uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Wei Han

AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.Sc. (Systems Science)

GRADE / DEGREE

Department of Systems Science

FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

An Integrated and Distributed Biometric-based User Authentication Architecture

TITRE DE LA THÈSE / TITLE OF THESIS

Dr. Tet Yeap

DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Dr. Ahmed Karmouch

Dr. Jiying Zhao

Gary W. Slater

Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

An Integrated and Distributed Biometric-based User Authentication Architecture

Wei Han

Thesis Submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for the MSc degree in Systems Science

Department of Systems Science
University of Ottawa

Your file Votre référence
ISBN: 978-0-494-49209-3
Our file Notre référence
ISBN: 978-0-494-49209-3

Abstract

Biometric authentication systems are used to guide the system security for many years in the computer world and make the user's identification easier and more convenient. Meanwhile, the systems encounter lots of challenges, attacks and threats, privacy protection and system management requirements, which affect the user's acceptance. Differing from the commonly used solutions, in this thesis the approach is to modify the system to meet these requirements, which results in a distributed architecture which can be composed in real time, and resolves the above challenges in one solution. A system prototype based on the proposed system architecture is designed as a sample for the reference of other system designers.

Acknowledgements

Here, I would like to thank the following people:

1) Professor Tet Hin Yeap, who gave me a lot of advice and supervised me in finishing my thesis and related research. I learned some thinking methods from him that are important for me to solve the problems I will encounter in the future.
2) My parents, who supported me to continue my studies, encouraged me and made a lot of sacrifices for me.
3) My wife, Dan, who makes my world complete and lets me know my responsibilities.
4) My friends and lab mates.

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Problem background and motivation

Security has been the objective of much more concern in the recent years in the computer world. The authentication system is treated as the base of the security of an application system, such as when a user logs into a web mail system. Therefore, keeping an authentication system working properly and identifying users correctly is an important and inevitable part of system security. Using biometrics, that is, the unique character of a person, for identification is the most convenient among all authentication methods. Biometric authentication is the natural way to recognize who the entity is, and it does not need to be remembered and stored, which may involve other kinds of security problems. Until now, lots of biometric methods have been developed and used in various systems: accessing control systems, banking systems and computer login systems. In some countries, biometric systems play a pivotal role guiding the nation's security. However, biometric authentication systems face a series of challenges that affect the application of biometric authentication systems in network environments. These challenges include the accuracy of the authentication, threats and attacks, privacy protection, and management of the biometric authentication systems. Although some methods have been developed to solve these challenges, they cannot face all challenges.

Do we have a solution that can fix the problems simultaneously? To answer this

question, an analysis of the current solutions should be conducted. This thesis contains this analysis and discusses the possibility of a solution with a new-layered architecture. A new architecture is proposed in this thesis, in which all components are independent and need to be authenticated before it can be treated as a part of a biometric authentication system. The components are connected with communication channels that are protected by dynamic keys. The new architecture reforms the structure of the system, rebuilds the system layers, and defines new operations derived from the new structure, with which the new system architecture has better performance in several aspects. The new architecture also gives a possible systemic solution that can solve challenges simultaneously. After representing the new system architecture, the thesis designs a token-based system according to the proposed architecture. The design also reveals the general principles that are applied in other biometric systems based on the new architecture, including the components definition, protocol design, and the transaction disposal. The proposed token-based system is compared with the current solutions by scoring a set of aspects that can be classified into three categories: system security, privacy protection, and system usability. The score indicates the solution performance, with the higher score representing better behavior.

1.2 Contributions in this thesis

The main contributions contained in this thesis are:

a) Summarized the challenges and the methods that can enhance biometric

authentication;

b) Revealed the vulnerability of the traditional biometric authentication architectures;

c) Proposed a new biometric authentication architecture that is the systemic solution for the challenges; and

d) Proposed a token-based biometric authentication system.

1.3 The structure of this thesis

The later chapters in this thesis are organized according to the following structure. Chapter 2 introduces fundamental information on authentication and biometrics. The introduction on authentication includes the purpose of authentication, the factors of authentication technology, and the commonly used techniques. The later part of this chapter is an introduction on biometrics that contains the definition and developed biometric methods. It summarizes the challenges and current solutions and points out the possible methods to resolve the challenges.

Chapter 3 summarizes and compares the current used biometric authentication architectures – centralized architecture and distributed architecture. The second section in this chapter analyses the vulnerabilities of the traditional architectures in the security, privacy, and usability aspects. The vulnerabilities

analysis reveals the requirements for the new architecture.

Chapter 4 proposes a new architecture for biometric authentication applications. This chapter introduces the reformation of the system layers, the new operation in the new architecture, the communications among the system components, and the modified authentication process.

Chapter 5 describes the enhancement of the proposed architecture in different aspects and compares the system based on the proposed architecture with other commonly used and newly developed systems. All of the performance items to be compared and scored are classified into three categories to measure the behaviors in different aspects. Each candidate system has a score for a category that indicates the system quality in this aspect; as well, the total score is the representation of the system synthesis quality.

Chapter 6 introduces a design of a system based on the proposed architecture that uses a token to carry the biometric components. The design involves the component deployment, component function definition, protocol design, and authentication process control. This system design can be a sample and is adapted according to different environments.

Chapter 7 gives the conclusion on the proposed architecture and the designed

system, as well as suggested future work.

Chapter 2: Authentication and Biometrics

2.1 Introduction to authentication

Authentication is the action that confirms an entity or a process by which identity of an entity is established [1]. Credentials owned by the proven entity are used to prove the identity, such as a passport, a password to your mailbox, or the signature on your credit card. Another definition from Bishop, "authentication is the binding of an identity to a subject" [2], gives a narrow interpretation of the word "authentication" for the domain of computer security, which the thesis is focusing on. The entity is regarded as an authentic one when the presented proof or credential is valid and sufficient to prove the identity the entity claimed to be.

2.1.1 Authentication factors

The credential information represented by the entity that invokes the authentication requests comes from one or more of the following three authentication factors [3]:

Knowledge – what the entity knows, such as passwords.

Possession – what the entity has, such as the credit cards

Biometrics – what the entity is, such as the fingerprint or the DNA code

If the information originates from only one of the factor listed above, the authentication method is called single factor authentication. That is opposite to the

multi-factor authentication, which involves more than one factor in the authentication process. Contrary to multi-factor authentication, single factor authentication is easy to perform but has less security. The most common multi-factor application is the ATM (automatic teller machine), where the user withdraws cash only if the card and input password are correct.

2.1.2 Authentication and authorization

Authentication does not determine which entity can obtain the access to a resource or whether a person has permission to a certain resource. Authorization is a process of finding out the relationship between the resource and authentic identities [1]. It binds the resources with an identity after it is authenticated. In any security system, there are three mandatory steps:

Credential acquisition: The action that collects the credentials from user who is requested for the service

Authentication: The process that tries to bind the user and the identity he claimed

Authorization: The process that allocates the resource to an authenticated entity.

The object of the authentication system is to identify the entity correctly and avoid failures as much as possible. There are two possible authentication failures, acceptance failure and rejection failure. In the first situation, the authentication system fails to authenticate an entity when the credential is not correct. In second, rejection of an

entity that represents correct and sufficient proof is called rejection failure. Failure to correct the authenticate user causes misuse of the system resources and inconvenience to the users.

2.2 Authentication methods and protocols

Authentication can be achieved using lots of methods. Selecting an authentication depending on the application environment is the crucial work in system design. The protocols that convey the information in the authentication process may be involved in some methods. A well-designed authentication protocol provides the system with high security and convenience.

2.2.1 Password authentication

Password authentication has been the most widely used authentication form for tens of years in information systems. In this authentication method, a password needs to be typed into the system.

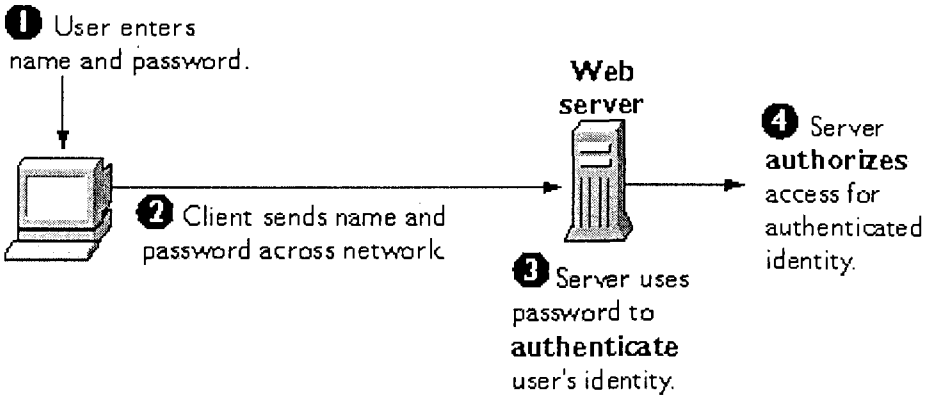

Figure 2.1: Password authentication

The figure 2.1[5] shows the steps using passwords to authenticate a user to a server.

1. The client displays a user interface that asks for the user's name and password for accessing the server.

2. The client sends the user name and associated password to the server, either in the clear or over an encrypted connection.

3. The server checks the name and password in its local reference database and, if they match, accepts them as evidence authenticating the user's identity.

4. The server determines what kinds of resources the identified user is permitted to access and then it refers the authorization process.

Since the password is normally simple and does not occupy lots of system resources, the password authentication is cost-efficient and easy to apply. But it is apparent that a system protected by password authentication is not secure. The obvious vulnerabilities are [4]:

Low strength – password may be easy to guess

Unsafe recording – writing the password down and placing it in a high visible area

Easy to be disclosed – discovering passwords by eavesdropping or even social engineering

2.2.2 Public-key cryptography authentication

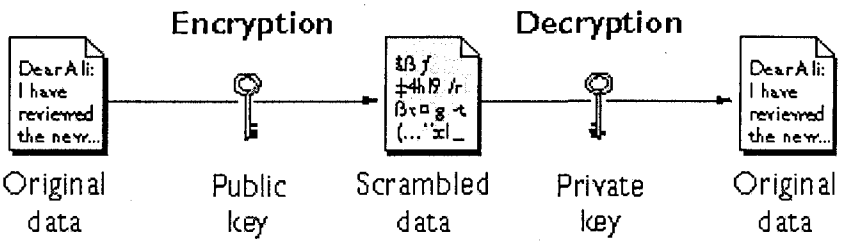

Figure 2.2: Public-key cryptograph

Compared to the password-based authentication, public-key cryptography authentication is a safe and strong authentication method that also provides authentication ability for entities on both sides of a connection. In figure 2.2[5], public-key cryptography makes use of a pair of keys, a public key and a private key that are generated from an extremely complex mathematical equation [4]. Each key can be used to encrypt a message and to decrypt the cipher message encrypted by the other part of the key pair.

2.2.3 Certificated-based authentication

Certificates are electronic documents that associate an identity with a cryptographic key to identify an entity. An X.509 (a specification on certificate

contents) certificate binds a distinguished name that identifies an entity uniquely with a public key. Certificate authorities (CAs) are the organizations or entities that validate identities and issue certificates.

Several types of certificates are widely used in authentication systems: Client SSL certificates, Server SSL certificates, S/MIME certificates, Object-signing certificates and CA certificates [5].

2.3 Biometric authentication

2.3.1 Definition

The term biometric indicates "statistical analysis of biological observations and phenomena" [6] and is adopted in other disciplines. In the computer security domain, the definition of the word "biometric," or the more precise terminology, "biometric authentication", is given by Wayman as follows:

"The automatic identification or identity verification of an individual based on physiological and behavioral characteristics." [7]

2.3.2 History and applications

There are lots of events and documents to specify that the application of biometric authentication existed for hundreds of years. In the Babylonian era, hand imprints

were used to "prove the authenticity of certain engravings and works" [8], which was re-found in 1823 by Jan Evangelista Purkinje [8], who noticed that hand patterns are unique. And now biometric systems are used more frequently and widely. According to Frost & Sullivan's report, the global revenues for biometric systems in 1998 were about US$113 million. This amount breaks down into the following application areas: physical access control (52.8%), law enforcement (12.9%), healthcare (10.2%), banking (8.3%), immigration (4.9%), computer security (4.1%), welfare (4.1%), telecommunications (2.7%) [9]. In 2003, the revenues reached $1 billion according the market report from the International Biometric Groups [10].

2.3.3 Biometric authentication

Biometric authentication is mainly high interested due to the two important reasons: the requirement on the security and use convenience. The biometrics is the natural unique and irrevocable identity of an individual and doesn't need to remember and record. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. The biometric characteristic can be used for authentication purpose as long as it satisfies the following measurements [11]: *Universality, Distinctiveness, Permanence and Collectability.* Additionally, in a practical biometric authentication system, the aspects of *Performance, Accessibility and Circumvention* have to be considered.

2.3.4 Advantages and disadvantages

The primary advantage of biometric authentication methods over other methods of user authentication is that "they really do what they should do" [12]. Different from the knowledge-based and possession-based authentication methods, the biometric-based authentication methods identify the user directly using real human characteristics that are not easy to copy, steal, forget, and forge to identify a person. Another advantage of biometric authentication systems is their convenience of use. Biometrics is natural for a user, does not need to remember it.

But some disadvantages cause people to use passwords instead of biometrics. First of all, also the biggest challenge of biometric authentication, the performance is not perfect what is measured by the accuracy. Since all biometric methods known and used today are non-deterministic approaches, unlike passwords, biometric authentication failures may occur. Biometric systems with high accuracy that have low FRR (false rejection rates) and low FAR (false acceptance rates) are still very rare.

Another major disadvantage is the source of biometrics, in which some persons are unable to provide their biometrics. The FTE (failure to enroll) rate measures the applicability of a specified biometric.

Additionally, for the biometric authentication applications, the cost is higher than using a password or token due to the more complex hardware, such as the sensor

capturing the biometric samples.

The ultimate goal of any biometric user authentication is to adopt the concepts for natural recognition or authentication of subjects, find techniques to automate this process, and implement these techniques in such way that a minimum of authentication errors occurs [3]. Therefore, these main disadvantages should be overcome before the biometric authentication systems are used widely.

2.3.5 Biometric authentication general model

Despite detailed techniques, biometric authentication can be depicted in a general model that is constituted by two modes and five processes and shown in figure 2.3[13].

