objects tablets such as clay and mud in the ancient Babylonia Empire, traces and prints (e.g, fingerprint, foot trace..etc,)) were used as seals and authorized documentations in around 14th century BC during the king of Persia in ancient time, according to the Bible.

In modern history, anthropometry of this discovery began in 1882 that researcher like Alphonse Bertillon of police in Paris excavated traces and measured of

parts of the prints [3]. Alphonse Bertillon's discoveries methodology includes historical facts and a research in archaeological evidence which measurements such as a period of times, head's length, head's width, finger's length, feet's length, and length of the trace's prints. Which portrays a naked male figure in overlaid spot [4]. These are identified the characteristics in which fingerprints can be identified based on prints and measurements. The same features framework that discovered are basically still a usage method until then, and these are commonly referred as "the theory of Galton's Details". Expanding to Galton's cataloging model, an anthropometric developed the 'Henry Classification System' (HCS) later. The H C S was to find out worldwide rejection theory a few years later. Some experts on forensic science devised the "12 points" of rules; the rules" to confidently recognize or confirm a criminal [5]. Recently, the need for authentication of persons' distinctiveness identification in Information Technology world are an increasingly crucial task as the limitation to implement and its tools lack performance.

Beyond modern footprinting and fingerprinting in forensic science, recent technology based prints can be found media, and also fiction movie and even in cinema that enlarges the idea of biometrics in the civilian application at atmosphere. Hereafter the extensive use of footprint and fingerprinting in written tales and novels, fiction movies and the series performed by James Bond, " Impossible Mission", "Star Trek" widely used biometrics verification and authentication. James Bond of "Diamonds are forever" displays biometric pattern recognition on fake data print techniques are deployed. The uses of alive DNA authentication for blood sample test, body hair sample tests are compiled to identify someone, such as "Big Brother"

misusing joint dread about the use of biometric in real life its offensive exploitation. “Minority Report” uses a high level of authentication is appreciation at detachment, a more glorified and futurist technology [6]. I mention this research to readers for remarkably famous movies with details in related to biometrics uses in each one mention the above lists.

To evidence the management of one’s identity authentication, there can be several methods:

- Something we possess (cards. etc,…)
- Something we use (PINs, Codes, Passwords)
- Something we are (Biometrics, Smart etc.,).
- Something we have (Sensors, network..etc..)
- Something we implant (Chip, RIFD, SIM, etc…)
- Something we need (Sensors-chip smart card,)
- Something we try (Biometric Sensors-chip smart card (BSCSC))

We generally give something to whom we confidence, but passwords can be transferred or predicted to individual personal devices which can be stolen, lost and borrowed. So three factors endorsement by the calculation of advancing to biometrics technique that will bring high assurance in our authenticated panelist and provides a non-repudiation for everyday life [7]. A general definition of biometrics it has: biometrics substantiation has the improvement of examination of the card’s holder characteristic. These characteristics are the physical based footprint, fingerprint, facial, iris and the behavioral based on voice, handwritten signatures, and keyboard patterns. However depending on the relationship of the two samples are determined by the algorithm

if the user is accepted or rejected. This arithmetical procedure will clue to a False Acceptance Rate (FAR) and a False Rejection Rate (FRR) [8].

Biometric recognition is based on the copy the imaging of bio-traits and its elements. The structure of valleys is recorded and stored in the database as the image of numerical template condensable complex data format, yet most requested supplementary related to other images' templates for the authentication process. Images of biometrics pattern designs are captured via sensors-chip. Which means the holder of the card and gateways embedded information data storage are meant to be matched uniquely without false and interact in the speed of light! Among these the biometric techniques that existed recently, fingerprint authentication based technique is the most use method that has been successfully applied to several applications, becoming automated archaic due to the advancement of technology the civilization of human race. In biometric sensor-chip identification via patterns, it is ubiquitous management system used by administrators for security and for the users safety, convenient and efficient inherent ease in the acquisition, and available.

This is and additional and optional biometrics sensors-chip card framework to be used as smart-card proposed might be costly, however, mandatory in all over the world as the risk levels of criminal and terror rise [9]. At the same time, we intend to develop a more reliable and secure pattern and IT development as today is a technological smart working world. So as to design a biometric smart card, it is needed to adequate frameworks infrastructure and reliable system pattern for biometric sensors-chip card as below:

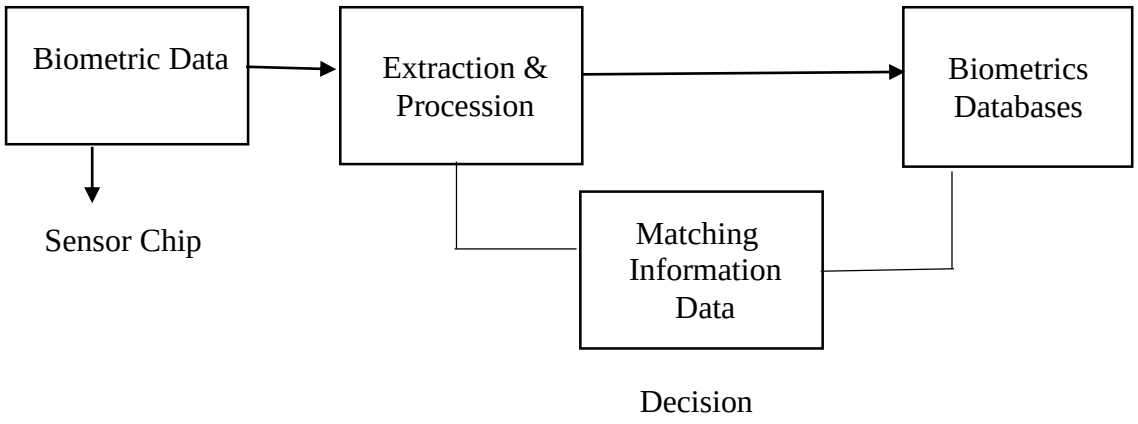

Figure 1. Biometric Pattern Design and Requirements

Such as face, iris, voice and finger recognitions are based on the imaging of itself. Structure verified as the image of the digital template, but non-mature, of a basic data format, for a further comparison with existing technology and the technology to come. Early iris, finger and face recognition algorithms used simple geometric models, but the recognition process for biometric sensors-chip has stimulated in the science of sophisticated scientific demonstrations the corresponding process. " Major advancements and initiatives in the past ten years have propelled this technology into the spotlight" [10]. This is most spontaneous biometric then, it is to distinguish human beings, and cast-off for security and convenient documentations.

2.1.1 Hand Geometry

The hand geometry recognition framework is a lengthiest applied biometric used, debuting in the late decades. That was most deficiencies of the palm geometry characteristics are not very unique, restraining the requests to authentication errands. The biometrics devices complied an unpretentious perception of computing and footage length, width, thickness, and surface area of the skin while directed on a plate. These model usages are based on a camera to capture and supply a copy of a shape image

of parameters. The data is warehoused in a tiny reference template, which is an enormously low number that paralleled as the desire for biometric systems [11].

2.1.2 Iris and Retina Recognitions

In this method, user's authentication is often constructed with the eyes differences from the two relatives: (one). The iris recognition is based on mining the archetypal statistics from the superficially evident, colored inside the pupils' sphere, while (two). The Retina recognition is done by the complete inspection of blood vessels patterns which placed a letter slice of the eyes. The computerized system of iris recognition frameworks is comparatively undeveloped and much reliable for authentication, existing. The iris authentication tracks are muscles within the eyes that normalize the dimensions of the pupils' pattern, monitoring the quantity of light that goes into the eyes. The color of the eyes ball is determined in terms of the "melatonin pigment' in the muscles. Therefore, iris imaging entails the use of high pixels called "excellence digital camera" [12]. Today's commercial camera for iris microscope is characteristically used near ultraviolet light to irradiate the pupil vein patterns without cause or harm to these elements for the eyes themselves. The "third and optional biometrics" which is Iris recognition mostly implement in e-Passports [13].

2.1.3 Vein Patterns Recognition

The reputation of biometrics sensors technologies for vein pattern recognition is beyond as fingerprints, retina, face recognition, in which harmonies much demand modalities to develop for biometric sensor chip based authentication system. However, the emerging vein pattern recognition and its unique structures and advantages, it has

been sustaining its standard defeat others. The vein pattern recognition is advancing impetus, though a complex and advanced technology, the fast growing technology. It is a progression to develop the cutting-edge candidate system to majority applied biometric technologies to a commercial deployment in industries. Technology tasks by ascertaining the intravenous influence such underneath the skin of vein patterns in a personage's hands, wrists and fingers. After a user's hand is positioned on a scanner which is the veins pattern reader, a electromagnetic light the location of the vein and copy of its pattern sample and store as it is, vein pattern recognition is, however, an unindustrialized exploration programs that interested and studied widely and recently for biometric technology authentication to both mammals and animals and which is proving promises to give an accurate and acceptable results within parameters. In vein pattern recognition non-public biometric is possible to implement, nonparticipation of public biometric, in which traceable information are kept in an encrypted database. Based on quantized theory, PPMF model, two patterns matching technique is an inimitable displaying of desired matching process for faultless authentication. It guarantees correcting matching and eliminates counterfeit biometrics information presentation.

Every mammal and human are unique in their own ways. Thus, the numbers of possible of physical characteristics of their traits of uniqueness are limited by our thoughts and capability to amount their characteristics. In biometric techniques, some distinctive can be noticed in classically because such odor aroma, vocal sound recognition, keystroke dynamics, handwritten signature, while several may seem esoteric because face thermos-grams, gait, and ear's shape in the biometric recognition system. The recent techniques covered bio-dynamic signatures, opt acoustic emission, and

brainwaves pattern [14]. The elements composed of physical patterns and behavioral patterns for recognition and authentication for identity.

Table 1. Physical Patterns and Behavioural Recognition Patterns

Physical patterns	Behavioral recognition patterns
Fingerprint	Hand-written signature
Face	Keystroke dynamics
Iris	Gait
Retina	Hand-grip dynamics
Voice	Voice
Vein pattern	Lips dynamics
Palm-print	Mouse dynamics
Hand geometry	
DNA	
Face thermos-grams	
Body odor	
Fingernail	
Brainwaves pattern	
Bio-dynamic signature	
Optic emissions	
Ear shape	
Skin spectrographic	

2.2 Biometric Sensors-chip Smart Card Design

This design generally composes of both hardware and software requirements as depicted in table 2. Biometric sensors-chip designing systems take contribution to

multiple requirements that apprehension more different modalities of hardware characteristics. For instance, systems of the element that combined face, voice, and iris data for biometric sensors-chip frameworks could be considered a "multimodal system" regardless of its different imaging devices or the same device. By the use of biometric sensors-chip in smart cards, the above difficulties can be solved for smart cards contain large memory capacity and secure storage for data and information and keys. The tamper resistant property of smart cards allows privacy protections, in which data are encrypted and stored in the cards from damage, loss, and theft [15]. Here, we need to architect a digital component for sensors so that it is capable of accessing sensors network and penetrating bio-information and hybrid actuator so as to applicable for software to be install within a system to rule was to be functional, tolerating users to be certified by means of either of the modalities.

2.3 Biometric Sensor-chip Pattern Requirements

With a biometric sensors-chip system-on-card (SOC), personal ID verification is accomplished independently with centralized existing sensors-chip technology and utilities existing infrastructure. Therefore, solve virtually all privacy and security issue related to SOC card-based biometric-chip smart card system component. I believe the following inset, Bio-chip and COS standards for software will meet the requirements for the biometric traits sensors-chip pattern smart card.

Table 2. Technological Installation System in a Biometric Sensors-chip Card

Technologies Installation System			
Layer	**COS**	**Bio-chip**	**Inset**
Reliability	● Physical, chemical and mechanical characteristics and components manageable by ISO/ICAO ● Security to amount enactment, robustness, and reliability ● Anti-fishing & durability and excellence guarantee		
Capability and Interoperability	● Support overall best standard between biometric and sensor and process in operating system ● Meet international standard, fast, safe and convenient		
Standard Suitability	● ISO/ICAO standard and multi-standard based suitability ● Java-based stands, and MultOS operable codes. ● Identity suitability with international tech and infrastructure quality software		
Security	● Certification for COS used in card shall be ISO15408CCEAL4+ or higher which meet two Protection Profile/Information ● Support smart card security its mechanism and supply security for protecting personal information for public uses ● Support additional security element		

Table 2 focuses on system description and administration such as networking management for the sake of both the users and administrators for a better work management. Accordingly, the system description for software model is drawn and designed to meet as:

Table 3. System Description for Installation

Part	System Description
Center	● DB Server, Server Backup-Be located in gateways ● Biometrics system-Be able to share with system of identification -Digitization system center
Issue center	● Personalization system ● Be located in all cities, necessities place.
Backup Center	● DB backup system ● Be able to share with system of NID center, Immigration offices, police stations and under government control
Districts	● Working Smart Workstation ● Operate and install in all cities offices throughout or ● The country with selection of principal cities
Consular office	● Working Workstation-Operate and install in the embassies and Consulates in overall provinces/states

It focuses on software components and its functional description for offices in which the system is capable of handling multi-tasking management. The expectation of upgrading biometric sensors-chip based identification card is to ease to manage international criminal in a border pass check gates, port security system and immigration management system to make a better and smart work for security. It is also intended to hand local criminal and a better information management. It is to construct integrated Infrastructure for the best information management system for public security, by use of smart card which requires rapid and accurate immigration service to compare with existing border control system. Adopt and install infrastructure (H/W, N/W, and S/W) which requires the service of information management system for gateways in a timely. Also, it supplies stable service through perfect integration test with application

systems. Apply new and certified information technology, to the service of information management system for immigration of border pass check gates. Then it provides enhanced national competitiveness, by improving administration quality for immigration check, besides it offers administrative efficiency for immigration check to prepare for increasing works.

Table 4 emphasis on the aspects of international competitiveness, administration sector operation, generating information by sharing data among regions or agencies, which meaning all the work of administration by enhancing security.

Table 4. Expectation Effects and Evaluation Results for Security

International Aspect	● Enhance National Security ● Increase National Competitiveness ● Increase Global Credit Rating
Administration Sector	● Increase efficiency of administration operations ● Reduce cost & process of illegal immigrant management ● Increase nation protection from international terror ● Reduce cost of generating information by sharing data among regions or agencies ● Save cost by reducing the time required for fingerprint identification, background checks, etc. ● Improve public administration

Table 4, three sectors' graph, is the estimation and expectations of the development benefit of this security technology. While table 5 highlights the requirements for the development of the card and the design levels and its components. This contribution to technologies requirements, biometrics based smart card, and the frameworks

of card is in which combines both public biometrics and non-public biometric infrastructure. This theoretical analysis and approach generate the possibility of enhancing biometrics card for administration and management in the coming a ubiquitous world.

The final sector contributes to technology business and education work for biometrics for a smart world and smart management frameworks. The benefits of its security and convenience are to promote crime functional backbone to enhancing administration. And, so as to level step by step for smart card apparatuses and its requirements.

In this case, in building the card chemical high tech for security adequate elements are installed and implement ultraviolet and microwave signal capable sensible network. As shown in the table explaining each factor by point to point for the requirements of biometric pattern capable smart card. As explained in figure 2, two request channels are interacted, sending back and forth, matching information to make a decision without fault, which is possible by handling with the above described in levels and in table 5. For security as the first priority, the biometric smart card and sensor chip must have a compatible in overall system and performance in order to conserve system failures, inadequate tasks achievement as well.

Table 5. Designing by Levels its Requirements

Level 1	● Visually distinguishable security, ● With 5features with the biometric system: Micro text, Rainbow, etc. ● Features , incorporating more features will increase the complexity of the overall design

Level 2	• Devices and tools used to e.g. Ultra Violet, etc. • Distinguish security features
Level 3	• Laboratory and precise select after considering Inspection for security • Security features

2.4 Smart Card Specification Design

A specification of the smart card specification of biometrics design is shown in Figure 2. The rudimentary component of its frameworks is data achievement detention data sensors, a communication channel for signal dispensation in data storage to the server database and the biometric sensors-chip based data querying step by step to reference templates in order to make a final decision.

In this design the matching is evaluated twice, original biometrics data and on-card data (preinstalled data and present data), sending back and forth into template via sensors so that authentication should dependable and a more security for the users and administrators. The concept is that, using two channels biometrics channels and smart card channel, combining two data in comparing the authentic information in two patterns. The complex design below is multi-two channels and patterns feature extraction in a matcher via query template image.

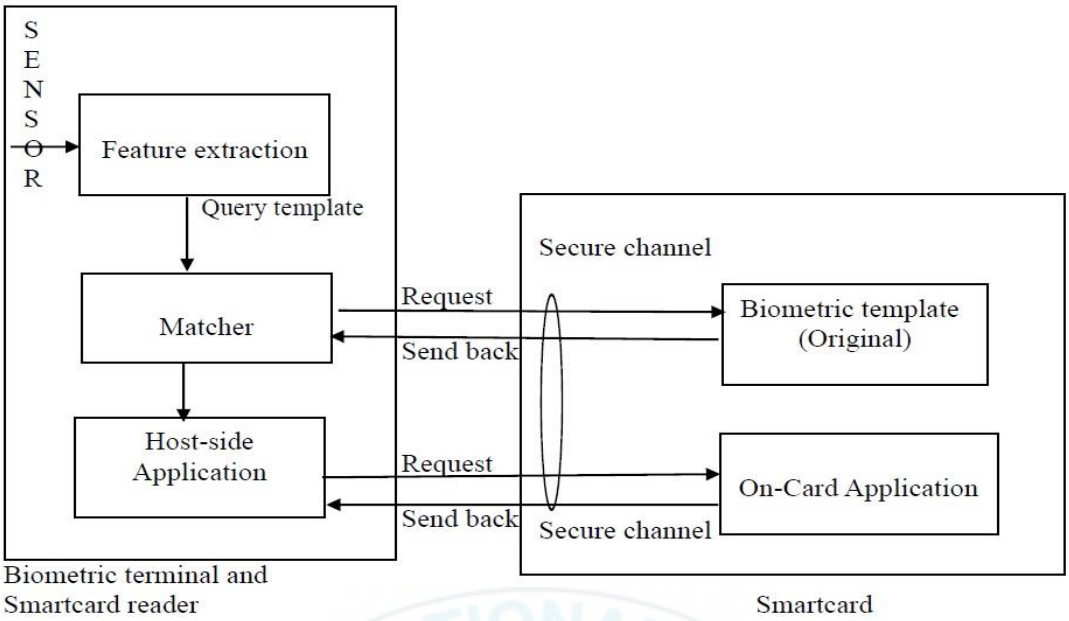

Figure 2. Architecture of Biometric Systems

In Figure 2, the data template stores a reference data of the user which was installed during the stage of a generated at enrollment so that it can be compared to the newly taken data for verification and authentication the user's identification for matching via the sending aftermath by the original template. Conditionally final decision-making procedures, match and fail or threshold of the given scores, (to generate one-time dynamic password) a real-time password is necessary. In this design, the real-time password is generated based on a 'random number generation technique', then the user's data will be accessed to the system, the information of a person be identified in detail as the preinstalled information.

2.5 Object Tracking and Recognition Requirements

In the requirements of ' extraction process developments' the original biometrics input signals for excerpt durable repeatable feature for building data templates. The determination of complying this method aims excepting data storing spaces for

object tracking with via bandwidth, yet effectual and compactness. In this tracking to the image of reference matching is about 105 Kb [16] and it may be represented within a particulars template of around 260 bytes.