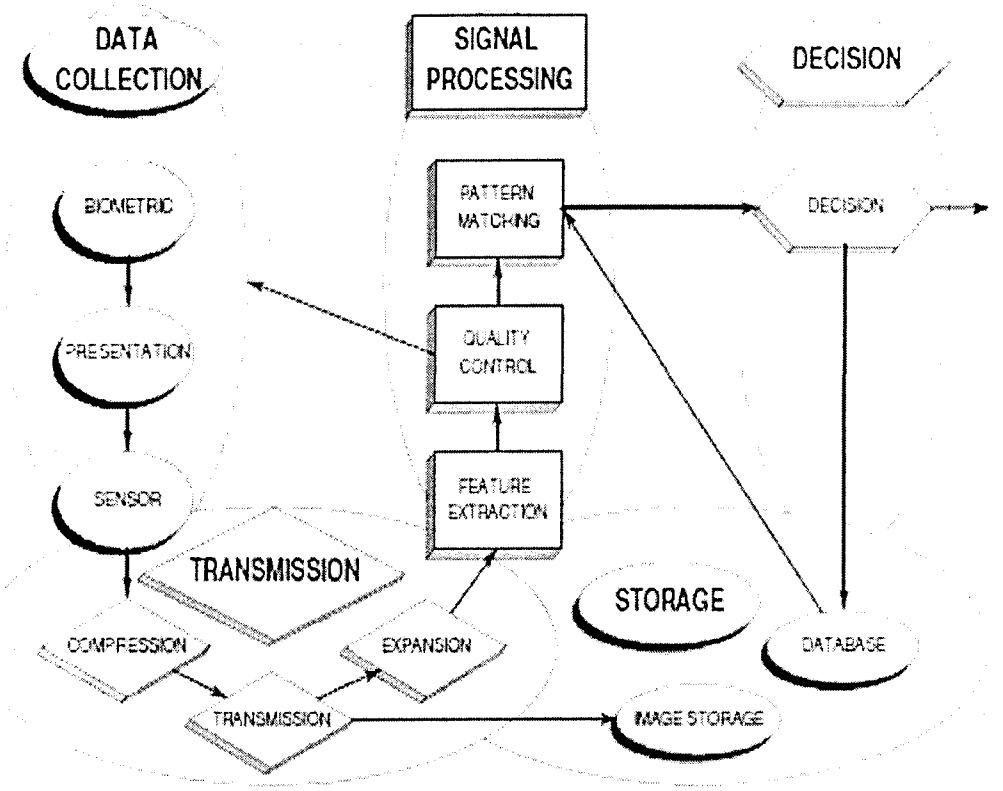

Figure 2.3: General model of biometric authentication

Data acquisition: In both modes of the system, the biometric samples have to be captured by the system sensor.

Pre-processing: It is a transformation from the raw biometric data to the digital data that are ready for the further processing.

Feature extractor: The process that encodes the characteristics or features on which the authentication system will operate.

Template generation: A template is "a small file derived from the distinctive features of a user's biometric data" [14]. It is the user's representation and is the

most critical data in the biometric authentication system. The process composes a template for the incoming biometric sample and saves it in the database.

Matching: A process occurs only in the authentication mode. It compares the extracted features with the stored templates and makes the decision of the authentication.

The two modes are the enrollment mode and the authentication mode. In the enrollment mode, figure 2.4[3], the templates that contain the biometric features are generated and saved in the database controlled by the authentication server. The system obtains the reference to a user and makes it ready to authenticate the enrolled user.

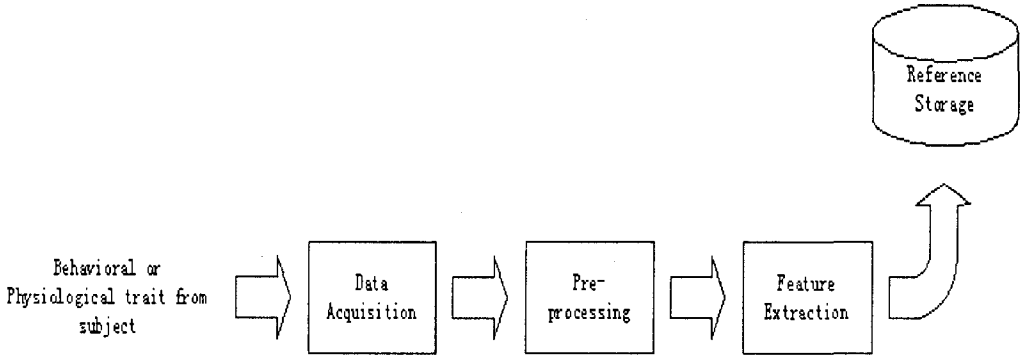

Figure 2.4: General model of enrollment mode

Contrary to the enrollment mode, the authentication mode in figure 2.5[3] identifies the user according the stored reference information formed by the templates in the database. The processes in the authentication mode are similar to those in the enrollment mode except that the template generation in the enrollment mode is instead with the matching process in the authentication mode. There are two functions in the

authentication mode – verification and identification. Verification refers to the process of verifying whether the biometric features from the user are similar to a template of the claimed person. Identification is the process that finds out to whom the biometric features belong.

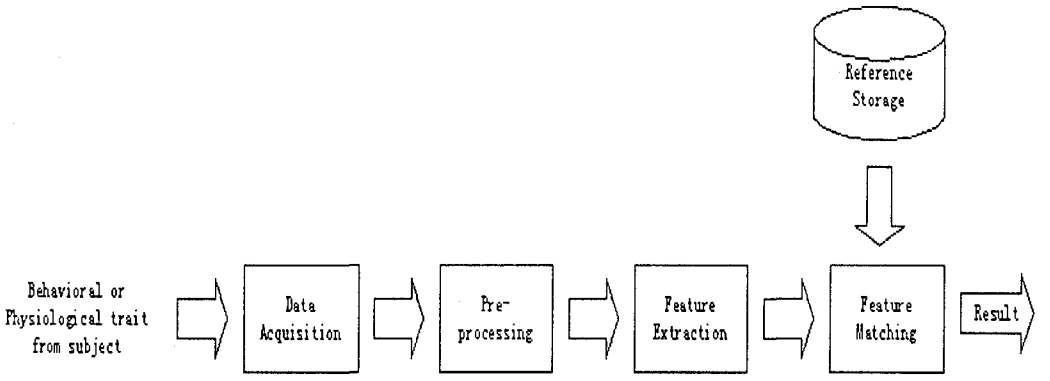

Figure 2.5: General model of authentication mode

2.4 Biometric authentication methods

According to the definition, biometric authentication methods can be divided into two classes – behavioral-base authentication methods and physiological-based authentication methods. The figure 2.6[10] depicts the market situation about the biometric methods used in applications. The physiological-based biometric methods, especially the fingerprint, are dominant in the market.

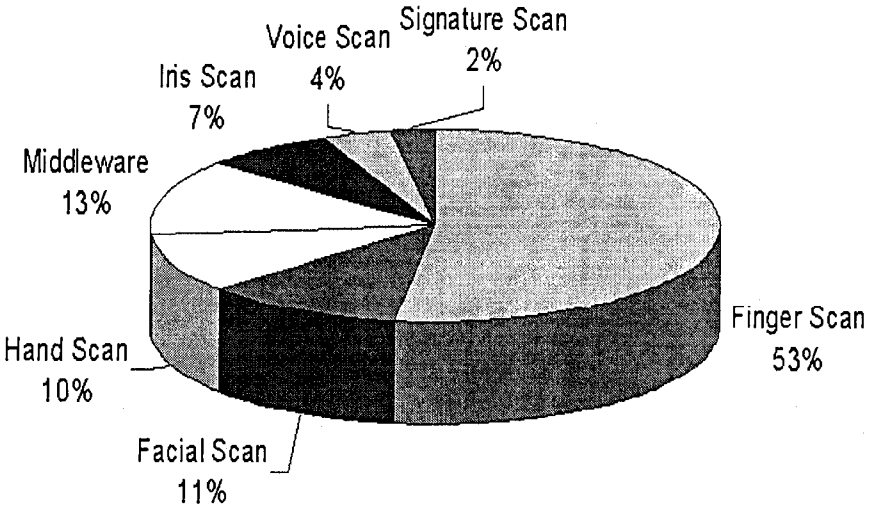

Figure 2.6: Market of biometric methods

2.4.1 Behavioral-based authentication methods

Behavioral-base authentication methods perform the identification by recognizing the person's behavioral patterns such as the signatures and keystroke customers. The behavioral characteristics are difficult to deal with and are easily influenced by the environment, which results in the high error rate to these authentication methods. But the behavioral characteristics are active biometric features that are captured easily. The major behavioral-base authentication methods are as follows:

Signature

It is a traditional and commonly used method in the world to identify persons by their distinctive writing style that is measured in the "shape, speed, stroke, pen pressure and timing information" of the signature signing [15]. The sample is when

you shop by the credit card and sign your name on the bill.

Keystroke

It is a new technique to identify persons by their different typing patterns. The authentication method can be combined with password authentication, which requires user type in a series of letters to improve the security. The user is authentic only when the user gives a correct password and proves that he or she is the typing customer associated with the password owner. The keystroke authentication method is also cost-efficient because no more hardware should be added into the system.

Voice

The voice authentication is based on a person's unique "dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the human body" [32] that identify that person. Research on speech processing and recognition has been taken for decades.

Gait

Gait authentication is quite new in biometric authentication. It is based on the pressure and duration of the interaction between a person's feet.

2.4.2 Physiological-based authentication methods

The physiological-based authentication methods verify a person by his or her

physiological characteristics, such as fingerprints, DNA code, or facial features. Physiological traits are natural and more stable than behavioral characteristics. As a consequence, physiological-based authentication methods produce much more accurate results than those from behavioral-base methods. It is also the reason why they take the main market share. But physiological-based authentication methods are passive methods, and the sensor cannot capture the traits actively. Some of these methods may harm the person who provides the biometrics.

Fingerprint

Fingerprint is used for personal identification for a long time [29], and most biometric authentication systems are based on the fingerprint pattern shapes that are created by the ridgelines. Fingerprint shapes can be divided into several types. The fingerprint is the most popular applied biometric technique that takes more than 50% of the market share due to its advantages:

1) This method has been vigorously tested and has high accuracy compared to most of the other biometric methods.
2) This biometric authentication method adapts to application environments because of its easy usage.

Nevertheless, some weaknesses prevent the many applications from using fingerprint authentication. The high FTE rate and the sensor limitation make some people unsuitable for this authentication method. Another social problem, privacy

protection, decreases the acceptance of this method.

Palm print

This authentication uses similar principles to those in the fingerprint method in the analysis of the palm to identify an individual. It needs much larger scanning equipment than the fingerprint authentication method.

Facial

This method recognizes the person by their facial features. The facial authentication method has some drawbacks. The authentication accuracy is lower than the fingerprint method; the biometric sample is influenced by the environment, the user's motion, and the position, which involve much noise and make the process difficult.

Iris

This technique is based on the individual's iris pattern, which is different from other people. The iris pattern provides more information and more stability over the person's lifetime; thus the authentication method is perfect for identifying an individual and has high accuracy. The challenge in this technique is data acquisition. It is difficult to operate the capture devices, and this method makes user uncomfortable, which leads to low acceptance and fewer applications.

Retina

This technique, based on the features of an individual's retina, is rarely used. Although it provides high accuracy, the difficult usage and discomfort make the application rare except in government and military facilities.

Other biometric authentication methods, such as ear geometry, body odour, facial thermographics, and hand-vein pattern, have been proposed and are under development.

2.4.3 Measurement of biometrics

It is necessary to have some measurements that can describe the performance and aspects of a biometric method. These measurements evaluate a given biometric authentication method and contribute to the selection of a biometric method in an application. The most important and common measurements are the FMR (false match rate) and FNMR (false non-match rate), which are the accuracy measures of a biometric method. FMR is the ratio between the number of non-matching samples and the total given samples, which the non-matching samples are matched by the system incorrectly. Contrary to the FMR, the FNMR indicates the ratio between the number of matching samples and the total samples, which the matching samples are supposed to be unmatched. The FMR and the FNMR are same as the FAR (false acceptance rates) and the FRR (false rejection rates) respectively in most cases.

In biometric applications, to reduce the searching time, the whole template set is divided into several partitions according to the biometric features. BER (binning error rate) refers to the rates of non-matching false from errors on selecting a partition. The PC (penetration coefficient) indicates the average number of comparisons for a sample in a given method. The time measurement is TT (transaction time), which the required time for an authentication process, including the collection time and computational time. The three above measurements are the important concerns when designing an application based on a biometric method.

2.5 Challenges and solutions in biometric authentication

Security is the major challenge for the spread of biometric authentication systems. As shown in the previous description, biometric authentication methods are non-deterministic approaches that could introduce some errors when identifying a user. Although some commonly used biometric methods can keep the ratio of failures in authentication at a very low percentage, biometric authentication systems are not as trustworthy as other deterministic authentication systems. Beside this, immunity to attacks and threats, privacy protection, system applicability, and manageability should be considered challenges. The biometric authentication methods suffer from various kinds of attacks that will be discussed in the later chapters.

Privacy is also an important concern in biometric methods. The biometrics of a

person is his or her permanent identity in the biometric authentication system; it is private and should be kept out of public view. The unchangeable privacy poses the following challenges: protecting and managing the privacy. When the security challenge and the privacy challenge clash, the direct challenge from customers is their acceptance of and the applicability of the biometric system.

To solve the above challenges, some methods have been developed. These methods can be classified into three types of approaches: improvement in a certain biometric method, hardware or software; coordination with other authentication methods; and reformation of the system structure. The improvement of a biometric method refers to some changes to a method that enhance the performance. For example, a revised algorithm makes the authentication more accurate. Employment of any other authentication methods with primary biometric authentication is the second type of improvement. This also includes the multi-biometric authentication methods that combine at least two biometric authentication methods. The last type is the reconstruction of the system architecture that solves several challenges using a synthesis approach.

2.5.1 Improvement in biometric methods

Some devices or software can be altered to enhance the performance of a certain method. The most significant enhancements in biometric methods are liveness

detection and high-quality sensors.

To prevent spoofing attacks, the function of liveness detection is added into biometric methods that may be defeated by fake biometric samples. A liveness detection device reads the signs from claimants to determine whether the captured biometric sample is from a living person; as such, fake or artificial samples are rejected by the system. The signs can be physiological signs or response signs interacting with the system requests. In the fingerprint method, physiological liveness signs include perspiration, temperature, pulsation, and electrical conductivity. As in the iris method, the pupil and eye movement are checked for the liveness of a person. In some other biometric methods, the system collects the responses from the claimant, who does actions according to requests from the system. In the facial authentication method, the system checks the liveness by the head movements and the emotional expression upon the command.