2.6 Structural Pattern Recognition Requirements

Structural Pattern Recognition Requirement (SPRR) routines for feature extraction, density estimation, transformations, and evaluation for processing simultaneously to integrating of its classifiers. Computer datasets are detecting and using patterns characteristic within artificial intelligence in supervised learning, which is clustering data in a set of general rule to expression profiling microarray pattern in line with bio trait data. The so-called reinforcement of a systematic process is spontaneous in which mechanism criteria on the application automated the analysis of microscopy data. In a matching process, it relates to position templates to regulate whether the flow and form of the same biometrics data sources are linked or not. In this case, mathematical computation and alterations are pragmatic in which candidate data templates to estimate the aloofness from a position pattern [17]. In digital microscopy data is to identify regions of interest so-called object. This object refers to such intensity, size, position shape the number of distribution. Structural Pattern Recognition Requirements (SPRR) is to process and identify the interest of the object, it is imaging experiment entirely under image processing biological experiment.

2.6.1 Specifying Requirements

Specifying requirements (SR) is the registration of the users and administrators or manager tracking task as authorized. One of the main core in SR is writing a

specification. Specification includes a description of work and all the process, which is a demand to meet its reliability, security, performance, features, and efficiency for tasks. This is called a one-shot testing, usually considered as checking critical measurements, reducing cost, which is a part of the systems, tools modeling and management. The value of the create reference prototype at specification requirements can determine the effectiveness of a classification while in using its 'development life cycle' installation. In security-oriented, criminal management applications, and the registration prerequisites the incidence of the user in an expert witness enthusiastic compartment desires period to attain users' bio traits to capture with a respectable detention images for biometric data interconnections via marker dispensation to authorize the excellence model successively verify non-duplication in a database [18]. Which depicts the enrollment to a determination to produce and a supply prototype pattern for the systems. As I mention in the above, the figure sample explains the flow of information to database temple.

2.6.2 Authentication and Verification System

Authentication and Verification (AV) is developed tools that can intrigue the matching comparison to biometric data in personal data reference to identify. It is the individual perfunctory to confirm distinctiveness of applicants by the use of sensors-chip through biometric data. This is one step at a time process, and is generally castoff for character documentation in communal devices, "National ID Cards (NIC)" and Passports etc.., for evidence of the holders as a legitimate holders of the identity [19]. It represents the confirmation design will strongly insisted on confirmation

process while the endorsement planning is expanding bimodal methodology. In confirmation process, biometrics systems attempt to response the inquiry “Is this X?” and verified and extract information according.

2.7 Identifications

Identification is the procedure of relating the unidentified a single biometrics sample to multiple data templates to catch out the uniqueness structures the user from the unidentified template. Both positive and negative authentication results may be obtained. Positive identification refers to verifying the connection “whitelist, e.g. VIP access to a secure area, whereas negative authentication refers to proving the non-membership of a group blacklist, e.g. pathological gamblers shortlist used in casinos”. “Who is X?” [20].

In Biometrics language, identification is conducted on by on step process, whereas identification referred to one to multi processes “i.e. the system has to find out who is the owner of the biometric candidate sample by comparison with a large database of biometric reference samples” [21]. Then, it marks differences while processing to the WHO ‘e.g identification and verification while information is tracking, the identification continuously precedes the authentication, it goes “we first claim who we are and then we prove our statement. Multi-two based identifications systems, by using two channels and two data comparison to avoid false and illuminate counterfeit data presentation.

2.7.1 Biometric System Evaluations

Biometric system has limitation for authentication and metrication in real life because evaluation cannot be cicatrized in a single sector. For instance, Biometric must compose of data quality, usability and security at all time since it is implemented for 24 hours to be accurate and false detect. The standards are occupied, a given factors by the uses of pillar systems, in the interpretation of criteria while checking biometrics systems as shown in table 6, portraying which of information and how is it provided and any sort of biometric attributes.

Table 6. Seven Pillars of Biometrics Systems

1.	Universalities	Who can provide a fake biometrics data?
2.	Uniqueness's	How can we find two persons with the same b traits?
3.	Durability	Durability is more than a generation
4.	Collectability	How convenient is to detention the biometrics?
5.	Performances	What can provide better systems?
6.	Accept abilities	How unique is the ability of systems performance
7.	Circumventions	How difficult is authentication of bio trait?

1. Universality: users will not be able to offer bio data as wanted.
2. Uniqueness: while facial recognition suffers from twins or looks alike, while bio-data must prove their uniqueness.
3. Permanence: Biodata will have to prove the information as good stability.

4. Collectability: fingerprint and facial recognition etc.., are set aside and place with DNA analysis and authentication, collectability by the biochemical process verification.
5. Performance: *High sensors network and illuminate old fashion such as the use of FAR/FRR levels* [22].
6. Acceptability: Dependent upon social taboos, most bio-traits are touching public devices might not be healthy "SAR disease in some country and Ebola in some part of Africa transmitted by physical contact" therefore, biometric sensors-chip card is to implement for local and international health management and its security are required. It can also detect diseases and drugs in a biodata examination.
7. Circumvention: while the system will be easier to attack at matching levels, presenting fake bio data, biometric sensors-chip card any false and fake information cannot be presented. The challenges of old fashion can be illuminated.

2.7.2 Biometric Systems Management

In Biometric Systems Management (BSM), which is in reference to its template because a better chance of matching appropriately against a live sample via sensing data. A biometric system, it required to update the reference to points to the biometric data, update the reference data capture multiple and use statistics to generate the reference pattern to correctly capture the fake less information, should be implemented. Automated Identification Systems (AFIS) sample is multifaceted systems. But mounting is a more complex because accomplished orientations must be fully anticipated.

The system process will also handle:

- Emergency actions in a case of frequent rejection caused by miscarriage to register information correctly triggered by rejecting the bio-data by fake data installation.
- Safety measures to avoid infection, diseases spread by touch-based biometric stations or check gates (e.g. Ebola or SARS (Severe Acute Respiratory Syndrome).
- Manager or Administrator are eventually assumed to educate and train the users on card or information for safety.
- Software, hardware, firmware and data upgrades and must be regularly updated
- Security trials to avoid threats against attacks and private information leakage to public [23].

It is usually assumed that biometric database information is opened to highpoint the fact that encrypted data in a database are secret. As said, biometrics or prints everywhere, yet biometric sensors-chip on the smart card goes to complementary process. It means that privacy-concerned organizations are somehow sensible to "biometrics with no trace". For instance, a vein pattern is a "no biological trace", invisible through eyes, it can only be possible by the biological dash exists after digital capture data in the biometric station. Actually, we ought to contemplate biometric sensor-chip data as it is private and confidentiality and completely different from secrecy on a security stance for such as it is needed by the user himself or government demands [24]. The evidence management can be either taken in public or unseen information management administrator during the biometric sensing while extracting at last phase of the captured data scan. In biometric system management, data protection

schemes and databases management are the core administrators and for which appropriate to use with the biometric sensors-chip card.

There are authentication's methodologies which are deployed in a timestamp or a token to create a random password in every few seconds. The leak of cause enrollees' information management should be disturbed by the biometric system manager to avoid the misapplication one's personal biometrics: by means of surveillance initially dedicated to public claim. This privacy subject that is similar biometrics to compare with some different applicants. This management is based upon PPK system.

2.8 System Installation methodology

With a biometric sensors-chip system-on-card (ASSOC), personal ID verification is accomplished independently with centralized existing sensors-chip technology and utilities existing infrastructure. Therefore, it is solved virtually all privacy and security issue related to ASSOC smart card system. The installation methodology and system requirement may be considered depending on use demands or public demands. We modeled the low-cost biometric sensors-chip component, which can efficiently handle information management for software model and system. The following Table 7 is presented to be installed within the smart device.

Table 7. Technologies Installation System Management in a Biometric Card

Technologies Installation System			
Cover Sheet	Inlay	Sensors-chip	COS
Credibility	● SatisfyISO14443&ISO10373-6's electrical, physical, chemical and mechanical characteristics ● Guarantee to supply performance, durability, and stability ● Anti-forgery & durability guarantee and quality guarantee		
Interoperability Interoperability	● Supply excellent interoperability between passport manufacturer and issuance process ● Interoperable with ICAO standard as international ID		
Standard Suitability	● Support ICAO standard, DOC9303, etc. ● Support ISO standard, ISO7816, ISO14443 etc. ● Support Java-card 2.1.1 or Multos4.2.1or higher in case of open COS		
Security	● Certification for COS used in card shall be ISO15408CCEAL4+ or higher which meet two Protection Profile ● Support smart card security its mechanism and supply security for protecting personal information ● Support additional security element		

- ✓ Credibility: satisfied ISO (medium software model) performance and guarantee to durability and stability
- ✓ Interoperability and Interoperability: enable to supply excellent operability for ICAO standard and international standard ID
- ✓ Standard Suitability: Support ICAO standard, ISO standard, Javae card standard or MultOs or higher.

System Installation within smart devices: In pattern recognition system infrastructure for a smart card, processes, and its validation are based on software quality and its reliability performance. While installing software into a smart device, it requires standard meet quality software. At the same time, we need to consider center, issuance center, backup center and office to management and implement biometric sensors-chip card for use with faultless. The system can be installing in all possible border check and immigration management or any major check gates.

Table 8. System Installation within Smart Devices

Part	System Description
Center	● DB Server, Server Backup-Be located in cities ● Biometrics system-Be able to share with system of NID ● Digitization system center
Issue Center	●Personalization system ● Be located in all cities
Backup Center	● DB backup system ● Be able to share with system of NID center
Districts	● Working Smart Workstation ● Operate and install in all cities offices throughout or ● The country with selection of principal cities
Overseas Consular Office	• Working Workstation-Operate and install in the embassies and Consulates in over countries and main offices

✓ Center: for easier system management, centers are to locate in order that shares biometric data management with NID (National Identification)

- ✓ Backup Center: database backup system and share with NID for ubiquitous computing
- ✓ Overseas Consular Office (OCO): This is to install for working stations to manage information and operate security tasks
- ✓ Government office manager installed data and database and able to trace users for security purposes and emergency demands.

2.9 Applications

Basically, old fashion based biometrics systems are used for either security or convenience within the limited place and settings from decade onwards. However, biometric applications are implemented always for a balanced achievement between two desirable but incompatible features that flanked by suitability, flexible and safety. Biometrics are used for both physical and logical control verification, there is a nonentity to misplace and forget, small and secure, but adequately sufficient uses since it is invisible data system that is encrypted.

Therefore, concerning protection, increased need for durable verification surfaces [25]. The owner proves a real identity by manipulative a reaction to that experiment on a preinstalled data and a response token. Managing criminal and convenience lives biometric sensors-chip card is proposed. In combination with pattern recognition and sensors-chip code, this proves the "physical link" accordingly.

A science report affectionate of microchip technology patented first perception of the memory card the innovative prototype issue for reimbursement in, which invented the first microprocessor smart card. The sample card for biometric-based smart card,

physical layer, is designed by the users of chemical sensitive ink, rainbow printing, fluorescent ink, and microcontroller line with ink. While biometrics information will be installed within the IC-chip and PC's database, the security of the card itself, sensible and observable elements components are embedded for the card's safety. So to say, these physically embedded elements will carry public biometrics and the IC-chip template will carry non-public biometric the combination of both biometrics system is implemented in the design of the smart card.

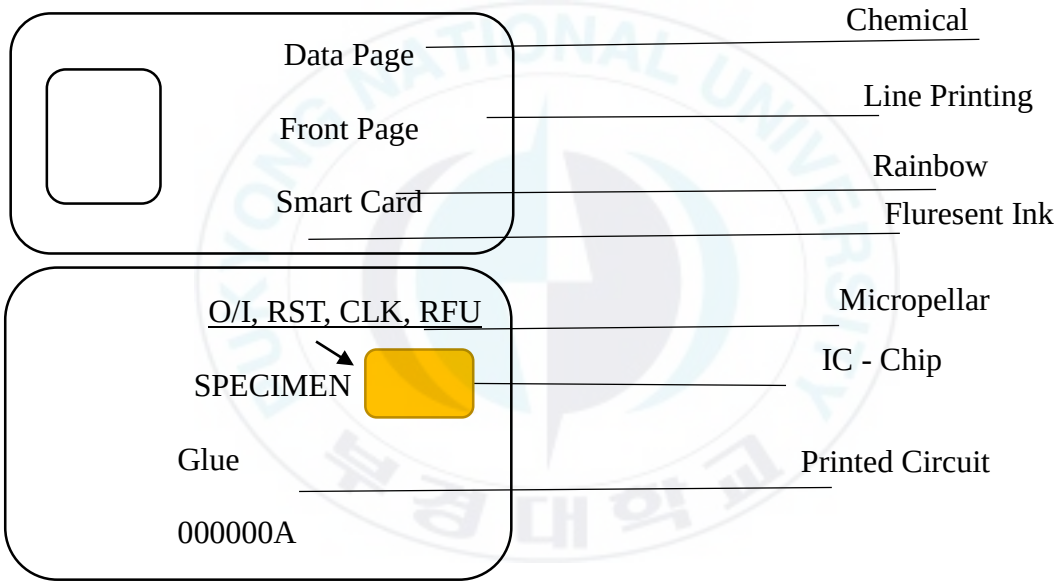

Figure 3. Biometric Smart Card Design

The idea of consumption a high memory volume of data in the biometric card in framework appears in several developed countries but with no misuse of these rights. This biometric card has 8 connectors: (IC-Chip) – C1 Vcc/C2 RST/C3 CLK/C4 RFU/C5 GND/C6 Vpp (old EEPROM)/ C7 O/I/ and C8 RFU (reserved for future use). For instance, "e.g, first mass use of the microprocessor memory chip-cards

was for payment telephone SIM card use". "The second mass use of smart cards, however, the first use of microprocessor cards, was with the combination of micro-chips into the use of debit cards". However, biometric seasons-chip cards are to deploy for being obtainable for personal documentation and verification entitlement schemes at local, national, and even to international levels use. Passport, NID (National Identification), drivers' licenses, credit card and health card schemes are more prevalent as I proposed as biometrics frameworks become most reliable form of cards [26]. This design is a bi-directional, in half-duplex mode, based on plastic support model. Needless to note that biometric implementation for criminal investigation, management and patient's dynodes' identification comply under the justice arrangement of government – it limits public uses till today.

Chapter 3.

Biometric Sensors-chip Card Architecture and Cryptographic Documentation Prototype

Public key cryptographic (PKC), also known as asymmetric cryptography, is a form of cryptography that users do not need be kept secret but the secret is kept already in documentation prototype. The private key (pk) is basically imitative from the public key (PK). This public key (PK) is not inhibited to the system's confidentiality as its information is encrypted with the public key (PK) only with the conforming PK. The PK is encrypted and stored secret, though the PK could be extensively distributed. Thus, mathematically speaking the public and private keys are related to the point of pattern recognition concept in data regularities mining while considering a person authentication and its architecture by the use of knowledge discovery in the database based on biometric sensors-chip pattern recognition system.

However, secret key cryptography (PKC), also identified as symmetric cryptography that practices a single secret key for both encryption and decryption instead of multi-secret keys. It is literally named as one-key and private-key (pk) encryption. Conversely, the requirement and information are shared secret by both parties in order that two side parties can have a copy of the encrypted information.

3.1 Biometric History

The earliest method of biometric authentication methods was by the use of handwriting (sign) and fingerprint. But, recently it expands widely. The so-called a

new password, biometric based card, is proposed late decade and it had/ has been applied in the hospital. Thus, it was usually appeared in scientific movies and in the novel which started with a scientific expedition discovering. In that telling story and movies, it portrays a very advanced civilization years ago. A futurist world we come closer using with the Multi-Pass based, a mixture of multiplication biometric cards handle confirmation two prints, one is users' information and the second is an actuality in which identical elements in another color.

In the story of biometric novels and movies, it is portrayed that uniqueness, measurability, circumvention, universality, acceptability and efficient performance. However, it has never been applied in real life. It was just a story that tells us about biometric.

3.2 Authentication

Biometric authentication is a physical characteristic for identification of a person by the use of eye, voice or fingerprint. etc., A biometric sensors-chip card becomes an authentication token for security. The definitive descendant of plastic cards into chip-card based and magnetic stripe cards into biometric sensors-chip card. These cards are to originally use for a unique identity number in the form of imprinted typescripts. Then, it can became a magnetic bar card that able to store digitally and response the information that matches to intended target That card used some kilobytes (kb) in a memory and secure information into encrypted for the user's name, validation date, birthdate, and account number. Biometric identification (BI) focuses on analyzing information and analyses to recognize its characteristics.

3.3 Smart Card Architecture

The smart card (biometric sensors-chip based) architecture of the composite product integrate provided by platform describes it functional performance and properties of protection to the card with bypass ability. This architecture is integrated to the application for trace and track a person's information which was installed and updated on the chip. So track and identify, the sensor-chip card will dispatch information and match the person in which verify bio-features and traits, without fraud and false. We architect biometric sensors-chip based smart card that tranquil a piece of silicon in a chip. The figure depicts the module of engineering which composes of silicon sensor – chip which is linked to a communication component, the whole being reported onto a chip describes a smart card module in sensitive data that contains the protection of the integrity of the chip. It replaces the rigged system of the traditional smart card.

Basically, old fashion based biometrics systems are used for either security or convenience within the limited place and settings from decade onwards. However, biometric applications are implemented always for a balanced achievement between two desirable but incompatible features that flanked by suitability, flexible and safety. Biometrics are used for both physical and logical control verification, there is a nonentity to misplace and forget, small and secure, but adequately sufficient uses since it is invisible data system that is encrypted. Therefore, concerning protection, increased need for durable verification surfaces [25]. The owner proves a real identity by manipulative a reaction to that experiment on a preinstalled data and a response token. Managing criminal and convenience lives biometric sensors-chip card is proposed. In combination with

pattern recognition and sensors-chip code, this proves the "physical link" accordingly.

A science report affectionate of microchip technology patented first perception of the memory card the innovative prototype issue for reimbursement in, which invented the first microprocessor smart card. The sample card for biometric-based smart card, physical layer, is designed by the users of chemical sensitive ink, rainbow printing, fluorescent ink, and microcontroller line with ink. While biometrics information will be installed within the IC-chip and PC's database, the security of the card itself, sensible and observable elements components are embedded for the card's safety. So to say, these physically embedded elements will carry public biometrics and the IC-chip template will carry non-public biometric – the combination of both biometrics system is implemented in the design of the smart card.

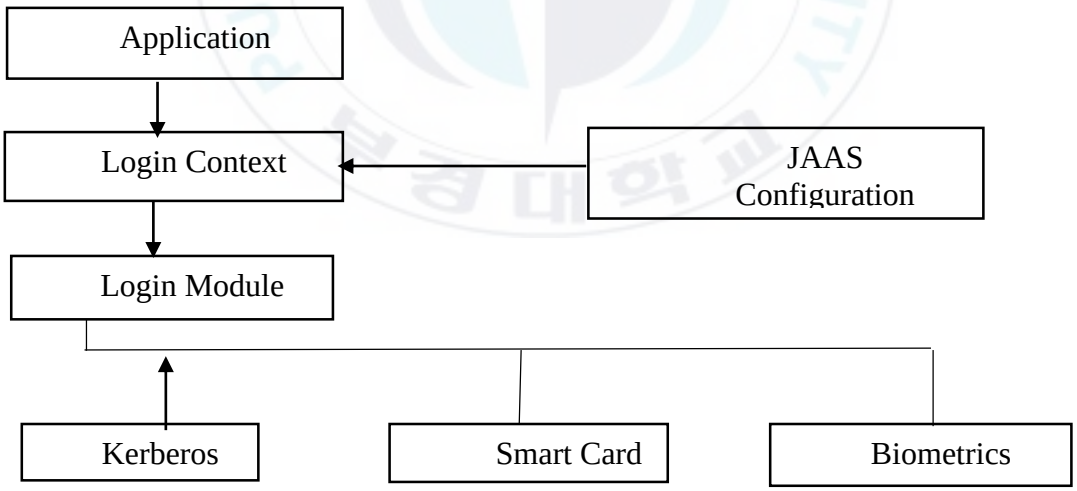

Figure 4 Smart Card Module Architecture

However, the card complete modular arithmetic is 14445, C++ is used for language to code the software to meet its module [27]. These features are well-defined by

ISO for electrical crossing point and transmission protocol in which sensors currents flow through the electrical network to transmission for character oriented.

3.3.1 Memory on Smart Cards (MSC)

The very first cards used many applications were a simple design with SIM cards for cell phone. These cards are both post and prepaid, and prices are deposited automatically in the phone SIM, which it is cut by the amount of the calls and charge when the chip-card data is used. The prepaid amount of charge which required by the users are stored in the memory card. Accessing to the memory card and its data are controlled by the administrator for the security reason. That methodology for the card was the simplest situation and that consists of only write protection and erase again for the data and its data chip. Thus, these types of cards only can be used not only for telephone calls, and amenities are retailed for preceding payment. [28].

This Microchip card is for memory card and it will be used in the form of transaction for information data. It will be securely stored private keys (pk) and execute up-to-date cryptographic that will make it possible to implement highly secure for information management systems. Conceivable, applications for microchip cards for biometric sensors-chip includes credential data identification, access control systems, secure data storage, verified electronic signature, and it is a multifunctional card integrating applications memory card. The biometric card is an operating system that allow applications to be encumbered with memory card hereafter information is installed for the user. This new flexibility biometric card is completely new application areas for security. The important benefits of microchip cards designed with biometric are large

“packing capacity”, the capability to safely supply in confidential data and the capability to accomplish cryptographic information.

A microchip card is a CPU and tautly a “Numeric Processing Unit” “NPU, aka crypto processor”, these are generally enclosed by supplementary well-designed blocks: screened ROM, EEPROM, Random Access Memory (RAM), Central Processing Unit (CPU) and the I/O ports [29].

Then, a biometric sensors-chip card differs from contactless smart card standard interaction supplied by its communications’ interface. A smart card on microchip card could procedure in a crossing point, time and again identifiable by the nonappearance of interaction on card template. However, contactless cards, data are transmitted without corporeal interaction with the sensors chip and the final terminal, then it has attained the standing letting very appropriate requests wherever the identity will not essentially be detained in the owner’s hand while using. Moreover, this type of contactless card also can erase manufacturing failure while electrical contact flows to the terminal. For instance, we architected contactless smart card and terminal contact.

Concerning in the core architecture, the different part of I/O from described architectures for a data memory and microchip. However, in some chip’s applications, the assessment and the impermeable check of the demands of the contract. After the source power flow on via sensor is impending may come along with the “Radio Frequency Interface (RFI)”, it can be recognized the fact that the dispensation command of a microchip will be depended on upon the distance of terminals and the reader interfaces, which is a complex computation. Contactless biometric sensor-chip smart cards are well-defined, based on card and terminal interaction via sensors or network.

3.3.2 Complex Architectures System (CAS)

A Complex Architecture System (CAS), biometric sensors-chip infrastructure, generally refers to the architecture inserting different two elements, but it is separated, microelectronic and applications, one card contacts and another one is con-

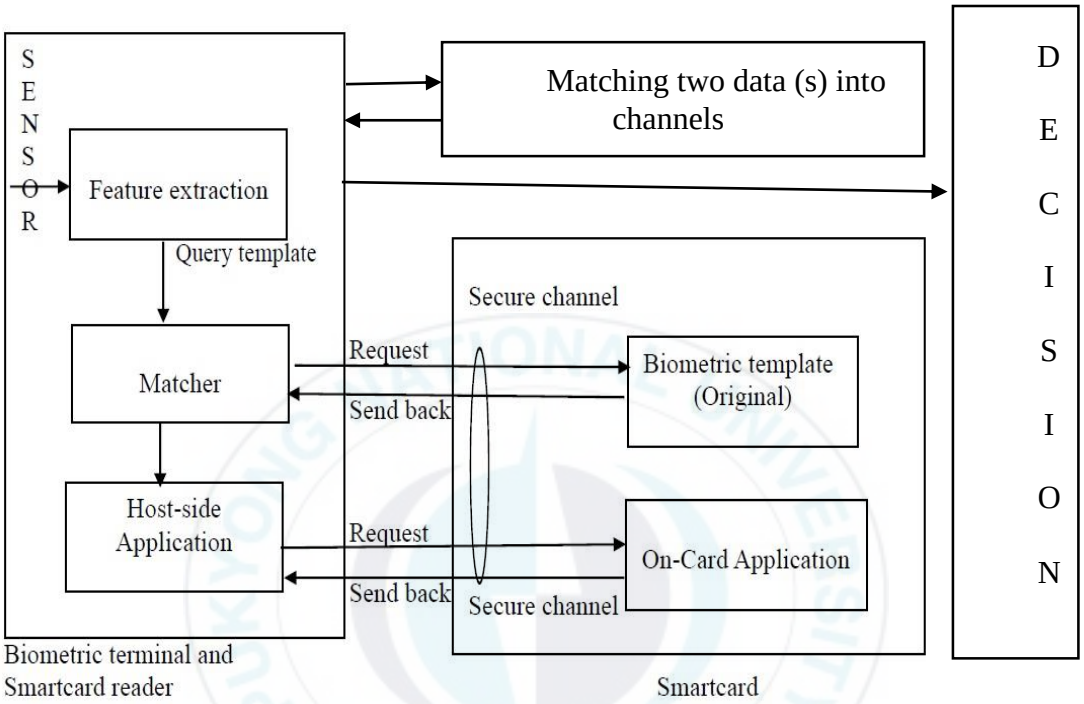

Figure 5. Architecture of Smart Card Communication

tactless. This is two separate cards, which have the same function, only differ in performance. The interface cards are deployed to a single chip and are accessible by both contact and contactless to reach the terminal. The concept is that two request channels, database biometric template (original) and biometric information on the card (present data) are matching information, to correctly verify and illuminate fake biometric. In the biometric matching process, original data template and matched directly interacted while on card data are hosted by the host-side application before it is sent to the biometric card reader and matches.

Therefore, these two cards are ideal for security, although the contactless edge is ideal for expediency. The representative application is a communal device by physical interference to contact controller and exchange massage in a biometric sensors-chip in a multiplication level. After the matcher inspected the information, query template in extracted to the matcher, the decision processes: reject or accept. Figure 5, details the two joint components, two databases comparison and matching process, passing two channel via sensors to correctly extract image and authenticate by multiple linking database and channels. Moreover, it maintains feasible and comfortable to use.

3.4 Smart Card vs. RFID

Inappropriately, it is sometimes referred to contactless smart cards as a Radio Frequency Identification chip. For example, 'biometric chip card is usually referred to as a RFID device. A RFID "Radio Frequency Identification" merely grants the identity of user devices by means of linking through radio frequency network, as a microelectronic code [30]. The RFID policies are less interfere resilient, but closable. However, a smart card is high cost and it is a physical safekeeping expedient, by calculation competencies and protected information storage. So, the modest application of a memory card can be called a RFID. By the operating system, generally named SCOS (Smart Card Operating System), which consents requests to be warehoused, recycled and managed autonomously in smart cards. Nonetheless, biometric sensors – chip card has yet developed. While RFID as a radio frequency based tech, smart card is sensors based authentication in this case.

3.5 Symmetric and Asymmetric Cryptographic

A virtual machine (VM) offers hardware abstraction layers, permitting applications, to run on VM acquiescent biometric sensors-chip card, hence achieving the ultimate flexibility and it is computed in a microprocessor. The data are supplied to seed in which it is used to create a real-time password generator by promoting to the random numbers' generator [31]. It brings the essential interoperability for smart card constructers.

In the development of a biometric-based electronic method, "MultOS Multi-applications OS", the functioning classification for the sensors-chip card was for a high-quality of the manufacturing. A decade ago, Java card is the most used solution on the market. Java-card built with Java programming language. In fact, Java card is a subsection of Java, developers should learn constrictions of java card, and the use apparatuses for compilation. A Java code is not friendly with the Java card code [32]. So, we implicitly discuss the current Java-card requirement from Microsystems.

Security Access Module (SAM) modules are found in electronic equipment's demanding robust authentication is primitive. For example, "e.g, security modules are found in Digital Video Broadcasting (DVB) devices and combined in communal for application". "Trusted Platform Modules (TPM)" tends to substitute Security Access Module (SAM) card where transportability is not an attar, yet TPM are fused with a mainboard, and these are no movable. As it is an application in telephony, protracted microprocessor assists a secure element for a portable application for protected microprocessor chip.

3.6 Identity Documentation Prototypes

Biometric cards are now issued without sensors-chip based administration management. Recently, these applications are characterized as the most advanced technology and it is convenient cardinal safety use. The significance of the digital utility is overriding and the features of the complete identification document are imperative, these forms serve as graphic documentation. Beyond protecting threats to a defensive, besides digital threads and counterfeit, which produces offer progressive physical countermeasures identity security for Optically Variable Inks (OVI) [33], called laser design.

Not silicon in a plastic card, but biometric sensors-chip based smart card technology has a tendency to multiple mechanisms. The core restraints are consistent card flexibility requirement demands. The impression of such card perception is to the improvement of the superficial of a unadventurous sensors-chip card. Components opposite to smart biometric sensors-chip card is to be flexible displays, microprocessor, silicon-based sensors and Micro Electromechanical System (MEMS). Sensors-chip card may be implemented interesting energetic safety structures for tamper-resistance for the light sensor, and it can give the opportunity to save Random Access Memory and the prospect for large assortment contactless frameworks' infrastructures.

A Biometric sensors-chip enabled smart card could provide prove that the physical link with the manager, administered and to the user via sensor network. This component infrastructure and deployment by the use of smart device within a biometric sensors-chip card will illuminate the existing technology in term of the card and it usage for safety.

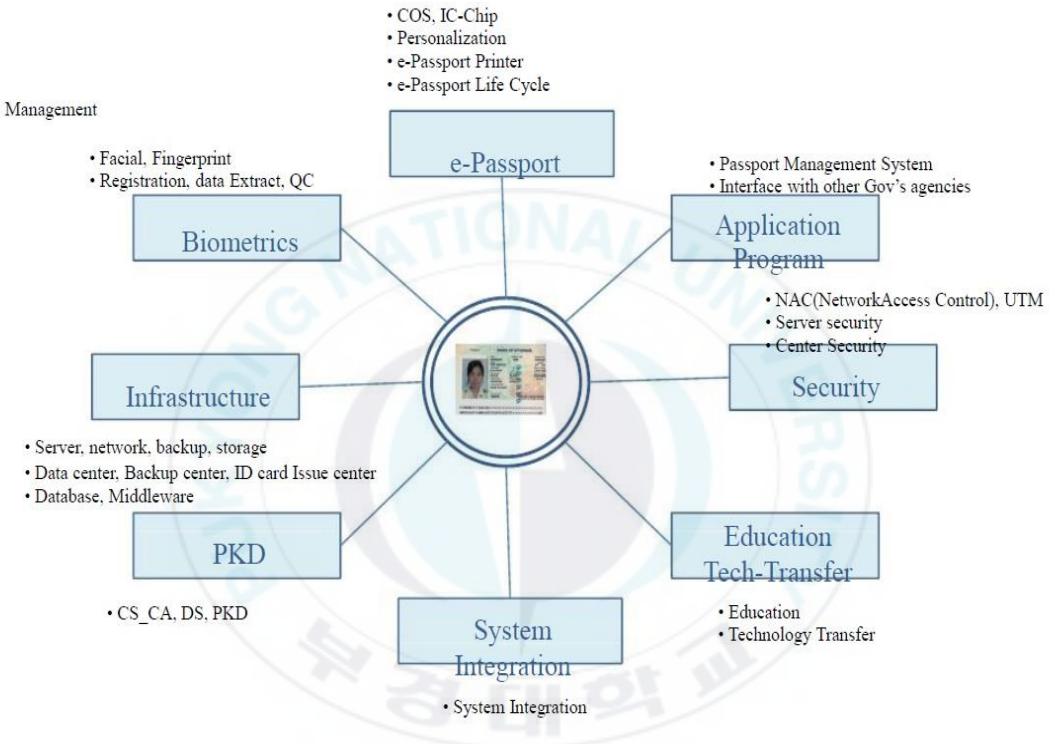

Figure 6. Concept on Card

Figure 6 shows that it is initially developed, all data in a card is of sorts of smart card components, for biometric sensors-chip smart cards with different display technologies. The concept of this study is to prove that it is a possibility and deployable artifact in authentication frameworks [34]. Another concept of the prototype is to encompass memory abilities of sensors smart cards the classical sufficient of kilobytes (kB) by

means of multiple biometric sensors-chips technology and the conductive glue interconnections each to others. These technologies are to be in the future world, for example, within the Microcontroller SIM chips, serial link is plugged in Smartphones and perform the activities with joint sensors-chip and smart devices.

Table 9. Smart Card Architecture and Module Prototype by Level

Level 1	• Visually distinguishable security • Choose from features: Microtext, Rainbow etc., features • Incorporating more features will increase the complexity of the overall design
Level 2	• Devices and tools used to e.g Ultra Violet, etc., • Distinguish security features
Level 3	• Laboratory and precise select after considering costs • Inspection for distinguishing security features

ID card requires more than 5parts of security elements on the surface to prevent damages. The appearance of biometric sensors-chip and frameworks inquiry in silicon chip addition, the awareness came logically that biometric-based smart cards could replace user's verification without passwords. This automated machine challenges in the combination and confrontation are of flexion, however, the issues could still remain concerning the microelectronic issues. The idea is that catching the image, data consumption of such sensors-chips and particularly image processing desirable for

biometric data and its image comparisons are out of the competencies of traditional smart cards to the sensors-chip card.

3.7 Confidentiality

The innovative application was suitability for Logical Access Control (LAC), sensors-chip capture image is changing password request. However, security is in mind that the orientation pattern is steadily the user's smart card instead of the patrons. In fact, it is satisfactorily protected. Yonder packing the orientation pattern, a probable feature for challenging technology, a CPU smart card can take benefit of its dispensation abilities to exceed the antagonism. Then it is originated to the idea that the study of the difficulty of biometric software primitives for extraction and to matching, and discover appropriate ways to advance tools into the incomplete stand.

The desire of "Match-on-Card (MOC)" features: then silicon based are stored the orientation pattern, and also is trustworthy during the calculation contrast. These features drive with numerous disputes such as a performance on the contactless card and contact card. Rather than receiving biometric data information from the uncertain external risk levels, therefore, a biometric sensors-chip card could embed the biometric sensor.

In the non-governmental applications, rules from the privacy-concerned organization cannot permit the invention of personalized databanks as a secret use. These principles also center the fact that an obligatory used of private use to the database of the users' biometric information tic data. The advice the procedure of "Match-on-Card (MOC)" alongside biometric sensors-card so as to clearly assurance the owner and the secure personal privacy and information management system. However, MOC, SOC

and TOC incomplete for biometric management and maintain for security related issue, as the high risks of fake and forge. So, in combining to models and an addition approach called PPMF point pattern matching framework for confidentiality. These modeling's combination to a single model, which develop card standard instead, not public biometric security in this case, for PPK access and private biometrics access.

3.7.1 Integrity

Integrity is defined by a virtual level of risk-reduction by a secure function of performance. The measurement of performance is based on functional safety standard and dependable standard. In essence, each risk reduction requirements levels, it is based on a probabilistic analysis and analyzing the maximum risk and failure fraction. The fundamental objective of integrity is to enable both hardware and software understanding requirements. Integrity is historically used in software development life cycle and diplomatic performances, it applies to the application requirements verified system and device verification. Which means the smart device and it software performance must requirements for categories to achieve systematic safety in redundancy development and protecting a dangerous failure in the systems.

3.7.2 Cryptology

Cryptology is the discipline of obfuscating. Obfuscating can also be called cryptanalysis. It is the knowledge based offensive systems and estimating the stage of confrontation a secret data outflow to improve keys development a rigorous concept

and suitable framework, thus it is evolving specification analysis. Cryptanalysis is commonly stated to as code breaking concept [35], and so the idea is to prevent the enemy from interrogation and disassemble, as to prevent to reveal the secrets information.

However, It is usually referred to "Secret Key Cryptography or Symmetric Cryptography" (SKC/SC), which is the solution to cryptography problems of public key encryption, sharing protocol, whereas fundamentally different. The second, recently, is presented in "New directions in Cryptography", trailed by the first implementations with a complicated solution to the problem which is called "a method for procurement digital signatures and public-key cryptosystems". The system here provides balancing keys that a certain newfangled problem about lattices, the assumption attack the scheme resisted several attempt to "private key" (PK), "public key" (PK), and "the public key" (PK) are desirable and confident operations. For example, "e.g, private key (PK)" is required an additional operation and decryption occurrence. This cryptosystem is usually denoted to as "Public Key Cryptography or Asymmetric Cryptography" (PKC/AC).

3.7.3 Application for Identification

IT identification applications are cryptography comprehensively, both unoriginal and current. Applications include a protection for mobile banking, mobile telephony management system, multimedia broadcasting, e-Government and identity documentation, access control, and network security, this is one of the best illustrations of the public and insecure communication network protection. In general such applications are related to a security element able to calculate "cryptographic algorithms and supply

large cryptographic keys", within that sensors-chip based a card microelectronic chip is utmost repeatedly used.

3.8 Primitives Cryptography

The first and spontaneous goal of cryptography are the security of privacy and secrecy, intercepting an encrypted information of communication can be incapable of recovering the innovative, without accessing into secret information. This secrecy information is only attained by the encryptions and with decryptions systems so as to preserve its development cycle of cryptography. And also in another word, a primitive cryptography, which exists within that primitive confidentiality.

This idea is close to straight to authentication message that a person is normally verified by a secrecy information that possesses itself. This identity management is known as a "Challenge-Response Protocol (CRP)". There is no comprehensive exist lists: obscurity commitment, non-repudiation, randomness, zero-knowledge authentication, and accessibility for services to the end users. This biometric is secret to the administration of information to the user in a check gate and is not to allow to detailed rather than it is demanded in a specific point, to automatically update as the card is used.

3.9 Encryption and Decryption Functions

Encryption and decryption functions are the methods of converting pure information to an unreadable information Cryptogram, except for who is having the special key. Although it illustrates an unequal encryption and decryption systems are wherever senders use the receiver's PK, whereas the receivers use the own private key to decrypt. It is noticed that the presence of classifications enthusiastic to encode

data denoted to cryptography and systems committed to encryption referred to as torrent encryptions or it is also recognized as symmetric cryptography.