Except for the improvement in methods, the hardware improvements also make the system easy to face challenges. High-quality sensors give biometric authentication systems more stability and accuracy. In the fingerprint method, the dominant biometric method, the high-quality sensor can alleviate or avoid the effects of spots.

2.5.2 Coordination with other authentication methods

It is easy to introduce other mature authentication method to biometric authentication, which has lots of challenges. The coordinator can be a token, a smart card, or a certificate, all of which are widely used in computer security. A password that will degrade the system convenience is usually not a good partner of the biometric authentication. Another special coordinator is the biometrics itself.

Multi-biometrics is a special case in coordination, in which another biometric method is involved. The concept of multi-biometrics merges different biometric methods into one authentication process, which is motivated by the following reasons – noise, intra-class variations, intra-Class similarities, non-Universality and spoof [16]. In general, a multi-biometric system consists of more than two biometric subsystems for different methods and can improve the system performance in the FAR, the FRR, and so on. The subsystems make fusions that combine the information from different sources in four levels: biometric sample level, feature extraction level, matching score level and decision level [16]. This gives the system more stability and accuracy, but it requires extra hardware or more complex software. Multi-biometric authentication applications are divided into four difference categories – multi-modal, multi-instance, multi-sensorial, and multi-algorithmic. The first category indicates the usage of multiple biometric modalities in multi-biometric systems. But it is not necessary to have multiple sensors; for examples Kumar et al. use one sensor and combine the palm print and hand geometry together to make a system that has a very excellent feature in

the FMR (false match rate). The second one uses one biometric method and repeats in different instances, like checking the iris for each eye. The systems in the third category have different sensors for each biometric subsystem. For example, in the BioID that is derived from SESAM, three biometric methods – speech, lip movement and facial image – are captured; and the three biometric methods are merged to decrease the FMR less than 1%. The last category is multi-algorithmic, which captures single biometric and processes them using multiple classifiers [17].

The token or smart card can be the coordinator that helps biometric authentication solve challenges. Tokens or smart cards indicate the possession of an identity for a person, and possession-based authentication uses deterministic methods, therefore, they are helpful in increasing the stability and accuracy of biometric methods. On the other hand, tokens or smart cards also provide storage for the user's information, especially smart cards, which provide a secured platform for the privacy. Tokens and smart cards can contain biometric sensors and store templates, the structured digital biometric features, which has advantages. The first advantage is that tokens and smart cards avoid the central management of the biometric data [18]. Another advantage is that they create the mobility that allows the user to carry the information from one location to another freely. Additionally, this deployment also makes users feel that they control their information, which increases the user's satisfaction and acceptance. There are hundreds of different bands of fingerprint identity tokens on the market, such as the FIU-810 from SONY [19]. Compared to the tokens, the smart card provides a

more secured storage for biometric authentication systems. Smart cards not only contain biometric data and the sensor, but also the programs that perform the matching algorithms due to their independent computational ability. Some smart card products combine biometric sensors, store the biometric templates, and perform the matching process in the chip have appeared on the market. Typically, some of them include an encryption technique to enhance the security. The product BioPass3000 integrates fingerprints with the smart card [20].

A set of new solutions comes out when coordinating with the certificate technique and the public key infrastructure. The solutions are mostly called Bio-PKI frameworks, which can be applied in Internet services. These recent solutions are based on the Qualified Certificate (QC) and Biometric Certificate (BC) proposed by Toshiba and Hitachi respectively.

The QC method employs a certificate format based on the standard of RFC 3039, in which the certificate contains the biometric information located in the extension field. Figure 2.7[21] shows the relationship between the certificate and the biometric data. The receiving application server obtains the biometric data according to the information given by the user's certificate, which merges the PKI and the biometric techniques [28]. But in this proposal, to maintain the usability of biometric authentication, the biometrics has to be an online published resource, which may cause privacy issues. The other limitation is that the QC framework only supports the client

authentication mode.

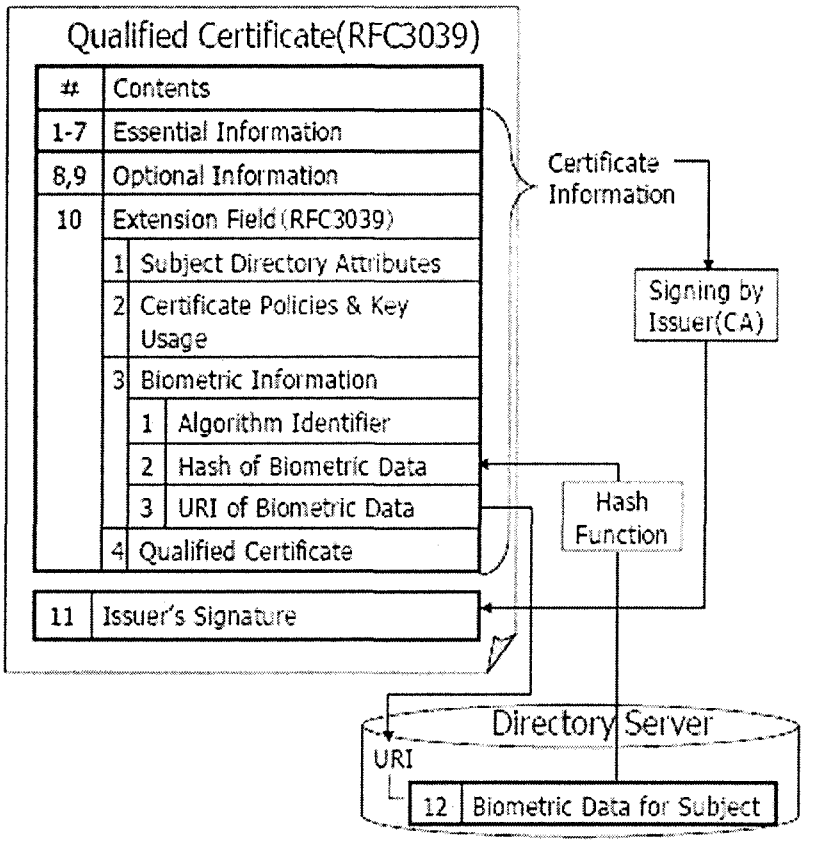

Figure 2.7: Quality Certificate

The Biometric Certificate combines the user's certificate in another way. The BC, shown in figure 2.8[21], is an independent certificate that contains the format identifier information for the template, the template data, the issuer information and the signature. The BC is connected with the user's certificate by loading the certificate identity information that is a part of the user's certificate issued into the BC. The BC framework isolates the user's certificate and the biometric template and keeps them independent, which makes it possible to store them separately. Contrary to the QC framework, the BC framework can put the matching process not only on the client but

on the server, which brings more flexibility into applications. During the authentication process, the user certificate integrity, user certificate ID and the BC integrity are checked in a sequence, regardless of what matching occurred on the client or server. The identity is authentic only when both the user and biometric certificates are keeping the integrity and the biometric sample matches the template. The detection of certificate alteration and biometric impersonation warns the system of potential attacks. The breaking of integrity implies that someone has compromised the certificates. In another case, when the matching fails, the system may be under a spoofing attack.

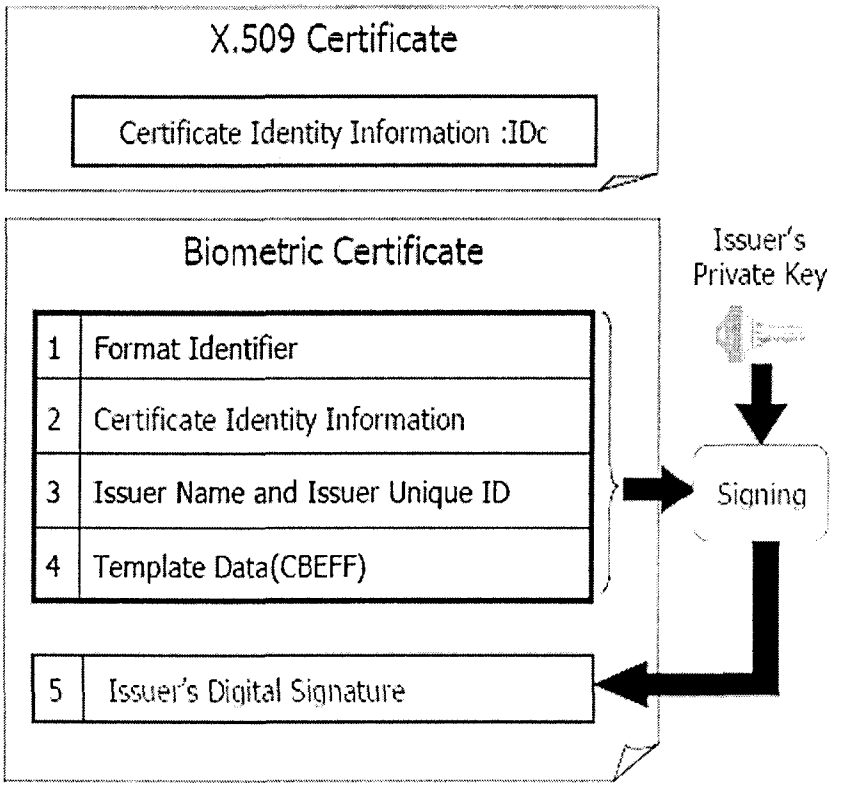

Figure 2.8: Biometric Certificate

2.5.3 Reformation of the system structure

The above-mentioned methods are the sole ways to solve a few specific challenges. The methods do not consider all of challenges and are unable to solve multiple challenges in an integrated solution. Since the system structures or architecture determine the system features and performance, the structural reformation of biometric systems is the systematic approach to improve the system performance and to solve the challenges synthetically. To reform the system structure, study and analysis of current used systems are necessary. The next chapter introduces the most commonly used architectures – centralized and distributed architecture – and analyses them in aspects of security, privacy protection, and applicability.

Chapter 3: Studies on Current Architectures

Before reformation on the system structure, the study of currently used system architectures is inevitable and necessary. The study includes the comparison between traditional architectures and analysis of them on the security, privacy, management, and application aspects, which is the base of reformation of system architecture.

3.1 Introduction to traditional architecture

In the real world, two current architectures are widely used for biometric authentication systems, centralized and distributed architecture.

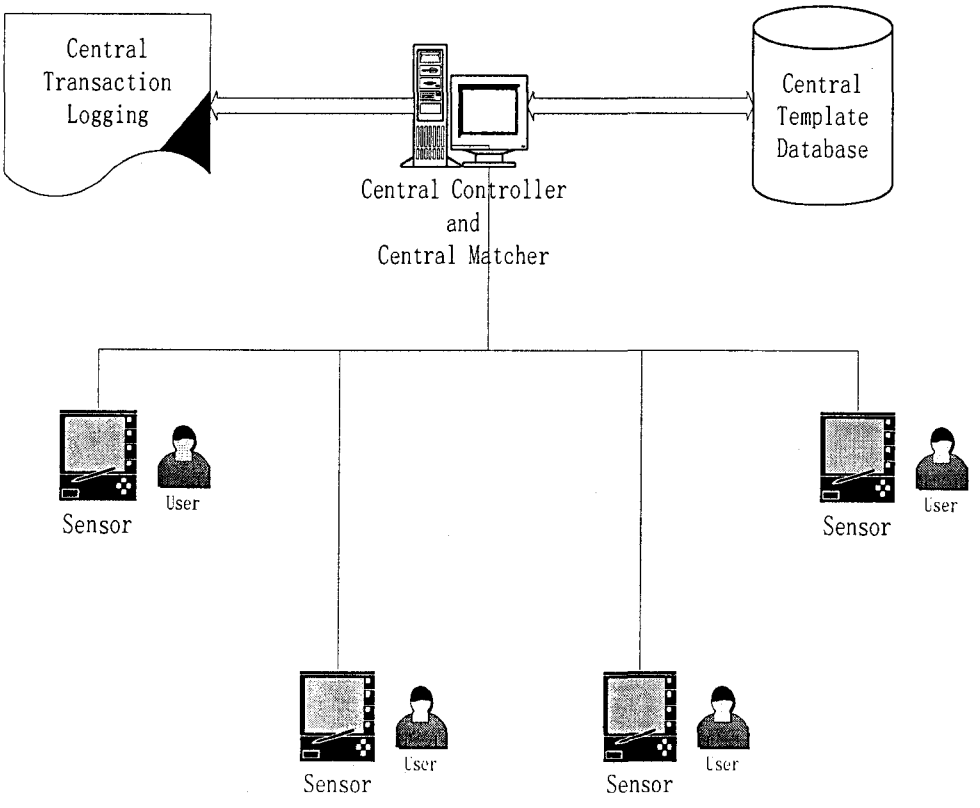

Figure 3.1: Centralized biometric system architecture

The centralized architecture shown in Figure 3.1[22] has a central matcher that is

connected to each checkpoint and only one central template database where the system stores all possible users' biometric templates. When a user approaches a checkpoint that has the sensor installed, the user's biometric sample and his claimed identification will be transmitted to the central matcher on which the comparison with templates from the central database is performed. The central controller records the match results and then sends back the related access rights associated with the authenticated user to the checkpoint.

Compared to the centralized architecture, distributed architecture in figure 3.2[22] duplicates the matcher and template database that stores frequently used templates in each checkpoint. The authentication process is the same as the process in the centralized architecture systems except that the matching operation is performed in local checkpoints and only the result is submitted to the central controller. Distributed architecture systems have more management operations than centralized ones, such as the updates of the database and matchers, if necessary.