Hashing functions are transforming the process and plummeting the invisible data of data representative of the message, also as bash biometric role of biometric functions. Hashing is a one-way function and it is preferably collision-free. Basically, the problem that is cluster together keys as distribution, chopping is lost and density occupation on high-order bits performance. Familiar solutions, and very much used in information technology record keys and value for actual keys, collections and is extensively used in large data management systems.

3.10 Message Authentication Codes

Actually, MAC is fundamentally a key to a hashing function. It is a palpable method to physique an MAC authentication codes to the confusion a encode phase during massaging biometrics data and switch with clandestine significant. Sometimes, it is known as wrongly "digital signature in symmetric mode" that demonstrates a binding hash function. Rather a "Digital Signature" it is a calculated system to signifying a unique validity of arithmetical documents. This arithmetical signature stretches the receiver and objectives notion so that data document is formed within an identified correspondent, and that it is not transformed. Fundamentally, the digital signature is contrary to encryption system in asymmetric approach, one uses own PKs to encryption, though verifier routines the sender's public key to decode [36]. The most significantly essential feature for the digital signature is a nonrepudiation of the author because it cannot be accomplished with an MAC, labeled in an MAC verifier which

possesses the similar key as the MAC and thus it can possibly counterfeit the message and generate its MAC.

A challenge-response mutual authentications are a family of protocols that one party helps and another party and carry an effective reaction, the response to the inquiry, to be authentic. The simplest sample of a challenge-response protocol is a PIN code's authentication when the requesting passwords to reply are the PIN codes. Currently, this protocol demonstrates the challenging party known as a secret but without interactive. Mostly, challengers direct a random value to a challenge party intending to encode the random value and comparison to the secret key, then calculate and conducts communication back to the challenger's result. Challenger responses mutual authentication is a 'two-way challenge response', by irregular cryptography and this also can be completed by validating the challenge key via a private key.

3.11 Keys for Protocols of Cryptography

The Key for Protocols of Cryptography (KPC) cohort in symmetric and asymmetric systems, it should depend on a random feature, the evading obviousness of the present key. In the particular asymmetric protocols cryptography, the random protocols manner creates the matching key is mathematically calculated from the first process. KPC for accessing information is based on PPK. On the other hand, it is generally insufficient, but conditions for the encryption systems to be protected is the key interplanetary to prevent comprehensive examination. The key contract is a device in which a collective secret should be derivative within two parties, as a utility of data connected to each of the other that no party can encode the consequential assessment. The objective key of a PIN code or a "One-Time Password" is, for authentication, to mark

it an extra complex process to advance unlicensed access to control assets. Conventionally, motionless passwords can simply be retrieved by an unauthorized impostor specified time. Through a repetitively varying password, as it ended with a "one-time password", risks can be significantly condensed.

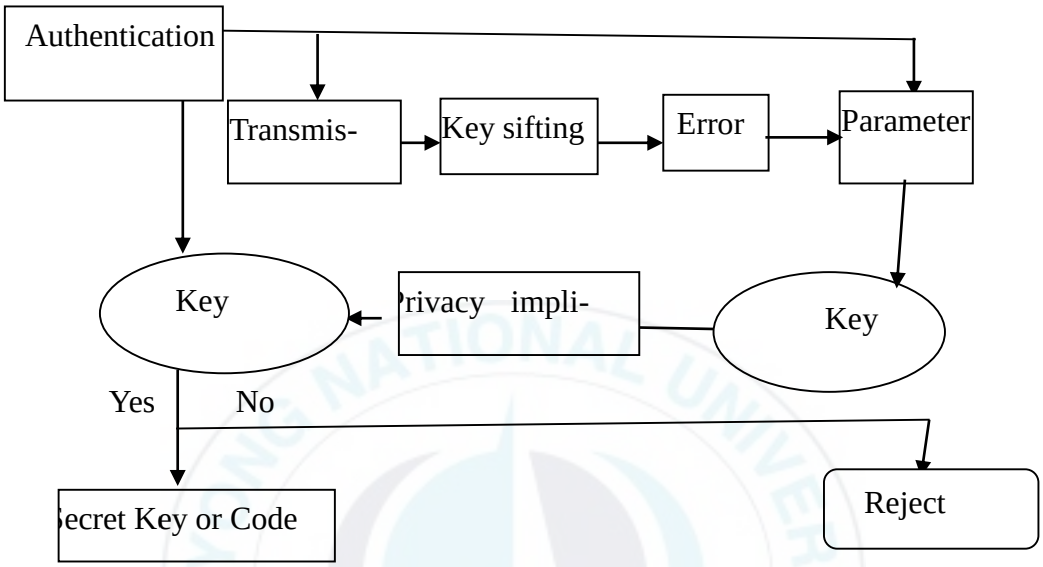

Figure 7. Keys for Protocols of Cryptography

3.12 Interaction with Smart Card

The anthropological simple eyes cannot remember a complex and large numbers, so it is required for locked cryptographic keys and cannot straightforwardly deploy the number to process a report to a trial. Firstly, biometric sensors-chip card is a seamlessly protected ampule, and such keys and computer of such as a verification processes. A sensors-chip smart card is able, within few seconds, the information will attract and spawn a key for the cryptosystems. Secondly, the interaction is to distribute information and agree with a key on the secure digital system. In fact, the smart card completely plays a part of a private perfunctory for the system verifies the entity

instead of the actual users. Nonetheless, a secret only distributed to the card that can activate to route via online confirmation. So, cards cryptography will attain a faultless two-factor validation within something you have and something you know about. Much more than a human guarantee, shared digital devices confirmation comprehensively procedures Secure Access Modules (SAM) cards, plugged into communicating systems of transparent and detachable and upgradeable security structures development.

Interaction of biometrics and cryptography is somewhat paradoxical in term of their interaction and authentication under security methodology. Cryptography requests identically reproducible and consistently distributed data, although biometric-chip data are basically not able to identically reproducible and it is non-uniformly distributed data. Additionally, ID and Passport, cryptography supports to preserve biometric data, are secured and perform admirably. Thus, these collective applications sophisticated the progressive interaction may lead to idealistic solutions as the use our biometric authentication as a cryptographic key with reproducibility tasks for the use of cryptograms repossess stored.

In the same realistic case, biometric sensors data could be never identically reproducible, negotiate a tag function of biometrics [37]. The interaction of card and bio database to the authentication process, card's reader connects to the card holder and original bio template of a person via sensors wirelessly and identify the users based on the interaction of card and previously installed data.

Chapter 4.

Identification and Authentication System

Biometric identification and authentication system becomes the modest and most attempt to deploy in biometric technique, in public administration and criminal management, because of its maturity and cost and performance effectiveness in detention and processing. The specific curiosity for biometric sensors-chip based card for the criminal investigation area is primitive to extract because latent limitations that remain in the objects are touched and handled. These are left scum made up of a mixture of secretion, silicon-based solid card as an amino acids element composed that other susceptible factual the data might have touched. Generally, the feature of sensor susceptibilities in the biometric system as portrayed as the below lists.

- A fake biometrics: it signifies the use of faked biometrics attribute regarding not - biometric sensors-chip based card systems.
- Replaying longstanding data: it signifies replaying a captured of previous matching data and contact to the system.
- An overriding extraction: it signifies spares of the malevolent package that can be a production for the preferred aggressor.
- Synthesized features: it signifies procedures theatrically manufactured template that prejudice for authentication progression.
- Override matches: it denotes an additional match with malicious packages, which will amount produced falsely high score.

- Modify template: it denotes the operation of orientation databases to add anticipated patterns.
- Intercept channel: this denotes the apprehension and additional reference data to be desired.
- Override decision: it denotes the auxiliary for the last result to vigor the access to the systems.

It should note that the major problem of a biometric system is user security. These methodologies are to hide reference biometric data for safety public use so that confident matching reaction to the contest but the candidate is a right, it is thinkable to the candidate that it pursues masterpiece of procedures related safely.

These susceptibilities are connected to identity threads, while the aggressor may emulate an authorized user. An additional issue of such structures is the opportunity of the duplication to characteristics in multi-enrollment. Based on the security requirements of the claim, the development scheme processes a contrast in its database encrypted data. Traditionally, attacks tackled by using cryptographic apparatuses for data reliability and verification, it is most demand in requirement process in a software system for the smart card. At the same time, these attacks cannot be tackled by traditional security tools of information management systems.

4.1 Identity Management and Continuum

In a "Storage-on-Card (SOC)": refers to biometrics sensors-chip frameworks in sensors patter reciting for systems at verification demand. The uses of the non-volatile memory, later permitting cost-effective biometric card utility. Nevertheless, a reference template is unprotected to dissimilar attacks when interconnected. In a

Match-on-Card (MOC): biometric reference templates will not be interconnected within the smart card database after it is written on the process of the enrollment procedure. The applicant template is referred to a biometric silicon-based smart card evaluation administered. It defends the biometrics pattern desires the authoritative power in terms of mainframe and reminiscence properties. This is predominantly stimulating once that effects on the validation of recycled locally, and the stimulation access is badge private key for arithmetical moniker performance. A malicious incurable apprehending an applicant templates will not partake while matching or not matching.

"Partial Match-on-Card *(PMOC)":* it results in the benefits for preceding solution, authorizing effective sensors performance and defensive to biometric information flow. Biometric data extraction is divided into two categories in the management system, first for a public part read in the terminal, which will be inaccessible on the screen of card's reader within a task implementation.

4.2 Authentication and Decision Making

First of all, a refuge of a PINs-based confirmation apparatus, ones in modest and outmoded smart card system is based on local storing of the cryptographic hash of the password. This is possible middle because it is a deterministic environment of confirmation, uncertainty the entered applicant password is the right one then its mess rate generations to the stored a jumble cost and the substantiation thrives, as the applicant entered aspirant as batch significance confirmation miscarries. In biometric system most concerned and risks are counterfeit information. Therefore, the simplest and feasible method is having to secure data's to be marched, pre and pro, before the decision-making process. In this case, both physical and behavioral characteristic should be

corresponding and biometric information are to comparable. When presenting fake information to the card reader, pre-installed on the database will enable mismatching the process and prevent from counterfeit information acceptance.

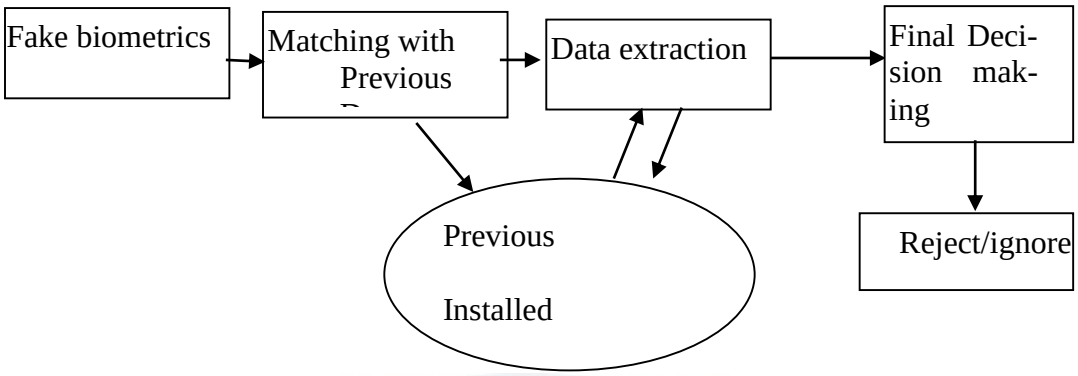

Figure 8. Flaws in Biometrics Systems

This method on safekeeping is dreadful to biometric data security. A new detention of a biometric candidates' results in fairly different data in which pointers of numerical nature of biometrics constructed for verification detachment to assessment models. The allusion biometric pattern is completely altered within mishmash processing matching on the applicant. The means the outcome is biometrics reference should be stored locally in the clear scheme.

The unfathomable physiognomies examination of password and biometric show a pure obstruction:

- Secret: PINs or codes are secret, but it has to be to make sure a difference between biometrics leaving traces
- Delegation: conditional countermeasure to the application, the designation capability is mandatory in data communications

- Changeability: in an incident of concession, PIN is denied and another one is distributed. It is not tranquil with biometric traits
- Personalization: a code is delivered, while biometrics requests user enrollment to security area of the process ability and information management
- Comparison process: comparison between two PIN codes or passwords as an inconsequential charge for biometric sensors card, though comparing data requires need to extract far more than calculation properties
- User convenience: password and PIN code should be memorized and it can be managed via several PIN codes, although biometric needs no effort
- Vulnerability to eavesdropping: a detached checking off activities may expose where biometrics recognition cannot comply in that way
- Vulnerability breakouts: to brute force, while a biometric pattern is insufficient hundreds of bytes
- Countermeasure: attacks against passwords are qualified, but countermeasures are developed. Attacks against biometric system is an innovative part with no mature countermeasure
- "Physical" operator verification: user confirmation is permissible with PIN code artificial, "this PIN code is personal, do not communicate it". Biometric is a rougher connection
- Capture: incoming a PIN code is the modest and inexpensive, but apprehending a biometric peculiarity is an expensive charge

In spite of the above-mentioned susceptibilities of biometrics traits, we need to counterbalance with circumstances where biometric is a case protected than passwords. This antagonism endorses the decent complementarily of passwords and biometrics sensors-chip based data. The replacement of one with the additional element ought to be prudently deliberate contingent to the embattled request.

"Information System Administrators (ISA)" complaints around manipulators marks the PIN to their PC' screen to unlock their phone and neutralize the safekeeping feature measured as counter convenient use. A complex password to be memorized is obvious henceforth and it could be effortlessly predicted in a modest vocabulary occurrence and additional sophisticated occurrences. Therefore, in most gears connecting none security awareness operatives of the atmosphere demanding a minutes of safekeeping, the expenditure in biometrics will deliver a weak, but tranquil safety apparatus.

4.3. Authentication Factor Concepts

A pattern for authentication is fixed of a skin line, locally equivalent, called points and vacant interplanetary between the two uninterrupted crests termed sales. The three shapes of the patterns, separated by semicircles hoops and spirals, are the level of information it might scrutinize to classify patterns. Then, a typical charge of a point to point incidence is about a partial millimeter and the normal value ridge stature. This information is impractical to advance with pattern corroboration. Pattern cataloging is obligatory for an effectual investigation for matching contenders inside huge folders such as AFIS and schemes in overall.

The second level of authentication concept is the called minutiae in particular. This is specific points of the pattern where a point is conclusive to forking. Thousands of such points may be extracted from a pattern, it is enough to keep with consistent pattern authentication. This technique is a criminal science that have used to conduct pattern identification. The other, level information are cored in a delta location. The shape of points and gorges, in its minutiae, cores and outlets are exclusive to each other's and allow to recognize constantly throughout the generation. Generally, an accurate corresponding the respondent's data extractions are about eight to twelve, which is minutiae that enough to achieve with a confident print recognition.

4.4 Biometrics Sensors Authentication Attestation

The levels of biometric sensors authentication on information is openings location along the ridges techniques described in line biometrics capabilities, it can be able to replicate initially and instant equal data examination. Biometrics data management on a fake information is a trial since the creation of fake tools and counterfeit materials are easy to mount as technology so advanced to catch up in general.

As mark duplicate solidity procedure is the typical for the altercation of 6-bit, 500ppi print pattern smiles inside the Criminal Justice Community (CJC) [38]. The ordinary pattern scope in this layout is of about 12 kB. This is the design deposited in the biometric sensors-chip identification card. The allusion principles are based on the models of ISO/IEC and ANSI INCITS [39]. For example, recently, IEC design to store "best National ID (BID)" card, "embedded electronics systems (EES)". Common prototype sized that compressed biometrics setup desires at least 250 bytes, double as to design in pattern recognition in restructuring, on sensors authentication attestation.

To state that these morals are somewhat not operational and variable since it is not actually accepted by a majority of the biometric sensors examiners and expert communities in obstruction to minutiae descriptions average and documentation and verification for a person information.

4.5 Pattern Recognition Spectral Data

The reference standard for spectral data pattern recognition is standardized as at least ISO/IEC 19794-3 model [40]. This spectral data average defines a system where a pattern image is segregated in minor covering some ranges, cells are implicit with values for such elements and parameters. This is approaching from pattern recognition occurrence on spectral analysis such as "Discrete Fourier Transform (DFT)", addition manifold utilities. The normal prototype choice in this design is at least 400 bytes. This standard of recognition spectral data is as stored, which instinct into a level of reference data.

Again, the reference standard model for skeletal data defines a methodology in which ridge appearances are characterized by pixel segments, all line are coded after a preliminary opinion to its conclusive statistic with uninterrupted fragments, the fragment existence comparative the preceding to one by a variation in direction. The mediocre pattern infrastructure scope in this design and system is of approximately 500 bytes [41]. Actually, to higher the model can make the system better, this standard required initially lacking at standardization because of its compacted magnitude in appraisal through compacted identical and capability systems on "pattern spectral techniques (PST)" for interoperability.

Chapter 5.

System Monitoring and Administration

A comprehensive summary of biometric sensors-chip technologies can be found in automated information data manipulation system. Different images are the captures of the same sample patterns for biometric, thus, it will not give unerringly the identical copy. The primarily outstanding technologies are the poles apart technologies obtainable with automatically detention pattern recognition system via biometric sensors-chip with the particular identical sensor, images might not be the matching, but inside elements such as DNA and Vein are unavoidable that biometric will trace to extract the accurate information.

In this case, the sensor is going to automatic devices are too cleanly capture biometric information under a developed system that enables to replace the elements of object layer-based technique authentication. One of the most significant technologies available in this case is constructed with various assets and endorsement [42]. These slopes are non-exhaustive. Nevertheless, the contemporary principal skills are of arcade and silicon-based, and these are of a capacitive and thermal measurement framework. To consider a complex system computer-based information administration, basically, it is necessary to ensure that the right set up procedures personnel data needed for task tracking equipment must be chosen. As many contemporary systems are more elaborate that corporate-wide function.

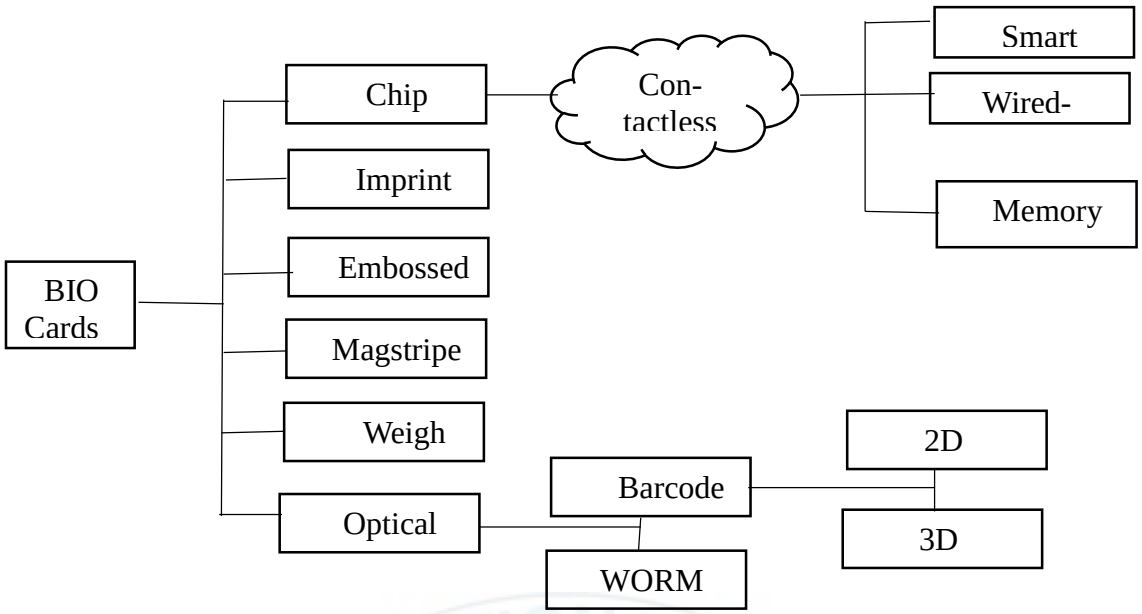

Figure 9. Infrared Biometric and Captive Biometric Transmission

5.1 Backups Technologies

In backups technology, some of the ophthalmic sensors established on the light reproduction to the whorl, if the exemplary and systems are constructed on biometric technology. To believe that the user just puts his digit or information on a smart device pattern recognition substrate because of the reflection of the light, successful penetrating to the layer's module as it is adjusted and recognized as true evidence. Therefore, supplementary compacted, such expertise usages light transmission to a surface portion of which adjacent interaction through the imaging microelectronic device over a thin optic fiber layer.

Biochip are connected to sensor and imprint via contactless smart login system into memory and store in original image while BARCODE and imprint are keep in high divination image such as 3D or 4D. This backup system is for two database matching processes and forge and lost protection safeguard.

Alternative marginal optical technology, and utmost immense is based on smart device sensors-chip through a vein, iris, finger, voice, and eyes, the light source is employed above those components, and the imaging element is placed under by using the biometric sensors-chip information management system as a backup's technology.

A most current technique is conventional to multispectral illumination of the palm and fingerprint, which is known as an unaffected and distinctive print examining replication of skin properties by which an extensive variety colors wavelength analytical proof.

The capacitive dimension of the pattern recognition is the most recycled technique in embedded microchip technology. These outcomes are compacted and capable of producing such a systematical sensor in semiconductor developments in which biometric and sensors-chip commerce.

5.2 Sensors Monitoring

Sensors monitoring is conducted ubiquitously by automated smart device. Field effect sensors are in fact an irregular of capacitive sensors, sometimes termed dynamic sensors capacitive. It is categorized by the circle from of electrically conductive place to place to the sensors cathode plate. Once capturing the information, a current will be functional to the circle, therefore engendering digit data. Starting from a standard electrical that monitors procedures of the neighboring planes, displaying the sensors engaged to the dielectric which can ubiquitously measure the character of the conducting exteriors. To invert the preceding sphere standard, each of micro-antenna can visibly be electrified produced from flowing the electric through

its final destiny. That circle is in progress and that can be enthusiastically diverse by real-time controls panel to adjust recognition of different kinds of extremity- print features. Additionally, it is claimed the benefit is the capability to capture accurate images with damaged data or its patterns, the sensing principle interpretation to the ridges found unprejudiced underneath for sensors monitoring.

5.3 Visualization In Real-Time

Alternative uses that extensively recycled sensors based technology expenditures of a combination of pyroelectric signal and relative material generating an electrical to the heat, whereas it is enduring these typical semiconductors engineering methods. Designed for mechanical reasons due to the assets of pyroelectric substantial element, the prerequisite of uniform reheating of the physical swiftly once insertion the slither verdures amount modifications. Hereafter, to put down the technique is extremity transversely the small silicon portion, resistance gives temperature to the pyroelectric cathode quantifiable, while valleys will have no effect on the pyroelectric factual. Nonetheless, it may annotation that Atmel finally motionless the developed of such an expedient afterward more than years of development efforts.

A silicon-based pattern infrastructure biometric sensors-chip derive, such as the touch sensor and the swipe sensors, in two different form-factors. There are some disadvantages, as actually easier to routine, yet agonizes from the touch sensor, which is a silicon area length that makes expensive because its surface can possibly trickle a comprehensive hidden photocopy with heavy usage of the surface that could become dirty, later complications to assimilate in trivial implanted computerized smart devices.

In critical perilous sensors, which might measure as user's inexpedient, it acquires appropriately critical remark data transversely to complete the perfect the sensor photocopy. Yet the correct signal comes in an infinitesimal event of training. The critical remark system routines a debauched share the pilfering images throughout, as it devoted procedure at this time for renovating the accurate spitting image since the some portions are reclusive. This seemed a little bit irrational when and after it is designed based on the notion of biometric-based silicon-based sensor manufacturer originates the merchandise choice. Still, persistently dropping silicon based area because of sensors communication and signal propagation, thus reducing evidence data from a biometric sensors-chip card, which can reach an achievability perimeter concerning the slightest satisfactory scope for a biometric sensor.

The flexible sensors is a high performance built-in and the comprehensive of critical to an artificial intelligence. It is the emergence of polymer microchip technology permits the progress of flexible sensors with a low control ingesting, with two physiognomies model compliance within embedded microelectronic procedures. Though, since the start-up dedicated erections for major microelectronic that have increased and collapsed in advance of such flexible sensors.

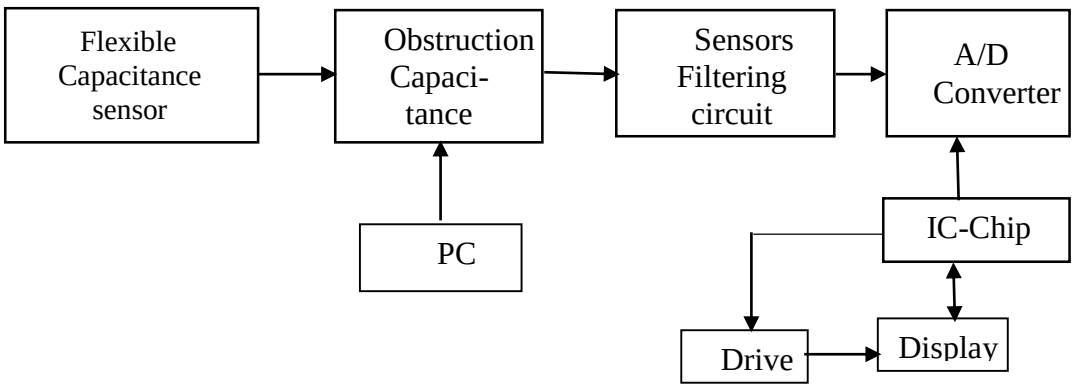

Figure 10. Flexible Sensors Comprehensive Intelligence

5.4 Change Management Administration

The Chaos Computer Club (CCC), the advanced group in Information Technology (IT), published the pattern recognition infrastructure for Change Management Admiration (CMA). The design for administration encompassed in more than reproductions of the flick elastic encloses moderately in desiccated glue. However, latter standard can be secretly attached to information management system and used to leave a person's prints in public, in the use biometric reader's plate.

In explanation of the attack trails, these are obtainable with either with digit owner or without any cooperation that displays diagrams slices manufactured either silicone or neoprene. Counterfeit informatics data might similarly be built in aspic, like material latex. It is built fake informatics data counterfeit with all these resources which had attractive respectable consequences in different sensor technologies, apart from gelatin, thus it is added some dilemmas to attain simply reproducible occurrences in silicon-based sensors. In that instance, it is ordinarily essential to catch out a blowing on the biometric sensor before capturing to improve the mugginess connection between

the counterfeit digit and the biometric sensor. These recognized artifices are also valuable to improve the eminence of the duplicate optical biometric sensors-chip pattern recognition.

The purpose of this effort is sponsored and being the capability to physique up simply reproducible attacks through long-life impression with reproductions on the projection to address international certification needs for pattern recognition systems for management administration at medium term, as at this time it is security criteria. Here, at first, the targets patterns recognition administration squint that it is supremacy and specific capacity to consent hints. The same exploration courses pointing additional installed biometric technologies are in the conduit.

The dramatis personae has the benefit of being tranquil flexible and unaffected afterward acclimatization, superlative for eliminating the optimistic. So, it can be obtained to mold with identical details of the information pattern. The mold is refillable manifold epochs, nevertheless, the recycled factual is never eco-friendly to mold additional pattern.

Another one is plasticized. Plasticizer is an oil-based soil generally recycled in animation. That is enough tranquil to deploy, then it is rapidly acquired a mold within elevation details of the biometric data. Still, the concern after expending it is of the material can be recycled multiple times to mold another existing digit to take care of the mold.

This substantial is not so appropriate to manipulate stretches virtuous outcomes in pattern's minutiae. This designed is mold manifold used substantial evidence for

this case. So to speak, Alginate is the utmost convenient recycled material for decoration in leisure activities, permissible remedy, and dental parodies [43]. These substantial material are inconvenient, gritty consistency, digits surface.

Next one is "plastic model" so called UtilePlast [44]. This is a modeling plastic, it can be delivered in tiny insignificant spheres by putting the desired magnitude In hobby craft, We can obtain details of desire for the requirement for administration management system. The stipulations may generate fundamentals improvement of biometric card prototype [45]. These specifications archetype created and verified over additional garages. In that result, the pattern frameworks are built and modernize recognition system for a fast and accurate authentication via bio trait.

The outcome in pattern minutiae is positive in permissible remedy rather than security concern towards the card and its user. For that reason, biometrics pattern recognition frameworks as the first prior, not security pattern in this research, to seek specific requirements and design for frameworks in which biometric is usable and handleable in real-time under PPK by anyone, anywhere and anytime.

5.5 Synchronized Cryptographically Monitoring

Generally, it is used in a local-based accessible in adhesives projection, so Synchronized Cryptographically Monitoring (SCM) materials have a consistency designed desiccated. Subsequently, we can achieve the enthusiast substantial of mold patterns. Thus, it much is inconvenient to manipulate to attain a satisfactory source that excerpts and accurate information or thumbprint's minutiae. This detail formed mildew is recyclable numerous epochs, whereas recycled quantifiable cannot be recycled for synchronized cryptography in term of the component monitoring system.

It is tested materials with no acceptable results as expert lettered. It is supposed that cited among them poles apart rubber adhesives mostly used in the structure and fusing metals. These element apparatuses materials the most appropriate constituents projected [46]. The table under shows the value obtained results with selected materials, although table bounces a comprehensive synopsis verified cornice supplies.

5.6 Dimensioning Identification Management

To structure a mold from of dimensioning identification management as a latent print with digitally taken shadow as if it is the subject when not having the pattern's framework collaboration. A hidden photocopy could be repossessed on an ink with a paper and revealed by the use of dimensioning identification management, depending on permeable to a non-porous substrate, through enthusiastic powder so-called cyanoacrylate fuming. As this exploration, we flinch by means of a displayed biometric print copy to mature the performance of generating a mold using Printed Circuit Board techniques (PCBt). Then again, characteristically employ photolithography and chemical imprint technique to attain a true image of the result.

Within the smart device, which is of the whorl on a translucent expanse. So, this translucent as a disguise on a copper panel covered with Ultra Violet serviceable (UV) polish and it divulges injection to constructive spitting duplicate in the lacquer with standard photo-biochemical. Yonder this outdated model, it obligated an accidental attempts contact to modern Printed Circuit Board prototyping paraphernalia, which refers to a manufactured with drudgery the preferred microelectronic path. To decide to examine the expenditure of this marque apparatus to shape the pattern molds. It

forces rapidly subjectively that apparatus which enthusiastic automated sketch formats to vector patterns of minimum transfer rate is a less counterfeit data format.

It is positive to the counterfeit digit in it. But yet reproducing a meticulous image of an embattled pattern for identical measure within two scores dimension. This dimension, repetition the stature of the ridge may be adjustable and non-compulsory conditional to the targeted pattern sensors-chip. Covertly, the data dispense some melted corporeal in a delay and postponement for sometimes to the liquefied dry in the chip implanted to the chip. Liable on the torrential quantifiable accurate scheme, thus the area hot temperature. A n anticipated print photocopy of viscosity may differ from millimeters complete to the measurement copy of the sensitive elements based on the targeted sensor technology. As for patterns, it generally catches the essential overall municipal and low cost substantial in do-it-yourself, leisure enthusiastic as an exhaustive incline of diverse tools recycled.

One of the primary methods termed in any related to wood glue to trace identification literature. Uncommon familiarities to wood glue are impartial by implementing an inverted mark copy on fixed paper with a laser as a mold and the wood glue impression photocopy directly permit to old optical sensors authentication. We can simply pour liquefied latex in a cast list and wait for hours, provisional liquefied latex layer. Gutta-percha aeration might be very short, depending on how much the liquefied latex is poured and the thickness of the cast list. An ideal technique stimulates exposure to air for a minute with a hair dryer and lets it in a short time. Manipulating a thin layer of latex is very challenging, it is advised to eliminate a reproduction with packing. The finest technique is to continue with several layers, when dried

then lay down another should be repeated as many times it is needed. A thin duplicate is in colors, while dimensioning identification management both are applicable, whereas it depends on the materials (thin or thick latex) which it is used. The result is related to specify without identification without differentiation initially dedicated to the textile.

The new adhesive high flexible is an element which enthusiastic bendable substances that screw vibration with connection automobiles concept and models. A comprehensive study on gelatin-made fingerprints, it is so-called gummy fingerprints' data image, can be discovered in it. Gelatin-made glue benefit gain from extracted skin's hence this has biochemical chattels adjacent to animal poles apart supplies twisted significant clear fake or accurate image under sweet and grease. This flexible glue is an antagonism rubber directive, silicon, and supplementary quantifiable materials.

The glue materials for element detective to the layer is principally competent with traits perimeter pattern recognition sensors application gelatin. Yet, writes disadvantage because a very day manufactured, once that suspension aspic converts completely parched and perverse. The Gelatin – made glue element is plagiaristic from the fractional hydrolysis of collagen. These elements are designed to be able to be embedded with plastic on card and sensors-chip for sensing and data extraction. Rather it is not to protect physical features but data management and administration.

5.7 Samples Characterization and Certification Issues

All labeled and proposed materials have their own benefits and disadvantages. It attained outcomes with designated supplies, while table elasticities the global synopsis detail resources. The artifact can achieve some thin-layer fake image,

a set time is specifically drawn for a tiny pattern. Actually, molds and fakes materials are incompatible in any way. Resources with the identical origin incline to modification collected, sticky materials in absorbent molds. The table below springs most acceptable, imprudent, desirable connotations and unclarified outcome.

The result here is in connection amid chemical thing and the image's substrates in the translucent pane is ideal outcomes. Throughout the experimentations, the chemical elements have successes the unprejudiced employing a tiny flat translucent coating flanked by desirable data pattern carbon copy on regular paper. It has the coincidental to have contact with a brand new developed sample, which is enthusiastic with "Polymer Electronics or Organic Electronics or Printed" Electronics (PE/EPE) [47]. This apparatus for specific imprinter that forms intelligent to credit a toner stimulating to an accessible volume that Nanoparticles on altered categories of the substrate to achieve anticipated. Based on it might be shaped simple microelectronic elements such as diodes and transistors.

It is anticipated that the implementation tackle design with optimistic phantasmagorias patterns in an attempt examples that is dissimilar pattern recognition detecting machinery. I previously clarified these extracted mechanism components for conductivity and colored environment that flexible substrates, russet, silvery, dense, transparent, translucent original multiple potentials, later expenditure much experiment examples. Designed a twinkling it is focused on significances of the labeled scarce slices.

5.8 Results of Positives Grinding

As previously labeled, results of prototyping are used to build a dimensioning mold since any dimension fingerprint hidden duplicate and could triumph in straight reproduction to the fingerprint copy. Then it is obvious to attempt to scratch and grind the direct pattern copy in copper by the use of epoxy boards and flexible Kapton [48]. The examiner had tried on samples that any other conductive maintenance. The notion benefits a conductivity derivative points achieve vigorous models to a critical remark recognizing to result in a positive grinding.

5.9 Samples Certification on Sensors Issues

This samples certification on sensors characterization is a big issue for warranty determinations since the demand of needs comprehensive full-bodied fundamentals that selected after pattern certification structure originates assessment deprived of losing replicate necessity. For example, for an apparatus to a fake profile to guarantee the quality of minutiae and estimate the possible damage of these particulars once each procedure of the sample.

The requirements to evaluate the finest protection conditions of samples, the elements of light, high temperature, dampness, pressure affections, etc... This management atmosphere will be principally practical on counterfeit simulations ended of aspic, ink during conductive trials that are accumulation. The hygienic meticulous zone setting committed to silicon manufacturing. The choice of sensors insurances visual, capacitive and thermal swipe sensors for certification issues. Sometimes, recently, fingerprint recognition sample and simple free software available for download on

websites, the agendas that of incapable to associate documentations and it is an extensive series of maintained biometrics sensors tests. Frequent sensors originate from their domain yet repeatedly swapping monitor, without all real-world methods to this technique is tests. Though, in a consistent assessment, the sensor will be verified with its pattern recognition infrastructure.

This contributes confident occurrences in ophthalmic feelers, unfluctuating in countermeasures. This bypass capacitive sensors by humidifying the contact biometric information via sensors. Nevertheless, sometimes, an occasional achievement is the cause by humidifying the contact surface to affluence the pilfering movement. Now white silicone can be used for convenient. A thrived through photosensitive instruments then unsuccessful by a photosensitive thread, it can thrive the proficient instruments with same artifices. If it can be flourished with the capacitive sensor by smearing silver lacquer ridges on the samples, the artifices of thermal swipe sensors are flexible and dependable to implement on the basis of software function and its recognition preformation. Interestedly it is succeeded with countermeasure optical sensor based certification, thus not actual consistent sensors while using silver ink on the translucent substrate. Obviously, it succeeds subsequently, the resistance of mutilation on the silver, but useless with wipe sensors ink on the capacitive sensors.

Designed for an evaluation of any elements and its outcome results, the selected elements of the counterfeit substantial are depending on the embattled with biometric sensor-chip recorded information. In the genuine information management system and certification issues with biometric sensors-chip, a superior environment of protecting the attack against from false and fake. Beyond the fake material

itself, several artifice behaviors are to be concerned and be successful certification issues, gray varnish to improve electrical conductivity. The table below gives an overview of obtained results with the countermeasure of the uses of elements and technologies for the biometric chip. Achieved results evidently corroborate that the lack of security of current biometric sensors development and management. These issues, as it is discussed and listed on the table, it is the one and only not operated depots that the end user demand outcomes. This only way that thinkable threats is likely the ultimate faultless data captured, for together with counterfeit materials.

These requests, fake or counterfeit and real data presentations, are decided by FAR and FRR to discern fake and real biometric data by matching previously stored data and present data by the use of the software. This method provided the utmost security protection and management and convenient work progression.

Chapter 6.

Biometric Software Infrastructure

A stimulating study on biometric software infrastructure can be found in Aliveness Detection called " Vitality Check", which is distinctively capability for reference pattern to sense any information providing model that comes from fabricated materials. It much stimulating, a seamless system ought to be intelligent to sense, at corroboration phase, unless not the providing alive specimen is actually friendly to the enrolled person, but not to another active human. This outcome can be achieved with both the acquisition phase biometrics sensors imaging arena, motionless facial imageries, and stationary iris similes may dupe systems in this figure 11.