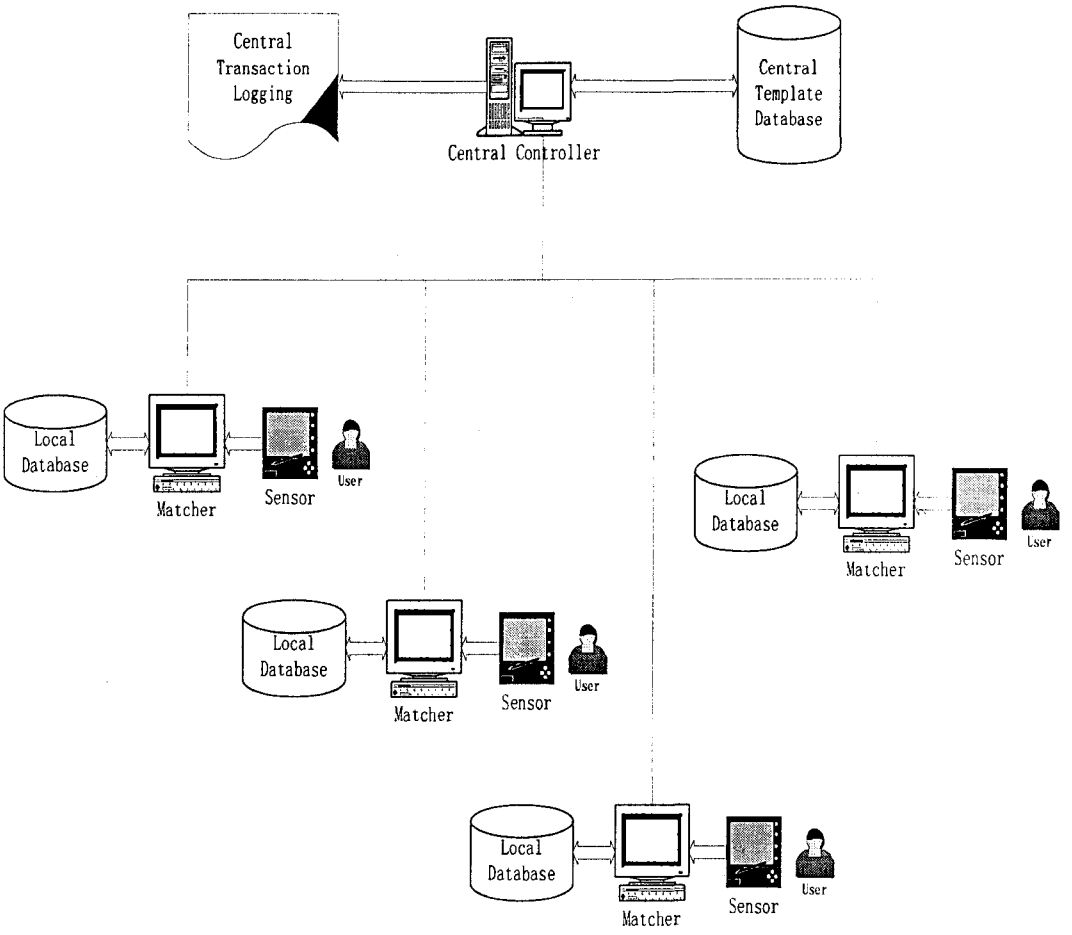

Figure 3.2: Distributed biometric system architecture

Both of the architectures have advantages and disadvantages. The centralized systems consume more communications between checkpoints and central server, but it is easy to construct and maintain these systems based on the centralized architecture. On the other hand, the distributed architecture-based systems reduce the demand of the communications and enhance the robustness against system-wide failures. Because of their more complex system structure, these systems increase the cost and difficulties of construction and maintenance.

Distributed Architecture	Centralized Architecture
Less communication loading	More communication loading
Less prone to system-wide failure	Greater risks of system-wide failure
Backup and maintenance are more complex	Easy to supervise and manually override

Table 3.1 Distributed biometric systems architecture versus centralized biometric systems architecture [22]

3.2 Security analysis of biometric systems

The security analysis focuses on two fields of a biometric system – the natural security features and the ability to prevent attacks.

3.2.1 Native security features

The purpose of authentication is to identify a person; therefore, accuracy is an important measure in any authentication system. Generally speaking, two kinds of mismatching exist in any authentication system, treating an illegal person as authentic or rejecting a correct person from entering. The first kind of mismatching threatens the system security particularly seriously.

In the security systems, to compute the strength of the security in bits helps us to measure the biometric authentication systems' security ability. Based on the analysis of probability, if there is a brute force attack that builds a set of fraudulent fingerprint minutiae to cheat the matcher, the fingerprint authentication system has 40 bits of information if the minutiae number equals 15 [23]. According to the figure 3.3[23], there is nearly a linear relationship between the minutiae number and bit length. Although the system security strength can reach hundreds of bits when the minutiae number is increased, the number is limited in a range and, for more typical usage, minutiae number m = 25, the information length is around 82 bits, which is as strong as 16-character nonsense password [23]. The result reveals that the biometric authentication system does not have stronger ability to secure the system than other authentication technologies.

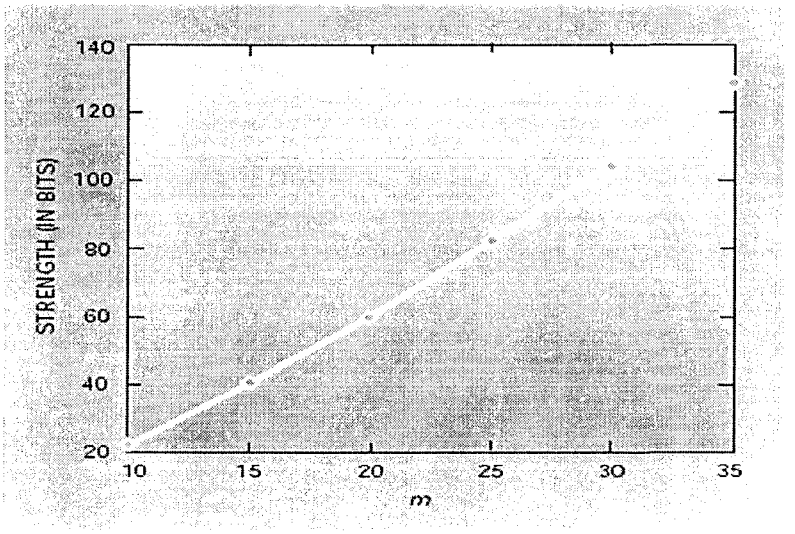

Figure 3.3: Minutiae number and system strength

3.2.2 Immunity to attacks

In the real world, an authentication system has to face various attacks day by day. The successful attacks defeat the system, misuse the system resources, and decrease confidence in the security system, which influences the spread of applications. The more immunity the system has, the stronger the system is. The evaluation of immunity starts with the analysis of potential attacks based on the biometric authentication model. Ratha and his colleagues identify eight potential attacks in a framework of a biometric authentication system, occurring on function blocks and the links between them.

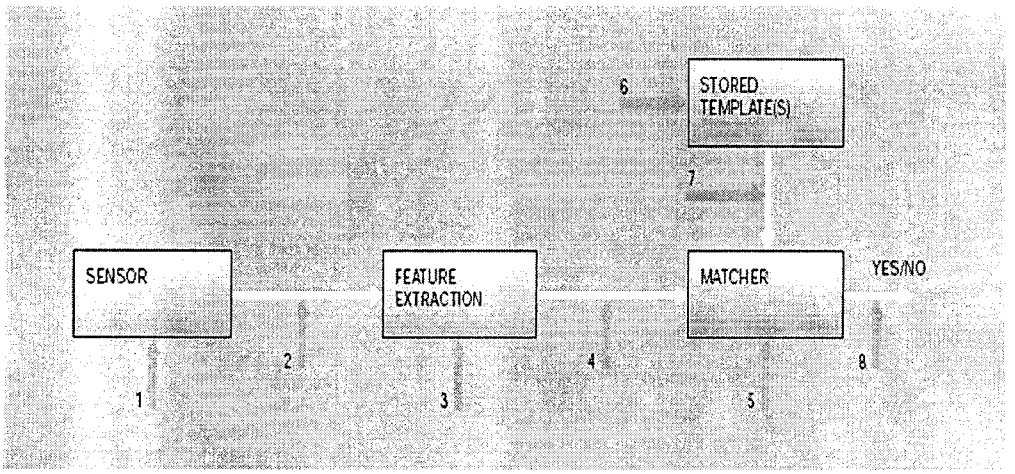

Figure 3.4: Attack model on biometric systems

Labeled 1-8 in Figure 3.4[23], they are as follows:

1. Presenting a fake biometric to the sensor;
2. Submitting a previously recorded biometric to the feature extractor;
3. Overriding the feature extraction process;

4. Tampering with the feature representation;

5. Corrupting the matcher;

6. Tampering with stored templates;

7. Attacking the communication channel;

8. Overriding the final decision.

According to the previous description, attacks against the biometric authentication systems can be classified into three types by the targets to be attacked – biometrics, components, and communication channels. Attacks against the biometrics fabricate biometric samples and fool the system by representing the samples to sensors or submit forged biometrics to the feature extractor, bypassing the sensor. Channel attacks that capture and change original data on the communication channel between two components exist in the channels connecting the two system components and make biometric systems fail to authenticate users correctly. Otherwise, the software, like matchers and feature extractors, in biometric systems may suffer from Trojan Horse that produce pre-defined data under some specific conditions set by virus designers. The attacks are classified as component attacks, whose object is the system components. Moreover, due to the unreliability of system components, the system is easily interfered with replacing a component with a fake one that can produce the attackers' desired output, despite of input.

Another paper revealed a smarter attack method that occurred in label 4 to attack

the user's account. The result indicates that, "on the average, the attacking program needed only 271 iterations for breaking into an account" [25]. Therefore, the hill climbing procedure is effective in attacking the minutiae-based biometric authentication system and makes attacks easier and quite frequent.

Additionally, other kinds of attacks against biometric authentication are mentioned. Other possible attack targets beyond the components inside biometric authentication systems are proposed. Figure 3.5[24] indicates four more potential attacks and corresponding threats on biometric authentication systems, which are tagged the numbers T11 – T17 [24].

Five complementary attack targets:

(a) *Cryptography,* for protecting the authenticity and integrity of data traveling in the channels

(b) *Audit,* major actions for system analysis

(c) *Power,* is an important concern for portable biometric devices

(d) *Environment and users,* general concerns in a system design.

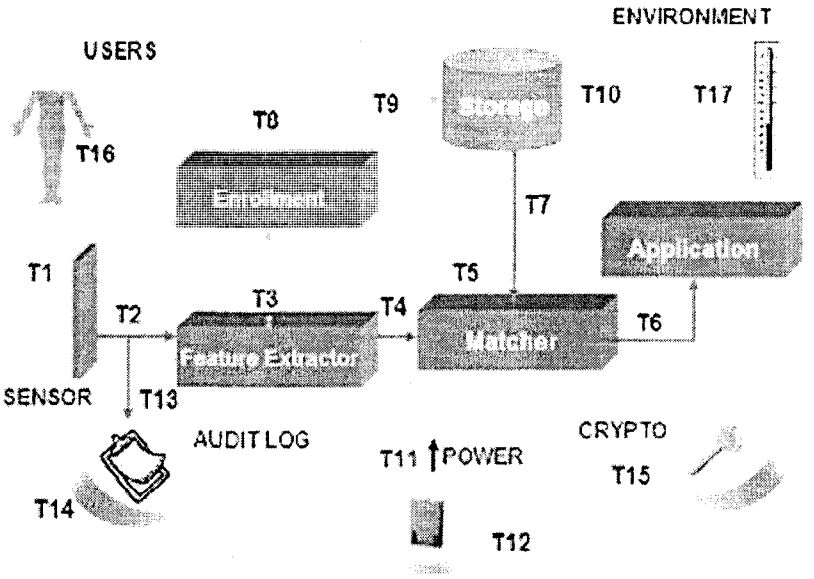

Figure 3.5: Attacks on biometric systems

Threats corresponding to the complementary attack targets:

T11 The power of the system is wrecked.

T12 The power of the system is altered.

T13 The audit records cannot be collected because of the damage of the channel that conveys the audit information.

T14 Audit records may be tampered or deleted.

T15 Security functions may be not strong enough and fail to defend the cryptanalysis

T16 Users can harm the security functions.

T17 The application environment features (temperature, humidity, lighting, etc.) and usage may decrease the security of the system.

Traditional architectures are sensitive to the failure of system defense, which means a successful attack may evoke serious results, even crashing the system. Attackers can obtain critical data by intruding on the central controller, the central template database, and local databases in which systems store critical information and user's biometrics. The biometrics is the identities of users; thus the intrusion will affect all users who have provided their biometric sample.

Pure biometric methods lack the ability to detect attacks. In deterministic authentication methods, such as the password authentication, a series of false of authentication implies that someone is trying to guess the password. But in biometric authentication systems, it is hard to confirm attacks due to the native false rate from a non-deterministic approach.

3.3 Privacy, manageability, and applicability analysis

Privacy protection obstructs the wide application of biometric authentication systems based on traditional architectures. User biometric is private. But in traditional architectures, the enrolled biometric templates are stored in a database managed by the system, regardless of whether the system is centralized or distributed, and it means users cannot control their own privacy. It causes low acceptance of biometric authentication systems.

Additionally, there is a basic feature of users' biometrics, which is the irrevocability of biometrics. It is an element of the biometric authentication, but it is a problem for privacy protection. The problem is concisely paraphrased by the following: "Theft of biometrics is theft of identity." [26] In traditional architectures, the defeat of protection of a user's biometrics causes the user's privacy disclosure and the loss of his or her unique and permanent identity, which means the user cannot use the biometric authentication system in the future.

Another possible vulnerability in traditional architecture-based biometric authentication systems is the disclosure of the critical data that refers to biometric information or authentication results. In centralized systems, the biometric samples and the user's identification claim are uploaded to the matcher via a communication channel between the central matcher and checkpoints. And in the distributed systems, the authentication results from local checkpoints are passed to the central controller. The authentication results are also pivotal information to the authentication process and should protected.

Traditional architectures are devoid of flexibility that makes system cart for different requirements. In these architectures, the sensors accompany checkpoints that have connections with the central matcher or central controller, regardless of whether the system is centralized or distributed. And there exists a default bind relationship that causes the loss of mobility, which means users cannot use the biometric systems until

they access a system-specified checkpoint. When the user moves to an other place without such a checkpoint, the system and the authentication service are unavailable. To solve the problem, system builders can set up more checkpoints, but it is costly to construct and maintain them.

Chapter 4: The Proposed System Architecture

A secure biometric authentication system largely depends on the system architecture, the biometric type, and the system management. Since the system architecture influences the management instruments, method, and policy, the design and selection of architecture is pivotal when designing a biometric authentication system. All systems can be broken down and abstracted to several components, each performing an important and necessary function. The design of the architecture is to deploy the abstracted components and define the function for each component and interactions among the components.

For the architecture of a biometric authentication system, these features – confidentiality in figure 4.1, manageability, privacy, and usage – are taken into account. Confidentiality is the secrecy of a system and is also the core function of an authentication system. Privacy and convenient usage influence the users' acceptance of the authentication. The manageability decides the maintenance and economy features for the service provider and also affects the global security of the system.