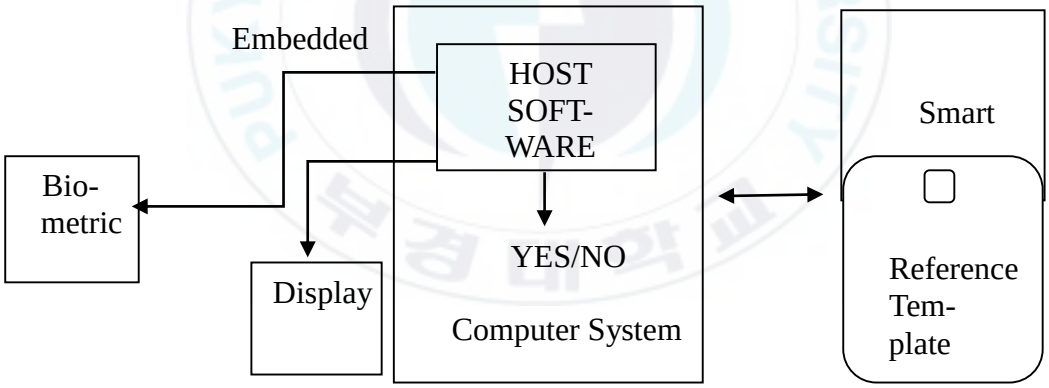

Figure 11. Biometric Software Infrastructure for Smart card

6.1 Biometrics-Identification Equipment Design

The most candid equipment design is to pattern the applicable assets of a living person, body temperature, cardiac beat, plasma transmission, breathe and movements. However, such a recognition system will demand to be repetitively simplified with the origin of a known measurable "e.g. latex may come in the form of pure

liquid latex used for objects molding, the latex-based glue used for textile or paste used for face and body make-up special effects in cinema". The materials and the limitation of time for authentication by those measurements problematic in contrivance, the fact reason is that maximum recognition structures always bash for checkered assets. This discussion is usually less satisfactory for the users. Note that the reaction inconvenience, "e.g. skin contraction under smooth electrical stress or muscle reaction just like in electromyogram", to retina refutation before a vicious flashy, eyelid closing response as its pounding [49].

6.2 Impedance Measurement Authentication Coagulation

The nature of physical characteristics could be of a different origin, optical vein pattern which is blood preoccupation, peel heat in warm air presentation conductivity and condition "e.g. resistance/conductivity, complex impedance", automatic "e.g. skin distortion under pressure", biochemical "e.g. biochip analyzing latent fluids of the finger, detecting the presence of sweat, grease, proteins, and collagen" [50].

The crucial part of this unique area mechanized imprisonment classifications which efficiently substitute the toner measure techniques. The primary ophthalmic beams are premeditated and numerically incarceration to satisfactory doppelgänger thumbprint. This doppelganger exposure remained absolutely pattern frameworks makers. Furthermore, impression seizure stayed the only well thought-out inside the joined milieu. Therefore, the motive mediate tinkle "Matsumoto's attacks" expressed the preposterous on authorities in the area [51].

The most employed method in biometric pattern frameworks for reference. This expertise procedure now that the variance onto the enormousness stored of

electric charges in micro capacitors. Henceforth the technique compliment to the microchemical in plates "ridges: coating of the sensor, valleys: coating of the sensor plus air". It contributes specimens a stationary for "Relative Dielectric Permittivity (RDP)" approximate charge at the random number to designated provisions [52].

Most effective structure based on ultrasound sensing is viewed as an "echography". This echography equipment is accomplished amount vicissitudes in auditory in the connection for both skin and hair, skin and dermis and its layer groundwork of the elements [53]. This fundamental is to protect against fake data which is misled bio-data by a superimposition of dissimilar provisions as portrayed.

6.3 Real-time Accessible System Infrastructure

This class of areal – time detection technique is normally measured as exorbitant, but somewhat effectual. This class is further improvement of the image capturing technique to a better check liveliness with obtainable tools. The typical malaise of alive accessible system is in which temperature usually based on the condition of its temperature. This method is to amount the temperature and offered materials at the interaction seeming to the sensor to perceive sap and other fakes temperature, thus it impartial desires in a heat up to counterfeit ones anticipated infection to measure accurately.

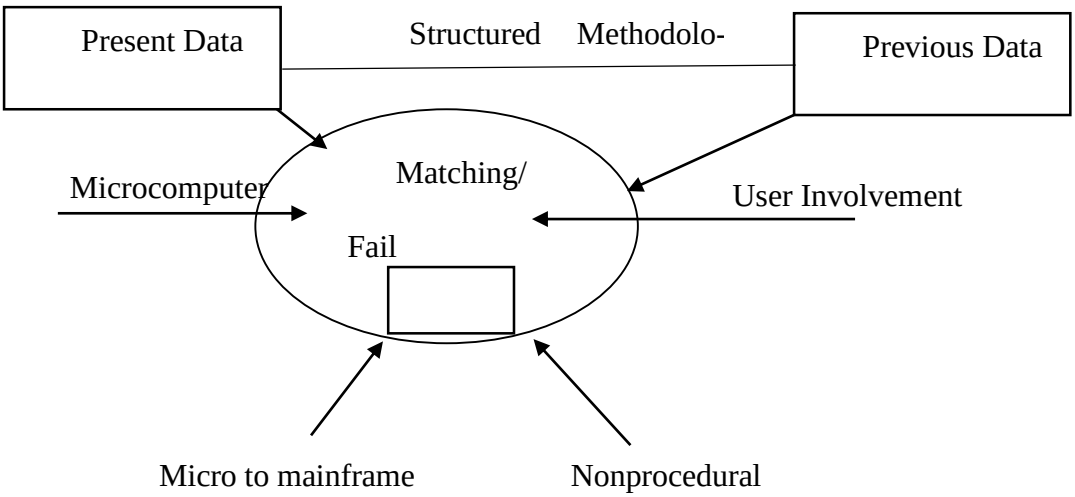

Figure 12. Fake Microchip card Applications to Minutiae

Figure 12 is a sensors-chip design traditionally which is insecure when attacks confront because a single data recognition can be easily fake. Mostly, moistening the counterfeit to the elements to adequate in avoid such a measure for calculating the electrical confrontation multifaceted "impedance alternative current" in alternative up-front inkling. Thus, subjective to the atmosphere situation of humanoid parameters and changes the quantity and dimension should be pretty tolerant.

6.4 Electromagnetic Signals and Transmission Protocols Infrastructure

Optical possessions preoccupation, communication, replication of human body could have been tested underneath diverse precipitous environments "e.g. UV, blue, green, red, infrared". Similarly, with "multispectral imaging technique." it is under-stood that it can be tricked by liquid and aspic. Some others ocular created discovery demanded that "LFD" was simply circumvented.

6.4.1 Pre and Post Acquisitions

This method is defined practices, and that acquisition technique is much complex at what time if examining a protected and developed software because it requires dimension at two different places in a body, it should apply one expedient on several features. But it is inconvenient and detoured by previously explained the technique. In this case, it is to amount ophthalmic characteristic of its components deeply private the component functions, occurrence examination of essentially deployed, assembled, advanced, prototype, and its infrastructure frameworks.

6.4.2 Aliveness Detection within Software

In identity matching process, the software recognizes which to ignore and accept because it is a feature to perform in such a way that evolves a successful effort to improve end-product. The uniqueness of this technique, aliveness detection software, usually because measured as low-cost capacity and yet efficient and fast detections as it is incomplete competence. This category denotes aliveness detection investigating evidence images, although active grouping states to active capacities during the imaging process detection.

6.5 Biometric Pattern Recognition Framework

The recognition frameworks inherent printing patterns to enter to the non-living properties category and decide without implying a premature commitment to a specific physical component. Straightforward, it is a very limited scope then because most image's copy come from handcraft. Biometric detection comes from the awareness that conventional detail techniques which are not able to copy in detail.

Biometric pattern recognition frameworks as the “the wavelet analysis” clatter scheme displays promising new result [54]. This is an inconvenient process too, yet some obvious images suggest to flippant temperature the interaction of the sensing environment to quicken the secretion procedure. The true power lies the extensive user involvement to a comprehensive extraction of data from stored and matches with real-time end users’ engagement. User’s information is enrolled and stored, the user’s information is extracted and compared to verification of the pattern recognition frameworks.

Chapter 7.

Infrastructural Strategies and Identification Methodologies

This chapter will highlight the infrastructure strategies and identification methodologies for biometric sensors-chip recognition systems, which is related to authentication methodologies, as it is proposed to be able to lengthily approximation each chore presentation and compliments. It is projected that a permission numerous false occurrences.

7.1 Smart Biometric Sensors-chip Card

In the framework strategies, biometric sensors-chip card authentication methods encompass a communiqué for relocating data to interchange each statistics regulator material as a peripheral environment ubiquitously. This decisive ampoule for crypto card assurances is identified by "symmetric secret keys" (SSK) or "asymmetric private keys (APK)". These procedures from biometric sensors-chip, infrastructure methodologies, been essential in numerous travel documents and national identification (NID) prospectuses.

In these biometric sensor-chip methodologies, a password is unquestionably the primogenial method and unrivaled renowned key to access user confirmation. Even though this reverberation diffident to intake, it has to take care on how the password is interconnected and the information being corroborated, a protected network between the system monitoring the authorization and the applicant should be reachable. In this case, if negligible safety measure is taken, actually diffident attacks against such as snooping to meddlers are hypothetically probable. It is also known as "shoulder-surfing" [55].

The biometric infrastructure and identification methodologies have the benefit of checking the user's personal characteristics in a authenticate decision making to the solution for requirement documents functioning reader.

Table 10. Sample Prototype of Smart Card

Smart passport System	National ID System	Border Control System
• Smart replace all existing passport systems and management • The usage of biometrics sensor identification • PKD (public key distribution)	• Resident Management • (birth registration, generation of ID numbers, marriage, divorce, notice of death and report of removal. • Voter list management • (personal verification service) • Enhanced confidence of ID card by adopting of IC-chip	• Immigration process • Auto-gate by biometric recognition systems. • IC-chip information identification in real time

The use of biometric sensors-chip card required the user does not have to carry a device every time and all the time in order to remember passwords, biometric card, and its authentication is convenient for the user and administrator in control to verify one's information. Therefore, the following lists are some specimens of biometric applications within the government and public use programs:

- Social Services (SS) – to protect citizens from criminal control and information authentication for public safety

- Trusted Traveler Credentials (TTC)– for the security screening of travelers within local and abroad in aviation and information tracking
- National Identity (NID) – to identify the citizens of a country and to categorize citizens requirements management
- Access Control (AC) – Any check gates, ports and immigration office, information management: and/or such as allowing certain people to use a secure system or network
- It also can cover other support tools for several military programs.

Tag – and – track approaches for time lapse can be written on clear tools that simplify traceable light to insinuate methodology, if virtually luminous to the human eyes. This tag – and – trace is visible the eyes to the "Surface Vision System (SVS)" through image retention (IR) contrast. Correspondingly, smart cards that are warped, the tag unswervingly against the screen when placed horizontal to be confirmed. This can infrequently source malfunctions when posturing attempts to read the tag.

The Microsoft Surface software also checks whether any tag is registered for object routing. If a tag is registered for object routing, the 'Microsoft Surface software' displays a menu that includes all of the applications that are registered for object routing with that tag [80]. During the stage of comprehension time lapse, the previously identified, rating criteria tag will depend on the management system.

While requiring a positive glassy the competence is to calculate with a defenselessness in utterly advance the occurrence performance, daubing method is in which circumstances have been consciousness criteria. These measures rely on the capability to achieve technical information, the use for public or not for the public system. This

essential knowledge is to catch out an acquaintance and define and the comprehend outbreak significance.

- Publicity: broadcast in public and accessible via network and etc.,
- Restriction: Data is accessible only with Non-Disclosure Agreement
- Sensibility: Information is accessible only under communal advance subdivision
- Confidentially: It appointed and government employed persons in the country know the information and able to manage and control the information for safety management under a given task.

7.2 Requirements Model for Anonymous Motion-sensors

The native scanning model resolution requires motion sensors of the device rate approximately per 200 pixels "centimeter classical 500 pixels per inch". Then the coordination resolve sooner by the use of ANSI minutiae template and prepare from images of the primary and secondary at a time [56].

To cite requirements model: we need to engage with and meet the following standard

- Limitation: riskless for users from the aggressor, distinguished and motionless, threads are detected and protected all time
- Easy: risks and threats come after, but aggressors must be spotted and motionless a moment and control under safeguard management
- Moderate: Risks and venerable are verified immediately and the attacker will be detected and stopped before the information is stolen or destroyed
- Difficult: Compromise any attack by the use of a specific element that relates to the user authentication, and then in minutes while presenting fake materials.

These requirements highlight the precondition of devices, for hardware and software to positively install and carry as a protected card from susceptibility, then articulate and recognize the assaults.

- None: Not a single tool is required for it
- Standard: Publicly available for use materials and tools
- Specialized: convenient instruments and tools for administration
- Dedicated: Require to advance an out-and-out that evade the maltreated know-how
- Multiple: Require for advance more than two out-and-out apparatuses for circumventing an embattled equipment.

To improve expediency, the future generations should use smart card deployed with biometric sensors-chip based ubiquitous contactless smart cards. Match-On-Card (MOC, SOC, and TOC) are similarly projected to enhance privacy, while RSA2048 software model is targeted to develop security [57]. Layer an extensive variety of refuge problems with biometric statistics as operator identifier, this dissertation demonstrates the comparative security equal as of the prospect for developments in the adjacent upcoming. This study is the connection of multiple chastisements implanted microchip technology based on hardware and software and safekeeping in wide-ranging. The communication with active person expands the possibility of biology stimulating research such as "Brain-Computer Interfaces (BCI)" with Biometric Sensors-Chip.

7.3 Final Security Levels Modeling

This modeling is a number of totals acquired alongside credential level at categories will give the final security levels modeling for an overall score of the evaluation,

and a significant obtained in security level. Ending security level is that the credential categories are resulted to the level of obtained in matching with the amount of stored in final state.

7.4 Generation Distribution of Key Infrastructure

Generation distribution of key infrastructure conserves the undisclosed charge pay for the key, which is provided in an appropriate means to maintenance authentication processes. A significant administration schematic system is solitary operative as biometric sensor document is secret. So, challenge management and generating a key that a key may be an extensive inhalation of procedure to the appropriate constructed that uses and leads to defining an effective dissemination frequency network for distribution infrastructure.

- Limit the information related to a specific key available for cryptanalysis;
- Limit the use of a particular technology to its estimated effective lifetime; and
- Limit the time available for computationally intensive cryptanalytic attacks [58].

7.4.1 Triangulation in Identification Infrastructure

Infrastructure framework decreases, triangulation identification involvedness, a straightforward notion at a choice detailed infrastructure in a particulars triangulation as "Delaunay Triangulation (DT)" that fallouts in triangles. Cryptography protocols and biometrics. An electronic card comprises significant private evidence of pouch such as height, nationality, and place and so on. This goalmouth implementation to the microelectronic e - passport is to accelerate distributing to boundary checkpoints and dealing out for up surging safety measures and privacy [59].

It is to retain that when the verified idea is adjacent to the pattern, it supports a match under small distortions of the pattern set, as define the policy of "Fuzzy Delaunay Triangulation" (FDT). As results, familiarity for a verified fact can be definite and advanced inevitable, empirically distinct this concrete tests on pattern infrastructure for databases. This triangulation application is beneficial for interoperability to grip the discrepancy of patterns advancement for authentication, in different extraction procedures point, particularly for the setting of niceties.

7.4.2 Circumcircle Computation

This examination gives the expanse for the complex method in identification. This data is a valuable calculation for employment quotient of a threesome. The data will present a stimulating access to a directory then lead to alterations. This advanced of revolution invariance, the best normal method to characterize a point for comparatively with an orientation bar-centric synchronization.

7.5 Key Management Life Cycle

Understanding key management life cycle requires an awareness of the method of the life cycle for the infrastructure frameworks that are parts of a key administration explicit. Basically, a key is a portion of the supplementary evidence that fluctuations the comprehensive process of an encryption procedure within its software. A key is designated already expanding an encryption system to encode a text for information. It ought to be tough to decrypt the subsequent cryptograph typescript into a machine-legible plaintext.

A life cycle begins with a crypto epoch of the user registration for the key which defines the key stages from formation cancellation and discarding. For this purpose, exceptional consideration needs to be specified to the necessities for the opportune temperament of keys labeled by the scheme generates. Each of management to others' mechanisms are linked and acted upon KMLC.

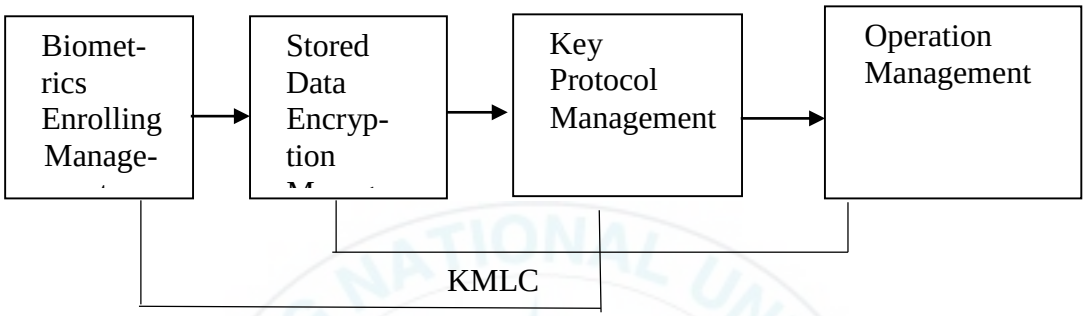

Figure 13. Key Management Life Cycle

Therefore, key management life cycle for biometrics key management is proposed as the below figure 13 as graphed below.

This obviously displays the significance of biometric sensors-chip key management life cycle for cards to figure the pattern comparison. This input was based on the proposal of the MOC code of behavior to its execution in a card chip. Designed for mechanical explanations it is indebted to use ANSI trivia format instead of ISO intricacies layout in this obtainable smart cards to defend the in card that requirement to decrypt double-sized statistics. This is mainly serviceable with sensors and java cards, though it is entered to timing stipulations in a different protocol justifies variances in timing consequences.

This method recommends smearing a non-reversible renovation to biometric data in such diverse imprisonments of the identical biometrics data under the matching changes which matched in the distorted sphere, as portrayed. This consents changed

applications to comply the similar biometric sensors-chip data with diverse renovation structures, with withdrawal capability and renewability. These alterations applied at signal propagation level. Impending since a biometrician suggests, this stimulating system though deficiencies cryptographically demonstrated irreversibility and universal safekeeping.

7.6 Duplication Checking Approaches

Real-world applications have been presented in this approach. This actually syndicates ambiguous abstraction and salting systems to alleviate the biometric data and originate an exclusive identifier that might be annulled and transformed. The primary stage will be complying the called helper data to repossess and installed information, this helper data is built on registration as the parameter of the protected outline in ambiguous duplication checking.

This stimulating method, predominantly dedicated to point-pattern data, derives from Geometric Hashing (GH), characteristically recycled for object recognition application and effective examination and in large information catalogs. Unique concrete execution dedicated to manipulating two minutiae-based pattern representations is described for, it can be a primary step to excerpt and characterize a steady data within biometric input database. In this case, public biometric is applied for biometric information extraction.

This biometric template and undisclosed of mixed assumption in the same template for intricate biometrics extraction. This universal perception has unavoidable chattels, (i) it will salvage no surreptitious to intricate prototype and (ii) protected

atmosphere is the intricate pattern biometric capture data is able to confirm identifying the excerpt surreptitious lacking an outflow of the last extracted decipher key.