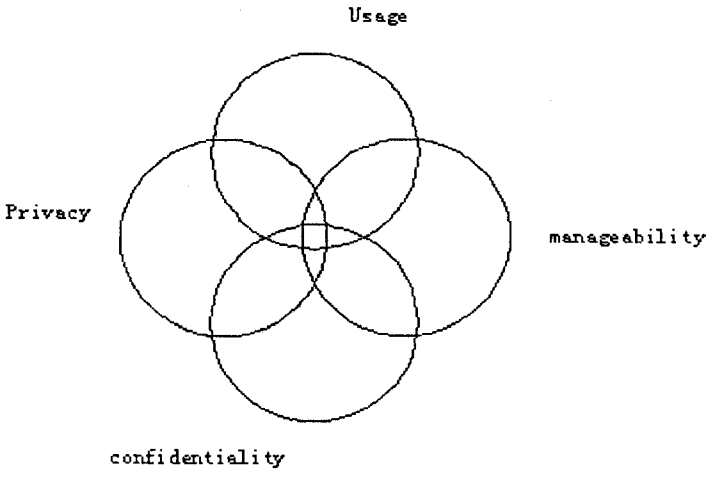

Figure4.1: System considerations

Traditional architectures have three layers classified by the location, server client, and user, which is shown in figure 4.2 and 4.3 for traditional architectures. The biometric components, matcher, template database, and sensor are smashed and merged into the server layer and client layer. The centralized architecture provides the indirect communications that rely on the relay of other components between any two biometric components, which degrades the security of the system. The distributed architecture moves the matcher and database to the checkpoint, which increases the management tasks and fights more attacks.

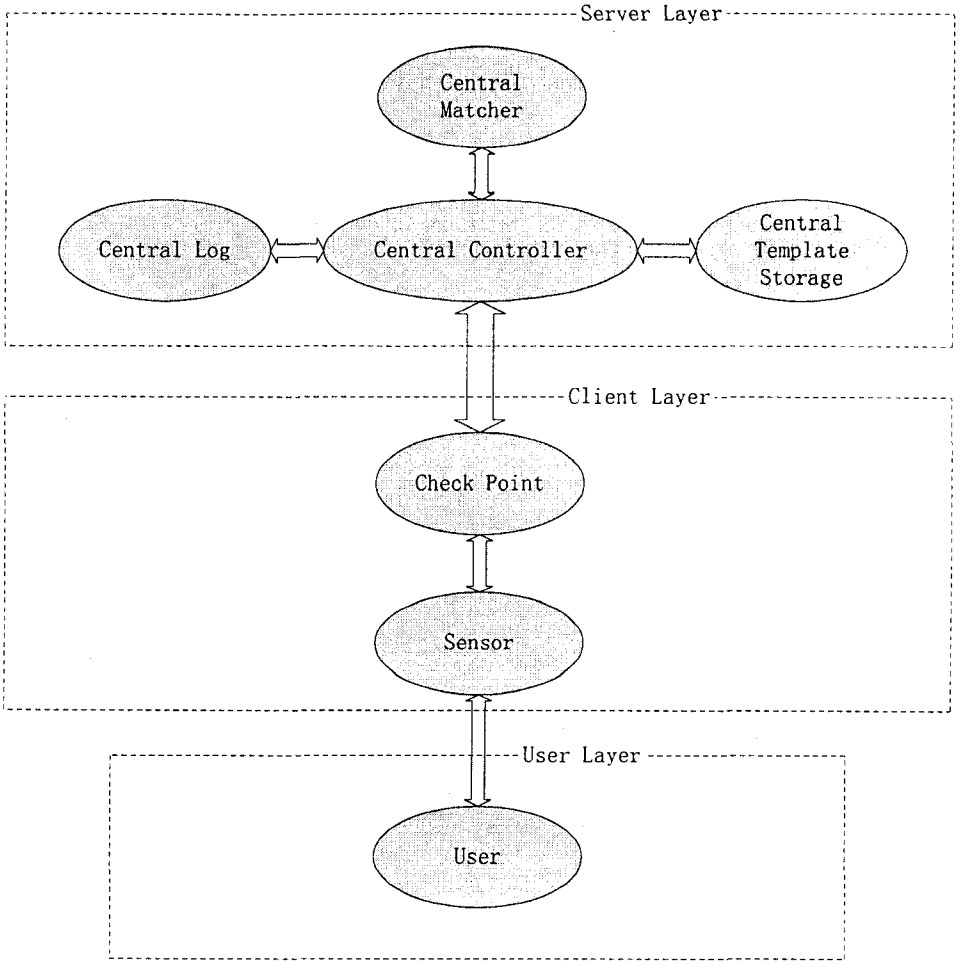

Figure4.2: Layer model of the centralized biometric authentication system

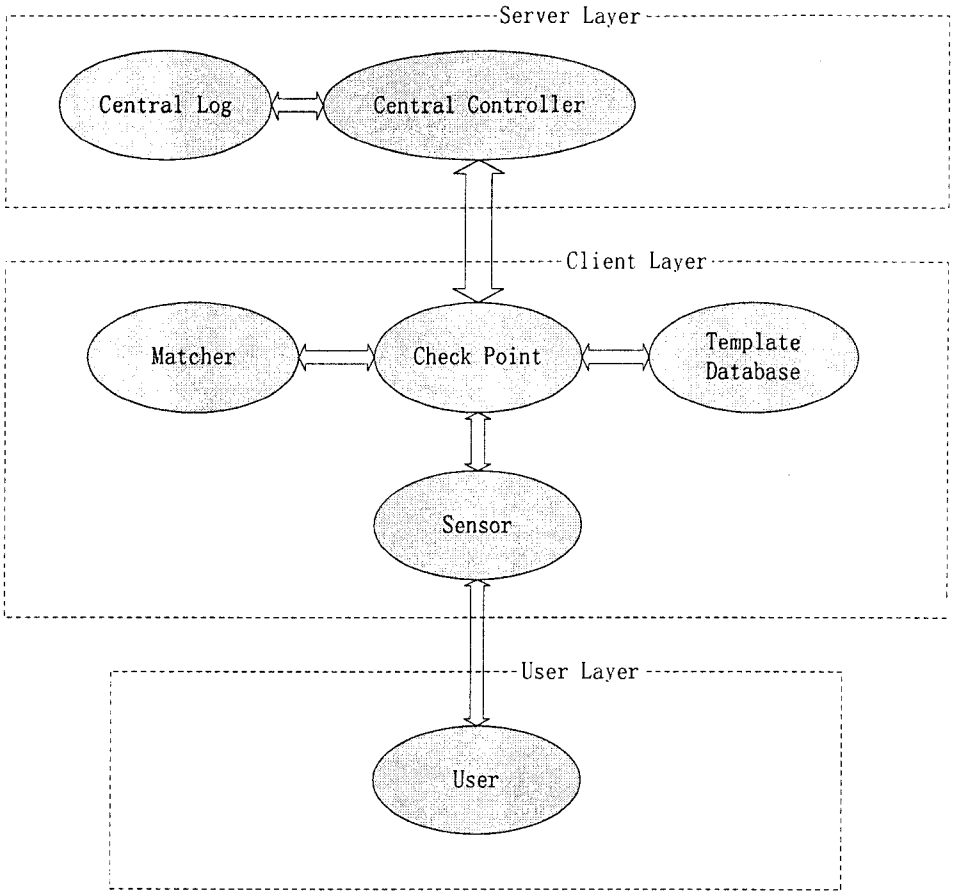

Figure4.3: Layer model of the distributed biometric authentication system

New system architecture is formed when biometric components are extracted and gathered into one new layer, called the biometric layer, where the biometric layer and all biometric-related components are connected directly. The new layer that has four layers can mend the system security, management, and usability, as well as the mobility, which is a new feature obtained from the new system architecture.

4.1 Proposed architecture

Composed distributed architecture (abbreviated to CDA) is a new model that has a more flexible structure, more security abilities, and more applicability for different application requirements. In this model, a biometric authentication system is made up of six parts (classes) – users, sensors, databases, matchers, check platforms, and a central unit – and each class represents a primary element in every biometric authentication system. All involved objects in a biometric authentication system, including persons, software, and hardware devices, can be classified into one of the six classes. These components interact with each other via the communication channels that exist between the two system components during the authentication procedure and convey the data exchanged between two components. There are four layers, the server layer, client platform layer, biometric system layer, and user layer, in this model, and each model contains at least one component and represents the structure of a biometric authentication system. In traditional architectures, all objects in the systems can also be mapped to the above object classes and divided into four structural layers.

The target of the new model is to provide more secure application architecture with system mobility and easy management. Different from the traditional architectures, the biometric-related objects should be authenticated before they are used as a part of a biometric authentication system. The check platform objects are the component that needs verification optionally when the system security requirements are high. The communication channels in the biometric layer are protected by the

encryption method that is retrieved from the central unit by components in the biometric layer after they are verified.

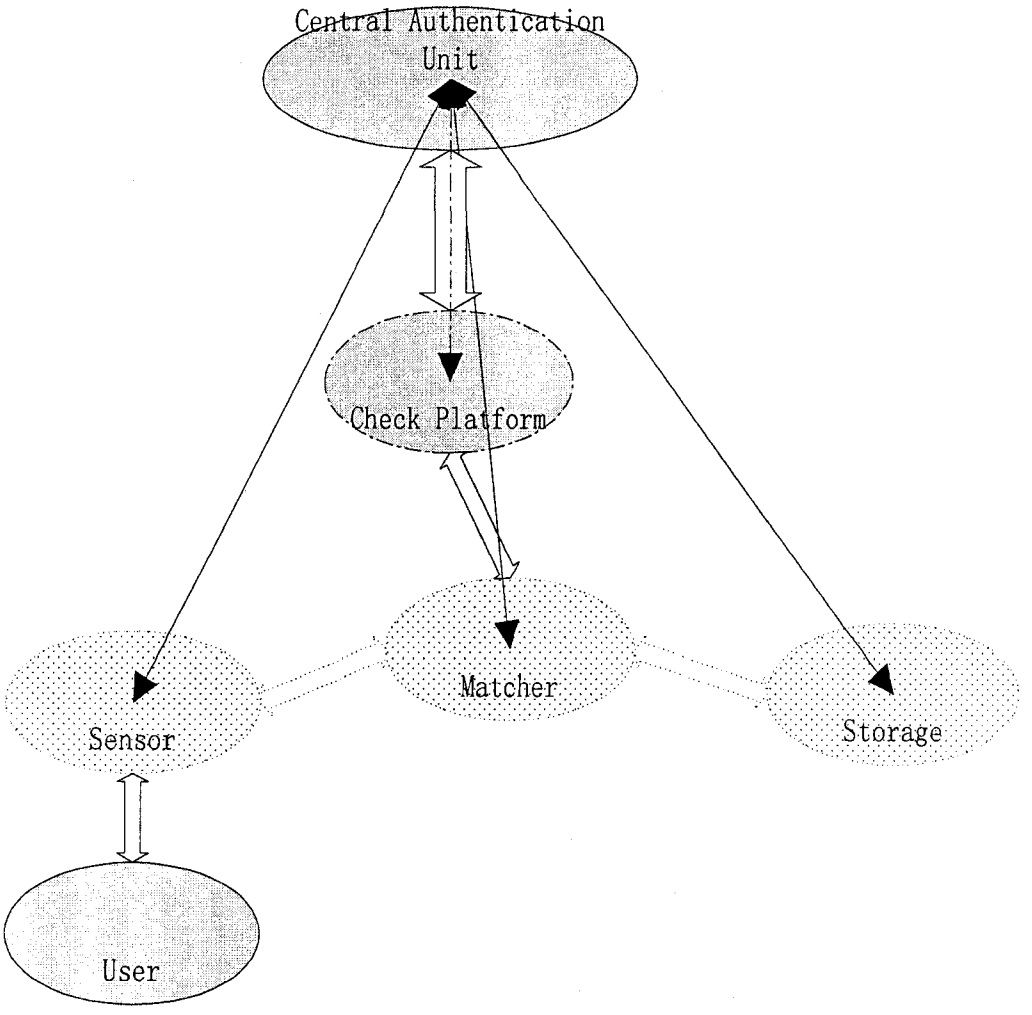

Figure4.4: The architecture of composed distributed architecture

This figure 4.4 depicts the components, connections, and relations in composed distributed architecture. The ellipses represent the components that are gathered together by the connections, and some of them need to be authenticated before they merge into the system and work properly. The dashed double lines indicate that the

connections exist temporarily and are protected by the dynamic channel keys assigned by the authentication server. The lines with arrows indicate the authentication relationship of the components. The authentication of the component connected by the dashed line is not mandatory and depends on the system design, security requirements, and application environment.

4.2 Components

Users in this architecture represent persons who attempt to access the resources that are protected by a biometric authentication system. They request the authentication service, conduct verification or identification operations, and retrieve the proper access rights on certain resources. An authenticated user is a person that meets the following criteria:

1) The user owns the proper system components, such as a flash disk that stores template data, a matcher program, and a combined biometric sensor. Or the user assigns the related components and has access to them, such as an online template database.

2) The user presents the expected biometric that proves who the user is.

Sensors, biometric information capturers, obtain biometric samples that could be an image or a sequence of signals from users when the authentication system is in use. Sensors convert the actual biology information to the digital representation that is

recognized by computer systems and is used in matchers to perform the authentication operations. For security purpose, the sensor object should be registered in the central unit in the enrollment stage, because the data it captured is the pivotal role of biometric authentication and is critical information that is sensitive to tampering.

Template database storage stores templates that are the mathematical representation in digitals, created in the enrollment stage, of a person's biometric data and can be retrieved during identification and verification operations in the authentication stage. Like the sensors, the template database storage objects should also be enrolled into the central unit, which protects the database and provides the system with a high-security feature. The database resides in diverse digital media, such as hard disks, flash disks, and smart cards.

Matchers can be software or a device that extracts the features from incoming biometric samples, compares these features with templates stored in the database according to a certain algorithm and scores the user's biometrics. Based on the scores, the matcher makes the decision whether the user's identity is correct. The matchers have to be approved by the central unit to prevent attacks.

The check platform can be a device or a system where the matchers perform comparisons when users ask for authentication service. The check platform provides the connections between the distributed system components and the central unit.

Therefore, the sensors, matchers, and databases connect to the platform before they are authenticated and communicate with the central unit via the channel between the check platform and the central unit. Sometimes the check platform also manages the communications between two system components when they are in authentication operations. The approval from the central unit to a check platform is not necessary unless the system needs high security. When the user uses real digital storage to contain the components, the check platform is the platform where the biometric authentication system runs.

To compose a correct and secured biometric authentication system, objects from sensor, database and matcher classes have to be authenticated by the central unit, and they are also able to connect and create the communication channels with the central unit when the system is in the authentication procedure. In some applications, only approved platforms are allowed by the system when high security is required.

The central authentication unit is a server that provides authentication services for other components in a biometric authentication system and stores necessary information used to approve the system components during the system authentication procedure. The central unit that all operations in the authentication procedure are involved with is the central and core part of this architecture system, which manages components and performs operations. In the enrollment stage, the central unit assigns identities to all system components that will be issued to a certain user and records the

information on them.

The central unit is also indispensable and mainly responsible for establishing a complete biometric authentication system in which there is at least one valid object in each class in the authentication stage. When a user asks for the authentication service using assigned components in the authentication stage, the central unit verifies the system components based on the enrolled information and then sends the components the credentials that are used to build up the communication channels and compose a complete biometric authentication system. The system verifies the results of biometric authentication with the information stored in the central unit and decides whether the user passes the identity verification. At the end, the central unit decides whether the user and his or her claim are valid or not according to the biometric authentication results from the composed system.

4.3 Layers and communication channels

In the system, a component interacts with others via communication channels in which the data is transferred. The communication channels also combine the components together and make all components work properly as a complete biometric authentication system. Some of the communication channels are only accessible when the components in both sides are authenticated and have gotten the credentials for the other components; therefore this mechanism improves the system security and

flexibility simultaneously.

Depending on the components' role and relationship to each others, the architecture can be divided into four layers: server, client platform, biometric system, and users. The server layer refers to the authentication service provider that is the central unit in this architecture. On the lower layer, the client platform is the place where the authentication requests come, and in the architecture, the check platform is the only element in this layer and it provides communication services to the server for the lower layer. In the biometric system layer, sensors, matchers, and databases employ the communication services from the client layer, build up a complete biometric authentication system, and work on the check platform to verify operations. The user layer represents the service requester who provides the biometrics and related components.

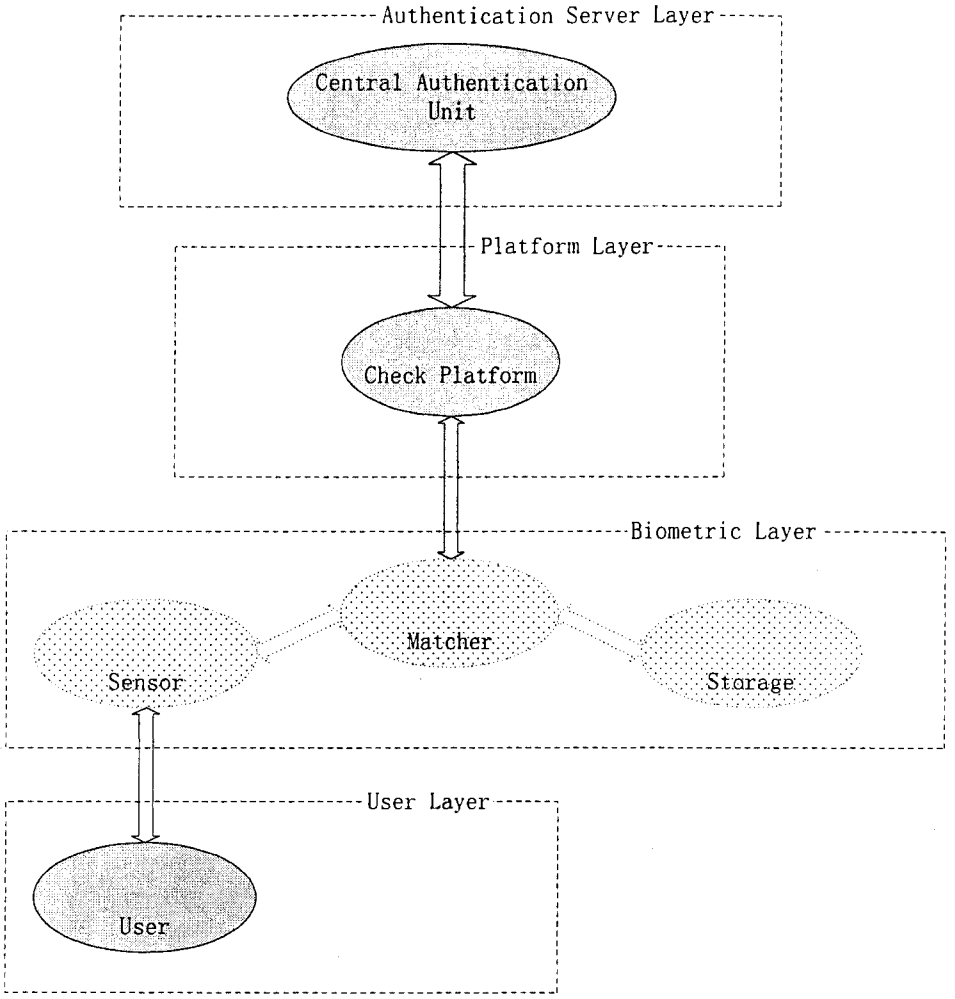

Figure4.5: Layer model of composed distributed architecture

All communication channels can be classified into two types, depending on whether both sides of a communication channel are in the same layer as the figure 4.5. The first type, type I, is the communication channel between two adjunct layers, such as channel A (central unit <-> check platform), channel B (check platform <-> matchers), and channel E (sensor <-> user). These communication channels convey the service request, response, and raw biometric data; therefore it is not necessary to authenticate components on the both sides of these communication channels. Contrary

to the first type, the other type is the communication channel that exists in a layer, which refers to the channel C (matcher<->sensor) and channel D (matcher<->template database). To secure the composed system, these two channels are not usable until the components on both sides are authenticated and get the credentials from the server.

The communication channels can be implemented using various techniques. In most applications, the channel from the central unit to the check platform is the Internet. In mobile phone-based applications, the channel can employ the IrDA or Blue Tooth to transfer data. For internal channels, the channel can be a virtual one that is implemented by the data movement in memory or an actual one, such as the Internet, if one of the biometric layer components is a network resource.

The composed distributed system architecture is a revised version of Distributed architecture. The components in the additional layer, the biometric layer, can be mapped to the components around the checkpoint in the distributed architecture. But the authentication process, the connections, and the component's functional definition are different. Moreover, the extracted biometric layer provides the system with the mobility that does not appear in traditional architectures.

4.4 System steps

All biometric authentication systems generally work in two groups of steps –

enrollment and authentication. In the new architecture model, according to the structure and definition, not only all users but also all objects that are used by users need to be registered with or obtain the credentials from the system central unit in the enrollment mode. Usually, a user provides his identity and biometrics that are stored in central unit and user-specified database respectively. For the authentication of components, the identities of the storage, sensor, and matcher are also recorded in the central unit, which returns to them the related credentials for further verification of these components.

The authentication mode represents the steps of identity verification and determination made by the authentication system. In the new architecture, firstly the central unit receives the component identities that refer to the objects to be used by user authentication. Then the central unit makes the decision about system composition, that is, whether a complete and valid system can be built up before the identity verification. If the composing operation fails, the subsequent operations will be ignored and the authentication process will terminate. Otherwise, the platform receives the successful response from system composition and is able to access the system components to accomplish the user authentication. It submits the identity that represents the user's biometric template in the storage object to the central unit in which it will map to the correct user. Finally, the user authentication process terminates with the mapping results whether the user is whom he claimed to be.

4.5 System operations

The biometric authentication system that is based on the new architecture, in figure 4.6, has the following operations: biometric enrollment, biometric verification/identification, component enrollment system composing, and system discard. In these operations, biometric enrollment and biometric verification (identification) are foundational operations in all biometric authentication systems while the other three operations are specific to the new architecture model.

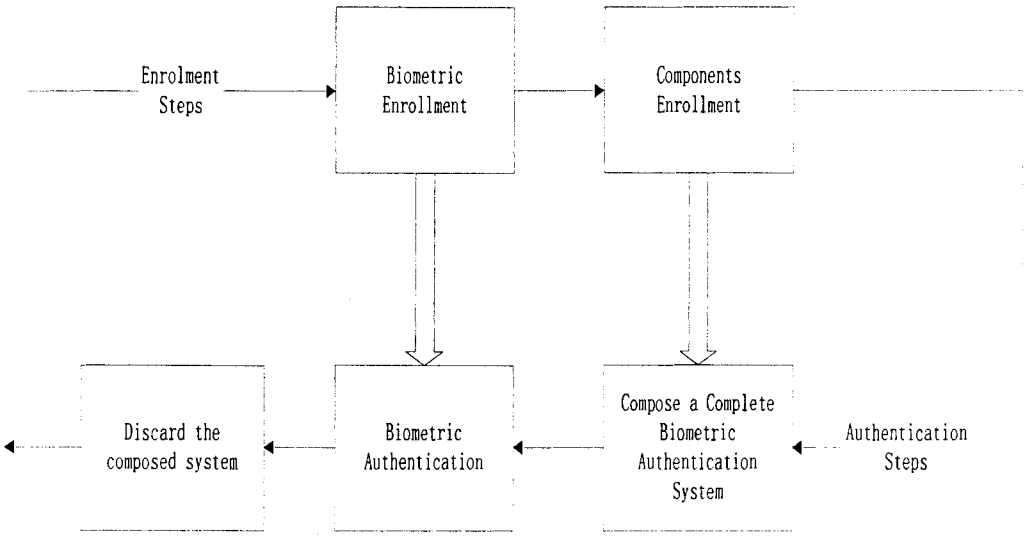

Figure4.6: System steps and operations

Normally, biometric enrollment is the process of capturing user's information for future authentication. In every biometric system, this refers to capturing the users' biometrics, creating templates, and storing them when constructing the system. Moreover, the user's identity should also be saved in the system.

Like the enrollment of users' identity and biometrics, the components related to a

user should also provide their information to the system and obtain the identities that will make them approved by the central authentication server in future use. In the authentication procedure, the enrolled components should be verified by the central authentication server, which results in the acquisition of credentials for communication construction. As described in the last section, the components that are related to the type II communication channel have to enroll themselves in the system. Therefore, the object enrollment operation is mandatory for sensor, database, and matcher objects that are security-needed components in a system. For the check platform object, it is an optional operation that is performed according to the system security requirements.

System composing is a process that attempts to pick the existing components and build up a complete biometric authentication system that contains all necessary elements and works as a proper biometric authentication. Differing from the traditional architectures, systems based on the new architecture have dynamic components instead of fixed ones, which means that the system does not know where the desired data source is and how the system works. Therefore, a dynamic system that contains all valid necessary objects has to be constructed before the verification or identification operations are invoked. After that, the following authentication service request is disposed of by the composed authentication system that works as a traditional biometric authentication system. When the authentication service terminates, the composed biometric authentication will be dismissed, and there is no data interaction between any two components.

Biometric verification is a process of one-to-one comparison [30] in which the biometric system attempts to verify an individual's identity based on the user's biometric and claimed information. If a set of biometric features is similar enough to a user's template that is claimed by the user, the system confirms the claim with a binary value that represents yes, and the verification is successful. Biometric identification is a process of one-to-many comparison [30] in which the system attempts to find out who the biometric sample submitted by the user belongs to. A possible implementation of identification is exhaustive verification, in which the incoming biometric sample is compared to all enrolled templates and determines the identity by the most similarity. Therefore, identification is considered a sequence of verifications for each stored reference template. Both the biometric verification and the biometric identification operations are four-stage processes that contain capture, extraction, comparison, and match/non-match.

After the system finishes the authentication, the composed biometric authentication system will be deconstructed, which the process is referred as discard operation. The system dismiss operation is responsible for furbishing the system to the state the system was in before the authentication was performed. In this operation, the system discards the credentials from the central unit, closes the communication channels, and releases the allocated memory, and all security-related data is erased. If necessary, the operation updates the information of the components for authentication

to maintain the system's security after the old information has been used for a period of time and expired.

4.6 Authentication process

The system based on the new architecture verifies the user and his or her claimed identity by comparing the reference information stored in the central unit to the information that is derived from the results of the biometric authentication performing in the check platform or online. According to the authentication criteria, a user can ask for the authentication service until he obtains an identity assigned by the system and some devices that contain the enrolled system components in the biometric layer. The component container device could be a real one, such as a digital storage, or a virtual one, like an online database.

When a user starts the authentication service in a system based on the new architecture, he has to make the platform layer and the biometric layer connective. If the biometric layer components are in a physical digital storage, they connect the platform via a physical interface, such as USB, and when they are online resources, the user should provide the information on how to find the online resources and access them.

After the system recognizes the necessary components (but they are not usable at

that time), it is ready to deal with the authentication request. The request information contains the identity to be verified and the user's biometric sample, both of which are submitted to the platform and sensor respectively. The central unit retrieves the reference information for each component in the biometric layer using the identity forwarded by check platform and returns the check platform the reference information to validate the components that have connected to the platform.

The reference information from the central unit challenges the biometric layer components that have connected to the platform, which results in responses from the components that verify themselves. If the components respond with the desired information to the central unit, they are considered authenticated and are ready for the next processes. Whereas the responses from components in the biometric layer are not expected; the component cannot be accepted for the next processes and no secured communication channels can be established, which means the authentication fails to verify a component in the biometric layer.