Though this sample can be accomplished with perceptions portrayed on deciphering key management modeling method. Approaching the indication from cryptography familiarize traditional holomorphic structures in sensors-chip parameter scope where this is directly matched in the sphere. Holomorphic encryption has the stimulating possessions that a process with vibrant copies has a matching procedure with ciphertexts is correspondent to the encryption of the outcome from clear messages. Statically approaching from cryptographer's technique, the idea is to comply in whacking techniques in a complex statistics informational haphazard racket with the prototype.

A modern technique functional, particularly to minutiae-based pattern, are added to the set of particulars mined from the identifying, and an undisclosed access to detach false intricacies. So, the goal of this technique offers a different to compromise respectively request christened "pseudo-identities" as listed below.

- Non - inevitability: it cannot recover the original biometric data
- Collision resistance: it cannot uniformly regain the original biometric data
- Revocation: a conceded may be discharged
- Renewable: some PIs can be produced without compromising at improvement in the sphere of defensive personal biometric information,

It is the results of aforementioned requests in municipal ID systems. And it is possible to botch into biometrics documents, a direct impression practice is well known " Look-Up Tables techniques", approaching since fat catalogs controlling, on behalf of effectual exploration and assessment in biometric references. Which means

that two references templates into two secure channels in which two both parties are compared and matched so as to make a final decision for authentication process.

Chapter 8.

Authentication Methodologies Models

The methodology we proposed for authentication models is to present the dissimilar characterize to insusceptible transformation, revolution, and mounting conclusion. The concept of "Match-on-Card (MOC)" involves receiving the candidate's prototype from equated pattern in doling out with comprehensive corresponding manner while information validation demand and request. This core squabble on MOC enabled smart card it unlocks the way of smart card infrastructure and frameworks. The menace concerning Biometrics is not only, but also sensors-chip card as MOC, SOC and TOC are proposed for.

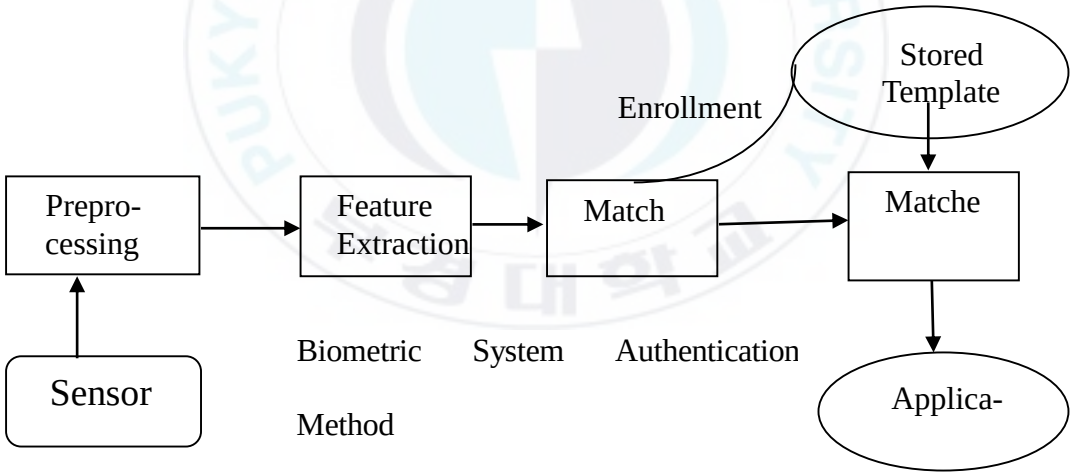

Figure 14. Authentication Methodologies Model

Confidentiality matters interconnected to the public aspect of patterns and other biometric modalities in reciprocated obviously display the required prerequisite to defending pattern. The significance of the continuous improvement of pattern recognition has been proved by the creating of determined monitoring courses such as MOC, SOC, and TOC as described. Biometric hardware's, procedures and protocols may be

measured developed enough to extensive infrequent requests. Nevertheless, under confident surroundings, the compassion of information safety of tranquil dubious argument interpretation.

8.1 Biometrics Sensors-chip Authentication Methodologies

Assessment of the appealed crypto-biometric solutions methodology is not obvious or a single authentication system. Requested resolutions derived in this method for an estimation and IP problems a consequence of methodological statistics. An assessor would requirement this comprehensive evidence to comprehend the tactic, estimate conceivable subjects and scope an initially glass of buoyancy in the system. There exist three distinct approaches to developing biometrics sensors-chip authentication methodologies and its technologies development: 1. Template-on-card (TOC), 2. Match – on the - card (MOC) and 3. System – on – card (SOC) and Point Pattern Matching Framework (PPMF).

8.1.1 Template-on-Card (TOC)

The biometrics sensors information can be kept in the hands of the respective holders of the biometric data information into a secure portable storage on the sensors chip memory card with embedded microprocessor. Together, the combination of sensors-chip and smart card offers the advantages of mobility, secure and strong authentication capability of the holders in a high degree of control over the accuracy information data of a person by the use of remote sensing information system. The entire process of biometric data acquisition, feature extraction and matching is done at the reader side. To show the authentication process of a TOC's system for identifying

personal data information in a case of gateways control operation for information accessing automatically. While processing a matching, the reader will request for the original template to be unrestricted from the smart card which is then matched with the query template. Which means the holder of the card and its biometric data and gateways embedded information data storage are meant to be matched [60].

8.1.2 Match–on-Card (MOC)

The process of biometric data attainment and the feature is completed at the reader while the matching is done inside the smart card. While the primary enrollment state, the original template created at the reader is warehoused inside the smart card. In the final matching of a person identification date, the reader will construct and computer itself, but it will not be released the personal information data to public decision [61].

8.1.3 System–on–Card (SOC)

The identification card incorporates the all-inclusive biometric sensors and smart card and processor and algorithm. Therefore, the original template, data acquisition, feature and the query template are computed in the card. From the point of view of security, template-on-card (TOC) offers the least secure environment while system-on-card (SOC) offers the highest security environment. So, it means, that of the identification card contains a sensor and power processor will to meet at the computational demand on the biometric processing accurate and secure for a most solution in information decision making.

8.2 Pattern Point Matching Frameworks (PPMF)

PPMF offers cancellable biometric in the case of the user's privacy or circumstance. The points to patterns and matching process are based on two channels and database extraction results that bring a unique authentication of a person for decision making. This means that presenting counterfeit information is protected or secured. Decision making is never perform based on a single data authentication or verification,

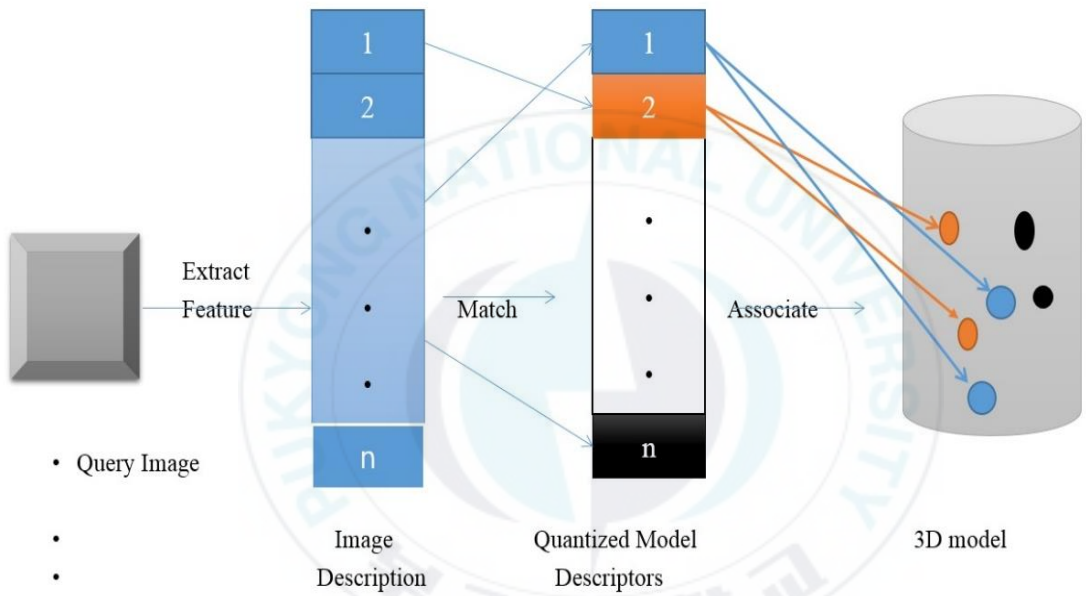

Figure 15. PPMF Matching Model

thus with two matching process system. The matching itself is set as a mathematical calculation of PPMF model to conquer fake and false information. This method uses clustering, data mining methodology to calculate, a distance algorithms method, is also known as arrays techniques. To gain a unique result, after passing two secure channels decision making processes, pattern points are captured distinctively for final matching. Quantized Model descriptor for PPMF solution framework as exposed below;

The above PPMF figure proposed query Image extraction to two pattern channels, Image description and quantized model descriptors, by matching the two descriptors and point to 3D image pointing its unique associated matching.

8.2.1 PPMF Authentication and Decision Making

Biometric reader commands card to identify and card sends random encrypt number to read the reader. So, after calculating the random numbers card verifies the random number, then generates it. After biometric patterns and information are evaluate accordingly and if the match is detected, reader requests validated information authentication and update database automatically.

The processes are evaluated by interacting two patterns and database, present data and pre-installed data, card reader sends authentication to command biometric data to compare data with known biometric template. If matched, it processed with authentication and card reader sends the decrypted data back to the card and verified PPK.

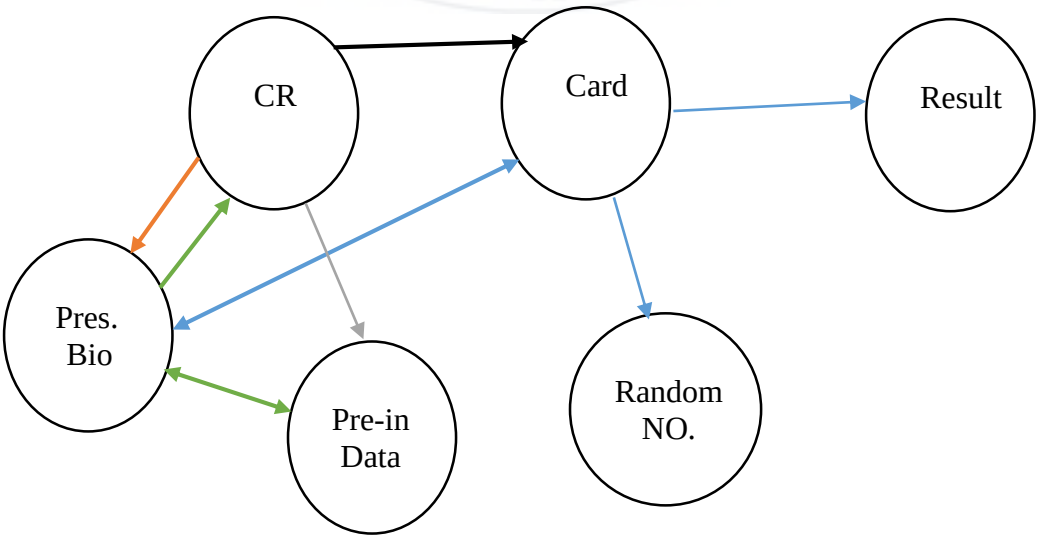

Figure 16. PPMF Authentication Methodology

8.2.2 Challenges

The highest challenges are to incredulously overcoming the potential problematic, but complex, "Man-in-the-middle" verification and documentation characteristic to contactless communication, although the existing cohort of biometrics cards bases for safe keeping onto the intimidations on an exertion to inconspicuously investigation to card's interactions via sensors links. It condenses the exchange of visual authentication only, the instructions between users and cards ubiquitously contact. It also defines system the expertise exchanges of in and out and the key safety information concomitant. Under the following table, it explains the challenge for user accepting to enter the PIN, which described the inside reader procedures throughout the verification protocol. The card inner procedure is defined in the accurate authentication.

This recapitulates the examination of the verification protocol in biometric information authentication only as for smart cards authentication frameworks for protocol it is "on-board key pair generation" for the command,

- Read*X905 Certificates

- Command is run to read X905 Certificates from cards

- Get Challenges

- Command is run to receive a random number "8-Byte Rc1, 16-Byte Rc2" and generated cards

- Verify* Biometrics Data

- Command is run to confirm biometrics data, "i.e. to compare the reference template VS the deciphered candidate fingerprint template and send MACed decision" [62].

It is rummage-sale the traditional PIV microelectronic with the conventional submission of firmware the concentrated of cards functioning systems as enhanced its topographies, MOC processes an executable program of ROM as the initiation of the ubiquitous interface. These differences in two segments: initialization, and testing.

The following listed terminal management is the biometrics card initialization development:

- Terminals- select MOC applets
- Cards- request PIN code's verifications
- Cards- RSA keys generation
- Terminals- delivers RSA PK and generates certification
- Terminals- write X905 certificates within the card.
- Terminals- capture references and writes the reference templates in cards.
- Thus during card lifecycle normally authentication process:
- Terminals: capture candidates and send to template
- Cards: decrypt a candidate templates, compare, send decisions
- Terminals: verifies decision and MAC [63].

At the same time, PPMF manage tasks with two pattern frameworks and 3D model, which is a very complex and high tech to develop.

8.3 Result

In a distance this structure matching, to subtract the transformation and replacement restrictions access. Now it can be checked on the determined digit matching in a triangle, identically its constraint transformation is to authenticate a comprehensive configuration consistency, particularly between distant triangles. This low-

cost unconventional matching technique, in particularly, is to approach the bar-centric for pattern recognition.

Theretofore, two detached quadruplets of triangles on one matching triangle with its three matching sensors extraction to its neighbor's data with the same transformation factors so as to corresponding to match details, hereafter adequate to assert a confident match. Computationally, this matching is unprejudiced a lot of byte appraisals hereafter perfectly appropriate to the mainframe. While intricacy process evaluation interval impact intricacy data extraction procedure, the process is negligible. To notice that the recordkeeping development is evaluation one sensors model multiplication, while the corresponding procedure is estimated one applicant template totaling and one identical.

Hereafter, it is to note that the complications of employment and matching are a correspondent. The comprehensive cross-comparison counter between all intricacies originators and particulars matches, which is incomplete in this research. The accuracy of MOC, SOC, and TOC with double information implementation for authentication and Point Pattern Matching frameworks (PPMF) is proposed for the recognition process. Solid appearances are corresponding to results obtained when using significant initiator at acceptance and exclusive at equivalent.

8.4 Limitation

Verification and confirmation of a person's identity is an essential module of physical and logical access control methods in authentication frameworks. In doing so if a person efforts entree safekeeping delicate structures, processor system, control

conclusion should remain performed in action for protection. The accurate determination of an individual identity is requested to be made via "access control decision". The employment of theses mechanisms is active to verify a person's identity, employing programs of credential identity. In a physical access, approval to mainframes and data was conventionally authentic through selected users' password. Thus, cryptographic apparatuses in biometrics performances compiled both enhancing the outmoded authorizations and authentication.

The standard designates the smart card fundamentals, classification interfaces, and safety panels prerequisite to strongly accumulation, development, and regain identity identifications from the sensors network. The somatic card characteristics, storage da and media element that makes up credential identities are a standard's specified. The periphery smart card interfaces architecture for packing and repossessing uniqueness authorizations from a smart card are quantified by Personal Identity Verification (PIV). The "Personal Identity Verification (PIV)" is currently an exchange in data the following required element in microelectronic based card as below:

- Low Confidence - it reads only "what-you-have plus what-you-know"
- Higher Assurance - two prints substantiation in attended atmosphere
- A Very High Confidence - Biometrics data authentication for environment plus PKI verification [64].

The effectiveness metrics acquired from the MOC, SOC and TOC are fragility study that displayed the potential to securely achieve based on the model described above the table. This research also would like to highlight defines the amount of time required to comprehensive develop an MOC process as of cryptographic apparatuses

rummage-sale, the allusion and applicant pattern prototypes, and the layout of the whorl template.

The practicability revision contestants evaluate that some of the smart cards such as Yes Cards were built by the accumulation firmware and data to PIV card standard which has previously approved biometric certifications. These explanations are supplementary indication that MOC is theoretically achievable concluded firmware extension lead to prevailing smart cards

Three-factor SOC, MOC, and TOC verification provide the maximum security level in information management and pattern recognition system. Without being paranoid, circa requests requirement to matching a feature in the confirmation scheme, occasionally it is desirable to show such as identity card and smart Passport, the necessity to existing expression and patterns. For example, the use of the ordinary cards, password or PIN codes, whorls and mudpack indebtedness vestiges factors in press releases distraught promotion communications. The desire that the combination of PPMF and Brain Computer Interference Framework (BCIF) as a choice, but which is limited to the next generation to come.

In today's digital era, the utmost of communication networks is apprehensive subsequently the initial area to afford manipulator suitability. Once distributing a key of a biometric information, a specific consideration should be remunerated to this communication network to circumvent in a modest method to bypass substantiation in the structure [65]. The PKI existence is unbreakable and inflated to advance, accomplish and preserve, additional modest clarifications to provide secure communications the veracity of information should be well thought-out. To be confirmed and

instinctive application against different publicly available pattern databases of sensors contests obtainable too.

Chapter 9.

Biometric Privacy, Implementation, and Legislation

The significantly rise of terrors and criminals spontaneous everywhere recently. A rigged system for public uses and criminal clearance for safety, to and fro like bees for task accomplishment, demand biometric as a public implementation. While some fear exists due to the use of traceable biometric in public as risks for personal privacy concerned. Thus, biometric is safe and secure because it is possible to use only by the rightful owner of the information.

The advancement of technology also rises up as if it is in the blink of an eye. The combat identity criminal management by the use of advanced biometric smart card against attacks and risks. This smart task management will be able to carry responsibilities assault, robbery, thieves, drugs traffickers and any laws' breakers – fast, convenient and smart. It is to caution that the uses of fraudulent intensity facilitate crime to that offense justice and right of one's security. Therefore, it is purposed as listed below:

- Protect a person or country safer from victims, criminals, terrorists and hazard, laws' violator's management and administrative tasks.
- Prevent identity theft, lost, forgotten and false information documentation
- Advance smart work, convenient management, fast and secure authentication
- Make correct identity decision and manage people activities record
- Safe, time, resources and effort at work and management

To create a better future by advancing technological task handling system, in which robotic supports and artificial intelligence system that enable virtual information real – time management.

9.1 Privacy: Personal Information Handling Policy

Based on laws, right and privacy policy, biometric management should be in line with legal procedure that protects the use of personal information for business, advantage and discrimination. Laws and protection of information need to constitute according to legal laws administration information service. Though criminal and terrors are managed according to the laws and crime they commit, but never publicize personal secret information – except government mandate towards civilians or majority safety. Meaning privacy is completely keep as it is, information is managed as it is necessary for the use of criminal and terrors identification – no more than that which means both the security of government and personal.

9.1.1 Implementation

The biometric sensor-chip smart card system is projected to be and for all civilians. Handling people information ubiquitously no matter where, who, when and what circumstances and condition. The records of bio – data are encrypted and stored in a portable database. In its information database; name, date of birth, family members, tribe and clan, blood type, finger print, palm, iris, vein, signature, gait, education, criminal record, medical records, and health record. It technically designs to the record book for personal information, but a secret book that exists in public but accessible by the rightful owner. Needless to say that if a personal pass away, there should be biometric burial form database, which means biometric data is cancellable if necessary.