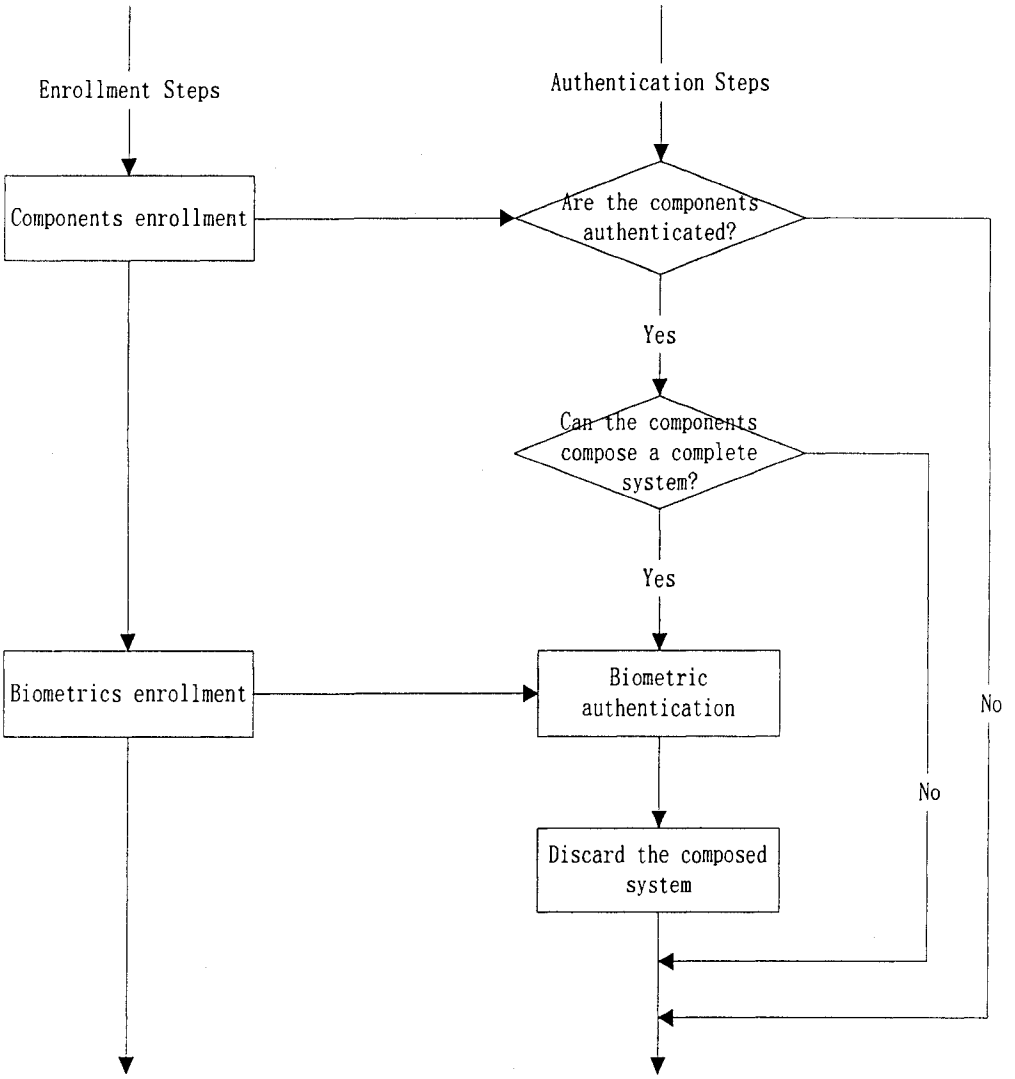

Figure4.7: Enrollment and authentication processes

When the all of the components of the biometric layer are authenticated, the central unit confers the components credentials to build up the secured communication channels in the biometric layer. If the components cannot exchange data by communication channels using the conferred credentials from the central unit, the authentication fails to compose a biometric authentication system. When the communication channels in the biometric layer are established, the components in the

layer are connected with the protected communication channels and compose to a complete biometric authentication system that has matcher, sensor, and template database. The composed biometric authentication system identifies the user's biometric sample that was submitted previously with the templates in the database.

The information associated with the identification results is sent to the central unit by the matcher component and is verified by the central unit in which the submitted information is compared with the stored information according to the user's claimed identity. When the information from the composed biometric authentication system is matched to the reference information that the claimed identity has, the user who provides the biometric sample and his or her identity is verified. The submitted information reveals the user, who is verified by the biometrics and the user's possession. Therefore, the user is authenticated only when the user who enrolled the information holds the biometric components and presents his biometric samples. The incorrect biometric system and undesired biometrics cause the submitted information not to match the reference information, which makes the authentication fail.

Chapter 5: Analysis of New Architecture and Comparison

The proposed architecture inherits the advantages of traditional architectures. The new architecture reduces data transactions, especially pivotal and sensitive data, between checkpoints and central servers to improve system security. Mostly, several objects will be integrated together for convenient usage, which results that data transactions are constrained in a local system. As a result, in new architecture systems, only the identity of a certain template in the local database and its related information, tens of bytes, is compared to several KB of biometric information will be sent to the central unit after the local biometric authentication is successful. Because of the distributed structure, the new architecture has less system failure. The analysis of the new architecture was based on the challenges and the vulnerability existing in the current system architecture.

5.1 Security analysis

In the new architecture, system security is improved in three aspects -- authentication mechanism, attack space, and resistance to attacks.

The single-factor authentication mechanism is applied in traditional architectures, central or distributed, and in these systems a user is authentic when he or her provides the expected biometric information identifying who he or she is. In the new architecture, some system objects need additional information before they can be

accessed and some kind of media to reside in, which involves other potential factors in the system authentication process. Therefore, the security of new architecture-based biometric authentication systems is strengthened by applying instinctive multi-factor authentication mechanisms that are usually more secure than single-factor authentication methods. According to the operations and process stages of this architecture, sensors, matchers, and storage objects enroll their identity previously and should be authenticated before they become accessible to the check platform object in the authentication procedure. As a result, in the new architecture, a user is authentic when he or she presents the expected biometric information and he specifies or provides the valid objects and makes them accessible. This process involves at least two authentication factors –biometrics, what the user is, and the objects, what the user has. For example, there is a system in which the templates are stored in a Smart Card that is protected by PIN number. In this case, possessions (Smart Card), knowledge (PIN number), and biometrics are all necessary for successful authentication.

The change to the mechanism also alters the system strength. The new architecture enlarges the attack space of the biometric authentication system and makes it harder to attack the system. Based on the attack space statistics, multi-factor authentication methods provide significantly larger attack space than single factor mechanisms in which the biometric factor is the smallest one. So the attackers should spend much more time, hundreds and thousands more times than before, to conquer the system if they use a brute force attack method that defeats an authentication system

by trying a large number of possibilities. As described in the table, the average attack space of a biometric method is from 2^6 to ^{219}, which means the attackers can break the biometric authentication system after 2^5 trails in the worst case. The small average attack space causes biometric-protected systems to be risky in this age in which efficient machines are developed, and it also makes brute force attacks effective. In the new architecture, the attack space increases remarkably. If the system objects reside in a public key token where the average attack space is 2^{63} to 2^{116}, the system integrative attack space will be 2^{82} to 2^{179} [27].

Typical attacks that are successful in traditional architectures are no more effective to the new architecture systems. In the new architecture, it is necessary to represent the correct fabricated biometrics and provide additional component information insicating when attackers can fraud the system. Since the new architecture endures the system's mobility that gathers the biometric-related components in a device or storage kept by the user, the attackers have to obtain the device or the storage that belongs to the user whose biometrics will be fabricated. Another way to fraud the system is to fabricate biometric samples and the additional component information. Compared to biometric information, the additional component information, such as physical token information or an issued public key, contains more information that makes it more difficult to fabricate, which makes the fraud attacks almost impossible (the success probability is as low as 0).

The new architecture has a mechanism against the channel attacks. Encrypted communication is the most widely used and efficient technology to protect communication channels. There are two encryption modes, symmetric and asymmetric such as PKI (Public Key Infrastructure). Whatever mode the system uses to protect communication, the pivotal step is to issue and share the secret that is used to encrypt the data transmitted in the communication channels. In the enrollment stage of new architecture, the user-specified objects should register their identities in the central unit. Therefore, the enrollment operation provides the opportunity to issue the keys or share the secrets between the central unit and the user's objects for future encrypted communications, for the keys and secrets are the milestone to build up the secure communication channels. The channel keys applied in the internal channels are dynamic, and the same biometric components are composed using different channel keys each time and contribute to the system's high security.

The dynamic keys not only protect the communication but also prevent Trojan Horses attacks in the new architecture. The Trojan Horse, like some viruses, produces some pre-defined data to cheat the system and obtain the credit when the defined condition is triggered. This is a feasible and effective attack method to systems based in traditional architecture because all components are supposed to be creditable and lack protection of the communication between any two components in these systems. However, in the new architecture in which all components have to be authenticated before they are added into the system, the Trojan Horse attacks become ineffective

even when the virus works properly. The communication channels can be built until the components on both sides are authentic and protected by encryption normally. Therefore, the data sent from Trojan Horse will not be accepted and recognized by any component in a system, which prevents potential Trojan Horse attacks and improves the security of the system. Furthermore, the data captured by Trojan Horses are also unreadable and meaningless for attackers.

The new architecture also stops another potential attack: replacing a component. The components in the biometric layer have to be verified before they compose a complete biometric authentication system. If one of them is substituted by another component that contains malicious functions used to attack the system, the system will not authenticate it and will fail to compose a biometric authentication system. For the components outside of the biometric layer, the check platform is responsible for forwarding the data packages that are normally protected by encryption and are exchanged between the central unit and components in the biometric layer, whose replacement does not affect the security of the system.

Attack detection becomes a possible feature. Because the multiple-factors authentication mechanism is implemented in the new architecture, the server can recognize the attacks from failure of the authentication. The failure derived from non-deterministic of biometrics only occurs in the biometric authentication operation taken after the system composing. Therefore, the attacks can be detected if there is any

false on authentication of the biometric components.

5.2 Privacy protection

The proposed architecture avoids the disclosure of pivotal data. The critical biometric data is kept in the biometric layer where the communication and components are protected completely. And the authentication result is encrypted and then submitted to the authentication server.

Another advantage of composed distributed architecture is that the information stored in the authentication server is changeable. In traditional architecture, the information used to verify the user and his or her identity is the biometrics that are constant since they were enrolled into the system. The stability degrades the security of the system and may cause the system unrecoverable failure. In the new architecture, the information in the authentication server is converted to the information corresponding to the results of biometric authentication occurring in the local platform. This information is not influenced by biometrics and can be changed due to strengthening the ability against the attacks. And the recovery of such a system based on the new architecture is much easier than in the current systems because the system does not need collect the biometrics again.

The new authentication mechanism does not store the template, a part of the user's

privacy, in the authentication server, and it prevents submitting the private biometric data to the authentication server during the authentication. Instead of the biometrics, the information stored in the authentication is the information associated with the biometric authentication results and can be changed on demand from the system. The mechanism enhances the privacy protection and the system security instantaneously.

Composed distributed architecture divides the biometrics from the architecture and makes management of the biometric controllable for the user. In the architecture, the critical privacy data and components are gathered in an independent layer that could be isolated from other components, which results in the self-management of the biometric-related components and data. Since the biometric-related components are extracted into one layer and obtain mobility, the users have the opportunity to conserve, manage, and update their biometrics and prevent the disclosure of their privacy.

5.3 System mobility and application flexibility

The layered structure provides the systems mobility that makes systems cart for different application environments. Differing from the traditional architecture, the biometric components in composed distributed systems don't rely on other components. They work as an independent system that attaches to a platform in the authentication process. Their independence separates the biometric authentication from the other components, so that the mobility is created. In the new architecture, it is

possible for users to carry the biometric components; for example, in a token, disk, or smart card.

Since systems based on the traditional architecture do not verify the biometric-related components, the components bind with the server and check platform to ensure their validities, which makes the systems inflexible. In the new architecture, the system is able to recognize and verify the biometric-related components without the location information, which is independent of where they reside; therefore, the biometric-related components have the ability of movement that makes the systems based on the new architecture flexible.

It gets much easier to merge different biometric authentication technologies into one system based on composed distributed architecture. In traditional architecture, centralized or distributed architecture, some shared biometric components, the matcher and template database, deprive users of the selection of different biometric technologies. In new architecture, the biometric components are in an independent layer that makes it possible for users to apply different biometric authentication technologies. And the reference in the authentication server is generalized to changeable information that is irrespective of the biometrics and their technology.

The mobility and flexibility enhance the application of the systems based on the new architecture in more environments. Without binding the biometric components,

more devices and systems, such as a mobile phone and a desktop, are selected as the check platform. The biometric-related components move among the check platforms according the users' activities. For example, there is an online-banking application that uses biometrics to verify the customer who is asking for services. Although mobility and flexibility cause the security problems as what contributes to the system, in the new architecture, the enhanced multi-factor authentication solves the problems and reinforced the security of the system.

5.4 Systems comparison

In this section, a system based on proposed architecture is compared with other popular biometric systems that are used to solve challenges. But it is hard work to compare systems without a standard.

5.4.1 Evaluation standard

For the biometric authentication system, multiple aspects are involved, and it is reasonable to score all aspects of the system separately. The evaluation standard includes three parts: the security evaluation, the privacy evaluation, and the usability evaluation.

The security evaluation scores the security related items for a system. Since security is the main goal for an authentication system, the item in the security

evaluation is the most important. The privacy evaluation focuses on the features related to the user's biometric samples. The end evaluation is the usability evaluation that assesses the performance and manageability of a system. For each evaluation item, the score ranges from 1 to 5, where 5 stands for the highest level or the best situation.

5.4.2 Candidate systems

The systems to be compared stand for the current trends of biometric authentication systems. To simplify the comparison, all systems are supposed to use fingerprints as the biometric method, which is the most popular and common in the real world.

The candidates include the centralized biometric authentication system, the system that uses liveness detection, the smart card-based system, the Bio-PKI system, and the system that is based on the proposed architecture. The system coordinating with the smart card attaches the sensor, stores templates, and matches in the card. The Bio-PKI system conserves the user and biometric certificates in a smart card and matches the captured sample in the server. For the system based on the proposed architecture, all biometric components are in a USB token and protected by an RSA key pair. According to these assumptions, the comparison can be reasonable and objective. The following is the system description and its code in comparison:

System A: the fingerprint authentication system using centralized architecture

System B: the fingerprint authentication system using centralized architecture and a liveness detection

System C: the fingerprint authentication system with the RSA key pairs and a smart card where the sensor locates, the templates store, and the matching process executes

System D: the fingerprint authentication system using certificates, matching on the server

System E: the fingerprint authentication system with a USB token that contains all biometric components, the sensor, the matcher and the templates. The biometric components are authenticated according the RSA key pairs. And internal communication channels are protected by a dynamic key.

5.4.3 Security evaluation

The security evaluation includes the following items: the authentication accuracy, the ability to detect attacks, security strength on bits, and immunity to possible attacks.

Since all systems are based on the fingerprint method, the accuracy is almost same in each system and the score in this item is the same for each candidate system. Except for the System A, all systems have the ability to detect attacks. The latter three candidate systems use a multi-factor authentication mechanism that has much better security strength than the systems A and B. Systems C, D and E are all based on the

public-private key algorithm, therefore, security strength are at the same level.