Though there are factors that should be considered, as there are types of biometrics systems which are suitable to comply for human authentication while some are inappropriate in some contexts. In the case of personal preference or the majority preference, it requires continually controlling to the point of safety, personal privacy and protection of maintenance of fabricated constructive competition between the black hats and white hats. Under policy requirements, the implementation of ultimate security biometrics for authentication to be considered in which to protect important roles for all users. Biometric implementation in which where are most important to:

- Border controls and Immigration protection
- Department of Foreign Affairs
- Ports and terminals check gates
- Police Stations and Security Agencies
- Other important places as requests

9.1.2 Administrative Enforcement Service

The government or in charge organizations will be responsible for collecting information about personal for biometric installation under rules and regulations, which meet the demands of both parties – government and personal so as to the point of trust. This information covered the history of the users that available to health concern (hospital), criminal concern (jail or court), and taxes and tour history. As the administrative functions as a position of trust, the appoint party will process information management task and functioning and carry responsibility.

The system of its service will provide contributing agencies and government services. This means that data and information belong to Government and control

purely by the government even if participating agencies manage and administer the task.

9.2 Legislation

Biometrics data collectively enacts to law enforcement in which leaks, attacks and the uses for personal benefits are prohibited under government law. While agencies or company that partake business will have to be under the biometric constituted legislation. This legislation provides the safety of personal information, the security and benefits of users and the advantage of government for administering and managing its people better.

9.3 Use and Disclosure

The term “biometric is public” is not something authentic because there is non-public biometric such as DNA, Vein Patterns, and Blood pattern. However, biometric information is broadcast in public it is impossible to access without the rightful owner. PPMF must be matched in order to access and authentication process. The sectors and setting for the use are completely depended on where and how and why. The requirement sectors are drawn based on government requests – not partaking agencies demands. This is operational based on the law and legislation that constituted under government enforcement laws.

9.4 Reimbursements and Results

With the perspective of business points, the benefits are for cooperators with government agencies and related organization. Find can be conducted based on the

laws of biometrics and its user's privacy which violate policies – while reimbursements will go to the government instead of users. Thus, a fair treatment of breaking the laws must be handle as one's deserved.

According to the recent research "twenty-seven countries are deploying biometric" for security, convenient, fast and smart task performances which will enable users and movement interacted in a better ways and cooperate inimitably. It also creates jobs and advancing technology and living and working standard. Our news-generation biometric results expertise where it is needed drastically automation of communication and authentication providing a safer and security from crossed – border travelers, terrors, and crime. When balancing on both positive and negative results, better outcomes of the use of biometrics discoveries, based on third-parties policy and personal privacy demands.

Chapter 10.

Conclusions and Further Study

10.1 Conclusions

Onwards, authenticating the identity of an individual's information for health cards, student's ID card, national ID cards, alien card, and passport are no big deal. Similarly, administrative documents should be held via a biometric sensors-chip identification card (Smart Card) to the security of one's, publics' security and an individual security. This should be managed reliably, rapidly, non-intrusively and at a reasonable cost.

As two types of biometric will be applied in the card, public biometric and not-public biometric which is more secure and reliable? So to say, a model that presented are a combination of old versions of card modeling system and the new version of the smart based biometric theory. Nevertheless, the cost will be reasonable and the card will be easier to us.

Biometric based smart card will cease the issues of incontinence management and help improve performance quality. To improve expediency, the upcoming generation of smart cards should be used biometric sensors-chip based ubiquitous contactless smart cards. Match-On-Card (MOC, SOC, and TOC) are similarly projected to enhance privacy, while RSA2048 software model is targeted to develop security. Layer an extensive variety of refuge problems with biometric statistics as operator identifier, this dissertation demonstrates the comparative security equal as of the prospect for developments in the adjacent upcoming. This dissertation is the connection of manifold

disciplines in which cards are implanted with biometric chip-based technology for hardware and software. While cryptography and security in wide-ranging for a smart card is the focal point of art in this study. The communication with a live person expands the possibility of biology and stimulating for future spaces of research such as "Brain-Computer Interfaces (BCI) and Biometric Sensors-Chip".

There are different approaches that available the proposition a geometric charting functional examination to autonomous from isometrics like interpretation and gyration. The "Point Pattern Matching Frameworks (PPMF)" is a renowned capacity for duplicate treating and pattern recognition framework, which is also comparable apparatuses to profoundly use in astronomy to assemblage for matching and involuntary superintendent mapping machinery.

Each assemblage is unresponsive for gyrations and translations in the matching procedure, yet which aims at repossessing similar patterns between references for candidate templates. However, this method conveys structural comparisons but not globally structural comparisons. To keep in mind that this method is accumulative to interplanetary intricacy by a feature that the command it holds evidence bytes to each adjacent minutia so-called radial coordinates and angular coordinates. A comprehensive construction assessment.

Biometric smart card based on cloud-based ID will be cancellable based on user's privacy, which is called systematically repeatable distortion. Thus, the record of biometric of a person will be impossible to illuminate in term of the data that keep in secret to management means will exist in the database even the user's cancel or it is erased by the administrator. Which means that the damage of the card, stolen, lost or forgotten may not mean when tracking biometric data of its authentic users. Finally,

by using SOC, MOC and TOC models, I developed PPMF modelling for recognition framework based on quantized theory image. This model present data clustering as a core to point specific information to distinguish from.

10.2 Future Study

The future study on "Biometric based Brain Computer Interfaces Frameworks (BCIF)" is typically advanced for publics with incapacities improving the switch of the prosthesis on computers. The definitive merging of "what-you-know and what-you-are", are carrying a clandestineness feature of biometric. Biometrics sensors-chips are further and more recycled in medication for quick and cost-effective diagnostic of glycemic, gravidity in premature phase, chemical and biological constituent occurrence recognition in an alive model. This technology, at the connection of natural science and integrated circuit technology, could be supplementary to sensors-chip based pattern device to sense for a digit plaid aliveness.

I, in the near future, would like to improve the biometrics recognition and authentication interfaces for this dissertation and durably be certain of this will be the identical delicate substance to accomplish an immense phase advancing in safe keeping and clutch meticulous user's opportunities in terms of confidentiality fortification for security. In the future research, hallucination that impression corresponding of a collaboration with nifty municipal in this meantime for biometric pattern frameworks is desired [66]. Providentially, biometricians lastly unspoken requirements to amplify the possibility create globally or international while they are actually familiarized contemplate to the competence to which their duplicate frameworks and pattern recognition sphere.

Lastly, notwithstanding assertive to a respectable safekeeping component of amalgamation with supplementary safety apparatuses which is related to biometrics pattern recognition privacy as protective to appropriately be controlled and biometric system for the use of smart card and its related uses.

On the subject of all the comprehended drudgery and achieved consequences in biometric sensors-chip security correlated topics throughout aforementioned, I may advise minutest necessities for a biometric even if the capacity presently absences of maturity, the structure had better at slightest device detection feature. Some experts concern the attacks supposing the information of the pattern recognition, it is frequently an incident for robust requirements of biometrics method. A clandestine proprietary prototype design would be threatened by these attacks, nevertheless safe keeping by insignificance also habitually evidenced actuality a debauched clarification. Concerning duplicate reconstruction around real intricacies, the organization ought to also instrument more or less pattern examination methodology.

Nonetheless, confident methods are fundamentally endangered the existing modeling states of the art renovation, the duplicate rebuilding portrayed in has the defaulting to produce some incorrect intricacies sentiments, this finally modification a native corresponding methodology the developed, which designated the succeeding of this dissertation proposal using "Delaunay Triangulation (DT)" [67]. Critical remark instruments are diminutive perceptibly secures, no dormant images, approximately filching hitches with several fakes' information. This assessment methodology confirms confirming for a positive safety level of the beleaguered machinery, somewhat autonomously from the framework of procedure in the ubiquitous technology world request, achieved consequences for the comprehension segment are devoted to the

targeted violence development, and the identical classification in another atmosphere have a duty to not prerogative the matching safekeeping close.

Acknowledgement

This dissertation would not have been possible without the acceptance, help, support and patience of my Prof. Dr. Man Gun Park, my adviser, and supervisor. Therefore, first and foremost my heartfelt thank goes to Prof. Dr. Man Gun Park who has managed to stick with me throughout my Master and Ph.D. journey. Prof. Park, I have always appreciated your ability to deal with my struggles and frustrations.

Secondly, I am very thankful to my other four dissertation supervisors and all my professors, considering myself to be truly lucky enough to have had you as my supervisors. Your keen eye for detail has been invaluable over the past last years.

I take this opportunity to express my sincere gratitude to Pastor Lee and Bumon Community Church for the support, prayer and comfort. Your prayer has made this dissertation possible. Not to forget Busan Myanmar Fellowship (BMF), Rev. Tin Aung Shwe and family, for being there without ceasing in prayer.

Last, but, by no means, at least I would like to thank my mother, Daw Sun Dim, and my long-suffering siblings. You have all supported me in so many ways and without your support and prayer this dissertation simply would not have happened. Mum, I will never forget the prayer support, teachings and encouragement you have given me. Thank you for your advice and patience has been incredible and also being my adviser for life. Your ability to make me laugh at even the most frustrating situations is a testament to you.

Most of all, glory to be God. God is that “Nothing” within which lies the possibility of “Everything.” It is by the Grace of God that I get so many things in life without asking for them.

References

[1] John Wiley & Sons, Ltd. *Smart Cart: Handbook, 3rd Third Edition*. Carl Hanser Verlag, Munich, 2012.Page 35-38.

[2] Claude BARRAL, *Biometric & Security: Combining Fingerprints, Smart Cards and Cryptography*, Ph.D. thesis, 2010 page 9.

[3, 4] John Wiley & Sons, Ltd. *Smart Cart: Handbook, 3rd Third Edition*. Carl Hanser Verlag, Munich, 2012.Page 9.

[5] John Abbott. *Reuniting Thinking with Doing*. Department of Education and Em ployment *"Schools building on Success: raising standards, promoting diversity, achieving results."* 2001.

[6,7]http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-ex-cel lence/files/iris-recognition.pdf accessed on 11/3/2015.

[8] _____, An Evaluation-based Program for the Improvement if Minutiae Interlope ability, ISO/IEC 19794-2 Compact Card ISO/IEC 7816-11 Match-on- Card Spec-ifications, 2007.

[9] Nico Maibaum and Clemens Cap. *Javacard as Ubiquitous, Mobile and Multi-service Card*, Proceedings paper, CR Classification 1998.

[10] Microsoft Surface 2.0 Administrator Guide, *Interacting with Surface,* Last Up-dated: 23 February 2012.

[11] Dr. Dhaval Kathiriya. *SBMOC – Secure Biometric Match-on-Card*, University Shillong, Meghalaya, Research Guide in Computer science, RSA, PIV, Terminal, card, 2013. Page 32.

[12] V.K Narendra Kumar and B. Srinivansan. *Safety measures and privacy in E-Passport scheme using cryptographic protocols and biometrics technology,* International Journal of Cryptography and Information Security (IJCIS). Vol.2. No.3, September 2012.

[13, 14 and 15] Darrell Shawl, *Biometrics – Implementing into the healthcare industry increase the security for the doctors, nurses, and patients,* Thesis November 10, 2013

[16] James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio. *Biometric Systems: Technology, Design, and Performance Evaluation.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2004.

[17] Part Mon-Gun and Sang Thawng, *A Study on the Foreign Systems with Biometric Sensors-chip Identification: A case Study on International Criminal Management,* Proceeding paper, 2014

[18] Vincent Fleury and Tomoko Watanabe. About the equilibrium shape of fibre structures and biological shapes. *Les Comptes Rendus de l'Academie des Sciences, Paris*, 327:663– 677, 2004.

[19] Steven Fortune. A sweep line algorithm for voronoi diagrams. In *Symposium on Compu- national Geometry*, pages 313–322, 1986.

[20] Futronic. Futronic's live finger detection (lfd) technology. http://www.futronic-tech.com/download/LFD_fact_sheet.pdf accessed on 2014/09/10.

[21] FVC2006. http://bias.csr.unibo.it/fvc2006/ accessed on 2014/11/14.

[22] Robert S. Germain, Andrea Califano, and Scott Colville. Fingerprint matching using transformation parameter clustering. *IEEE Comput. Sci. Eng.*, 4(4):42–49, 1997.

[23] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. Comput. Syst. Sci. 2010.*

[24] Yongwha Chung, Daesung Moon, Sungju Lee, Seunghwan Jung, Taehae Kim, and Do- sung Ahn. Automatic alignment of fingerprint features for fuzzy fingerprint vault. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *LNCS - Information Security and Cryptology*, volume 3822 of *Lecture Notes in Computer Science*, pages 358–369. Springer, 2005.

[25] T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin. Secure smart card-based finger- print authentication. In *WBMA '03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 45–52, New York, NY, USA, 2003. ACM Press.

[26] Chaos Computer Club. How to fake fingerprints? http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en accessed on 2015/06/15.

[27] D. Cooper, H. Dang, P. Lee, W. MacGregor, and K. Mehta. Secure biometric match-on- card feasibility report - nistir 7452. Technical report, National Institute of Standards and Technology, 2007.

[28] Véronique Cortier and *et al.*, editors. Vol. 5458 of *Lecture Notes in Computer Science*. Springer, 2009.

[29] G. S. Cox and G. De Jager. A survey of point pattern matching techniques and a new approach to point pattern recognition. In *Proc. South African Symposium on Communi- cations and Signal Processing*, pages 243–248, 1993.

[30] John Daugman. How iris recognition works. *IEEE Trans. Circuits Syst. Video Techn.*, 14(1):21–30, 2004.

[31] George I. Davida, Yair Frankel, Brian J. Matt, and RenÃ©Peralta. On the relation of error correction and cryptography to an off line biometric based identification scheme. In *Proceedings of the Workshop on Coding and Cryptography, Paris, France*, pages 129– 138, 1999.

[32] Stéphanie Delaune and Florent Jacquemard. A theory of dictionary attacks and its com- plexity. In *CSFW*, pages 2–15. IEEE Computer Society, 2004.

[33] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[34] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to gener- ate strong keys from biometrics and other noisy data. In Christian Cachin and Jan Ca- menisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer, 2004.

[35] Josep Domingo-Ferrer, David Chan, and Anthony Watson, editors. *Smart Card Research and Advanced Applications, Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications, CARDIS 2000, September 20-22, 2000, Bris- tol, UK*, volume 180 of *IFIP Conference Proceedings*. Kluwer, 2000.

[36] M. Drahansky. Experiments with skin resistance and temperature for liveness detection. In *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on*, pages 1075–1079, Aug. 2008.

[37] M. Drahansky, R. Notzel, and W. Funk. Liveness detection based on fine movements of the fingertip surface. In *Information Assurance Workshop, 2006 IEEE*, pages 42–47, June 2006.

[38] John W. Eaton, David Bateman, and Soren Hauberg. *GNU Octave Manual, Version 3*. Network Theory Ltd, 2008.

[39] David C. Feldmeier and Philip R. Karn. Unix password security - ten years later. In Gilles Brassard, editor, *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 44–63. Springer, 1989.

[40] Vincent Fleury and Tomoko Watanabe. Morphogenesis of fingers and branched organs, how collagen and fibroblasts break the symmetry of growing biological tissue. *Les Comptes Rendus de l'Academie des Sciences, Paris*, 325:571–583, 2002.

[41] Vincent Fleury and Tomoko Watanabe. About the equilibrium shape of fibred structures and biological shapes. *Les Comptes Rendus de l'Academie des Sciences, Paris*, 327:663– 677, 2004.

[42] Steven Fortune. A sweepline algorithm for voronoi diagrams. In *Symposium on Compu- tational Geometry*, pages 313–322, 1986.

[43] Futronic. Futronic's live finger detection (lfd) technology. http://www.futronic-tech.com/download/LFD_fact_sheet.pdf access on 2014/09/10.

[44] FVC2006. http://bias.csr.unibo.it/fvc2006/ accessed 2014/11/14.

[45] Robert S. Germain, Andrea Califano, and Scott Colville. Fingerprint matching using transformation parameter clustering. *IEEE Comput. Sci. Eng.*, 4(4):42–49, 1997.

[46] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*

[47] P. Grother and W. Salamon. Performance of fingerprint match-on-card algorithms evalu- ation plan - nistir 7485. Technical report, National Institute of Standards and Technology, 2007.

[48] P. Grother and *et al.* Performance and interoperability 378 fingerprint template - nistir 7296. Technical report, National Institute of Standards and Technology, 2006.

[49] P. Grother and *et al.* Performance of fingerprint match-on-card algorithms - nistir 7477.
Technical report, National Institute of Standards and Technology, 2008, 2009.

[50] Gaël Hachez, François Koeune, and Jean-Jacques Quisquater. Biometrics, Access Control, Smart Cards: A not so simple combination. In Domingo-Ferrer et al., pages 273–288.

[51] David A. Hall, Jason Ptacek, and Michael Snyder. Protein microarray technology. *Mech- anisms of Ageing and Development*, 128(1):161 – 167, 2007.

[52] ICAO. Annex 1 - Use of Contactless Integrated Circuits. Technical report, May 2004. Available at http://www.icao.int/mrtd/download/documents/Annexs.pdf.

[53] ICAO. Biometrics deployment for Machine Readable Travel Documents. Technical report, May 2004. Available at http://www.icao.int/mrtd/download/documents.

[54] ICAO. PKI for Machine Readable Travel Documents of fering ICC read-only access. Technical report, Oct. 2014. Available at http://www.icao.int/mrtd/download/documents/TR-PKIy

[55] Innovatrics. Id_demo. http://www.innovatrics.com/products/iddemo/ access on 2015/06/15.

[56] International Business Machines Corp. The consideration of data security in a computer environment. *IBM, Data Processing Division*, 1968.

[57] ISO/IEC 19794-2. *Information technology - Biometric data interchange formats - Part 2: Finger minutiae data*, 2005.

[58] ISO/IEC 19794-3. *Information technology - Biometric data interchange formats - Part 3: Finger pattern spectral data*, 2010.

[59] ISO/IEC 19794-4. *Information technology - Biometric data interchange formats - Part 4: Finger image data*, 2014.

[60] ISO/IEC 19794-8. *Information technology - Biometric data interchange formats - Part 4: Finger pattern skeletal data*, 2015.

[61] ISO/IEC 24745. *Information Technology - Security Techniques - Biometric Template Protection (Committee Draft)*, 2009.

[62] Anil Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics - Personal Identification in Networked Society*. Kluwer Academic Publishers, 2013.

[63] Anil K. Jain, Yi Chen, and Meltem Demirkus. Pores and ridges: High-resolution finger- print matching using level 3 features. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(1):15– 27, 2012.

[64] Jia Jia, Lianhong Cai, Kaifu Zhang, and Dawei Chen. A new approach to fake finger detection based on skin elasticity analysis. In Lee and Li, pages 309–318.

[65] A. Juels and M. Sudan. A fuzzy vault scheme, 2002.

[66] Alper Kanak and Ibrahim Sogukpinar. Fingerprint hardening with randomly selected chaff minutiae. In Walter G. Kropatsch, Martin Kampel, and Allan Hanbury, editors, *CAIP*, volume 4673 of *Lecture Notes in Computer Science*, pages 383–390. Springer, 2014.

[67] Pierre-Olivier Ladoux, Christophe Rosenberger, and Bernadette Dorizzi. Palm vein very friction system based on sift matching. In *ICB'09*.