Immunity to attacks is the most important feature in the security evaluation. There are four common attack types that will be assessed, which are the spoofing biometric attack, channel attack, the Trojan Horses attack and the cryptanalysis attack. System C involves the smart card, which is commonly considered a secure method. But it is not absolutely secure, and there exists some attacks against it [18], which result in the degradation of system security. For the spoofing biometric attack, every system may be defeated, but the multi-factor authentication mechanism makes it harder to succeed as well as the function of a liveness detection. In systems C and D, the smart card contributes the secure platform and is the base of the immunity. All communication channels in system E are fully protected by keys, whereas only some of them are protected in systems A and B. And in systems C and D, the smart card keeps some channels secure. Immunity is not derived from the system but from the smart card; therefore, it is not as strong as in the system E. Trojan Horses attacks can conquer systems A and B easily but are ineffective to system E. In systems C and D, if the biometric components appear out of the smart card, Trojan Horses attacks can be successful. The last kind of attack is the cryptanalysis attack, which depends on the weakness and dynamics of the keys used in the system. System E employs the dynamic keys and RSA key pairs that are strong enough to prevent cryptanalysis attacks.

	A	B	C	D	E
Accuracy	3	3	3	3	3
Security strength	1	1	5	5	5
Attack detection	1	5	5	5	5
Immunity to spoofing biometrics	1	4	4	4	4
Immunity to channel attacks	1	1	4	4	5
Immunity to Trojan Horses attacks	1	1	4	3	5
Immunity to cryptanalysis attacks	1	1	3	3	5
Subtotal 1	9	16	28	27	32

Table 5.1 Security Evaluation

5.4.3 Privacy evaluation

In this section, the privacy protection of each system will be assessed. The evaluation considers the critical data transferring, credential representation, templates location, and system recovery.

The candidate systems A, B, and D submit the biometric samples to the authentication server, which may cause privacy disclosure. The credentials used to prove the user's identity is another factor in privacy protection. In systems A, B and D, the credentials are the biometrics, whereas the biometrics are hidden in systems C and E. The templates are also critical in the biometric authentication system, thus the

storage location influences the privacy protection evaluation. Users prefer the self-management on the template that stands for their own privacy.

	A	B	C	D	E
Transmission	1	1	5	1	5
Credential representation	1	1	5	2	5
Template location	3	3	5	3	5
Subtotal 2	5	5	15	6	15

Table 5.2 Privacy Protection Evaluation

5.4.4 Usability evaluation

The usability evaluation considers the usage, performance, and economy features of a system. The usage includes the management, mobility, and assistance requirement. The mobility that allows people to use the system from place to place emerges in systems C, D, and E. Systems A and B limit the location the user can use. In system D, a trusted third part is needed, which increases the complexity of the system. And in systems C and D, the smart card is the major source of system security.

Another aspect for users is convenience. The less actions the authentication needs, more convenient the system usage is. Unlike other systems, in system C, the smart card-based candidate, usually a password for accessing the smart card is needed. And in systems D and E, the multi-factor authentication systems, certificates or a token are

needed to attach to the client, which is an extra action than the simple biometric authentication systems do not have.

	A	B	C	D	E
Mobility	1	1	5	5	5
Assistance requirement	5	5	3	1	4
Convenience	5	5	2	4	4
Cost	5	4	2	1	3
Available system resources	5	5	2	5	5
Sub total 3	21	20	14	16	21

Table 5.3 Usability Evaluation

Other concerns are the economy and system resources. Multi-factor authentication systems usually are more expensive due to the added security mechanisms. In the candidate systems, systems C and D score low due to the high price of the smart card. Available resources refer to the resources that the system can use. This includes computational ability and storage space. For the candidates, most of them utilize the client or the server resource, which is enough to perform the necessary operations. Only system C has low system resources because it performs the matching on the card, which has limited resources. This lack of resources may deny some biometric methods that need more computation and storage space yet have better performance and security at the same time.

5.4.5 Synthesis evaluation

The total score for each candidate is shown in the flowing table. System E, which is the system based on the proposed architecture, has the highest score, 68, out of 75. The comparison also shows that the proposed architecture is a good synthesis solution that makes the system satisfy the multiple challenges.

	A	B	C	D	E
Security evaluation (Subtotal 1)	9	16	28	27	32
Privacy protection evaluation (Subtotal 2)	5	5	15	6	15
Usability evaluation (Subtotal 3)	21	20	14	16	21
Total scores (over 75)	35	41	57	49	68

Table 5.4 Total Evaluation

Chapter 6: A Token-Based System Prototype and Protocols

6.1 Introduction

In this chapter, a biometric authentication system scheme based on the new system architecture mentioned in the last chapter is proposed. In the proposed authentication system, the token is issued to a user and the system maintains the biometric-related parts that are used to perform biometric authentication to verify the token holder. The keys represent the credentials in the new system architecture, which is used to establish secure communication and verify the biometric-related components.

6.2 Application and environment

The token-based biometric authentication system can be applied in applications that will work in a network environment where the platform computers and server are connected together and work to provide services to users. The system also provides high security to the applications that are deploying the authentication system to prevent various attacks. For example, online banking service applications work in a network environment and transmit critical data via the Internet between the user's computer and the server in the bank. The token-based biometric authentication system can be used to verify the user, who requests certain services, and to keep the application system secure.

6.3 System and elements

In the token-based biometric authentication system, there are three elements – the authentication server, the user's token and the client computer. According to the new architecture, the components in the biometric layer are represented by the programs that implement the specified functions, stored in the user's token, verified by keys issued to each component in the biometric layer, and used to establish secure communications, as shown in figure 6.1.

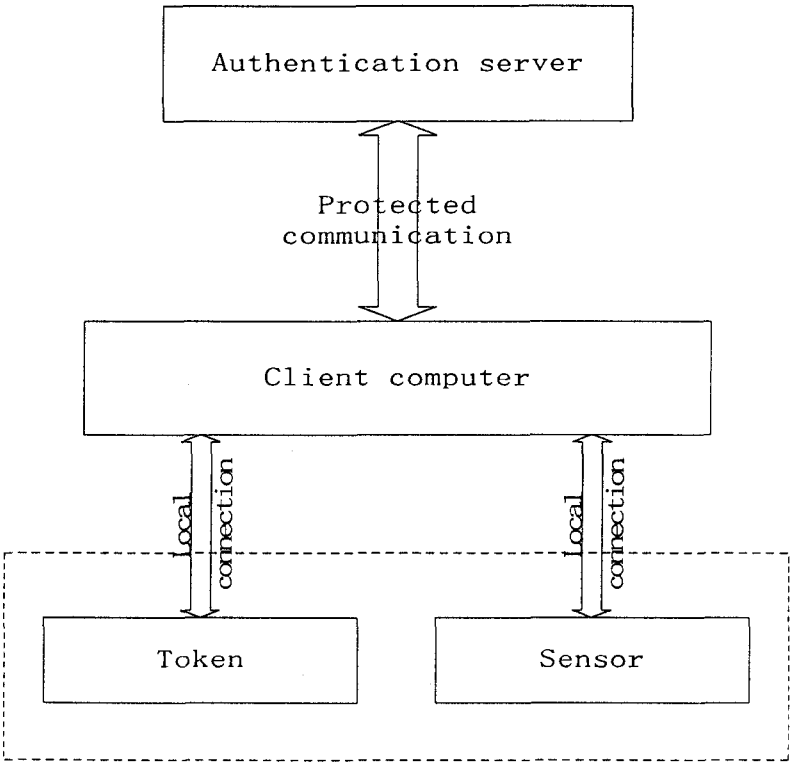

Figure6.1: System elements and connections

6.3.1 Authentication server

The authentication server is responsible for storing reference information for user authentication, communicating with client computers via networks, controlling the authentication process, and verifying the components and the user's identity, displayed in figure 6.2. Moreover, the server generates the key pairs for the user's biometric-related components that have to be verified before they are used as part of a complete biometric authentication system in the client computer and symmetric keys for channel encryption purposes. Therefore, based on the functions in the authentication server, three auxiliary components – the key generator, the reference database, and the communication management program – work with the authentication management program to deal with authentication requests from client computers.

The key generator produces not only the key pairs for biometric components but also the random key for temporary usage in secure communications. The generated key pairs are stored in the database as reference information for biometric components and are used to verify these components before the biometric authentication system is composed. It also generates the random and temporary symmetric keys on demand upon the establishment of the secure communications.

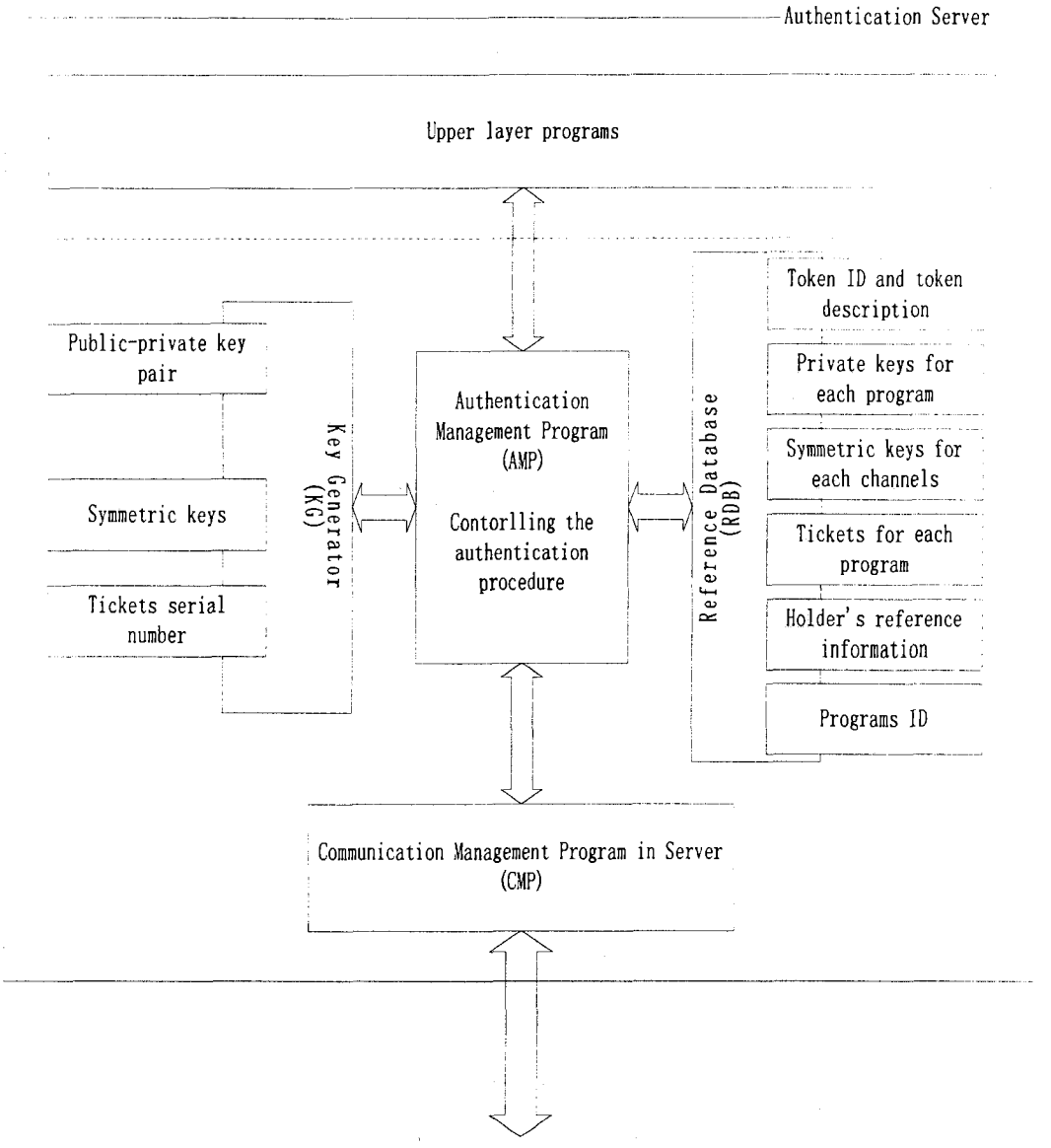

Figure6.2: Illustration of authentication server

All information related to the authentication process is stored in the reference database that also provides the storage space for the temporary data when the authentication management program deals with the authentication requests. The data in this database includes the user's identity, token ID, biometric components ID (Program ID), private keys associated with the biometric components, and the

authentication reference information. During the authentication procedure, some temporary information, such as the symmetric keys and communication tickets to the biometric components, is generated and stored in the reference database until the end of the authentication. Since the system verifies the token and the biometric components at first by submitting the information about the token, the data in the reference database is organized by the possession relationship, which means that, in the database, the token ID is the key and the index data that can retrieve other related information. Like the private keys, some information in the database could be updated when they are used for a period of time and become insecure.

The communication management program is responsible for dealing with the communication requests, building up communication, controlling the communication channels' states, and exchanging data. It implements the protocols below the application layer and monitors the resource usage of the server. The communication management program will close the service when there are not enough resources to deal with more communications. All communications to the client computers or the biometric-related components are in secure mode, which is implemented by the public-private key encryption mechanism and symmetric encryptions that decrease the resource consumption.

In the authentication server, the authentication management program is the vital role of the whole the system. It controls client and biometric component enrollment,

user identity verification, and the management and maintenance of reference information, which incurs access and information updates in the reference database where the user-related and token-related information are stored. It also works with the key generator and communication management program to provide the secured communication channels for the data that they convey.

6.3.2 Client computer and user token

Client computers, shown in figure 6.3, are just the resource providers in the system and are not involved in the authentication processes. In the token, there is no memory, CPU, or network interfaces, which are necessary for the programs' execution in the network environments. Therefore, the programs in the token need a platform that provides the resources for them, in which the platform is the client computer in this system. The copies of programs from the token run in the client computer what the token has attached and utilize the resources from the computer, saving the data in the memory, computing via the CPU, and accessing the Internet via the network interface, to complete the authentication procedure. When the token leaves the client computer or the authentication terminates, and all resources used by the biometric-related programs are released.

The user's token is created and issued to a user after the user information, token information, and biometric component information has been enrolled into the

authentication server. The token contains the system-defined unique token information, which is used as proof to verify itself and a series of executable files, in which each file represents the program of the biometric related components -- matcher, template management, and sensor.

The system confers upon each token a unique token ID that is also saved in the authentication server, where the ID is used to identify the token and is treated as the index to retrieve the information associated with the token from the reference database. As the ID, the token description is created by the server and depicts the token in text. The token ID and token description are stored together and are accessible for the matcher program that is the primary program in the token and that starts the communications to the authenticate the token with the ID and description.

In the token, each biometric component program contains a public key that is issued by the authentication server in the enrollment stage and implements the protocols used to communicate with the authentication server. On the authentication server side, the private key associated with the public key in the token is kept in the database that is retrievable by the token ID and is deployed in the process to verify the biometric component. The protocols utilize the public-private encryption mechanism to authenticate each other. Another kind of protocol applied internally between the biometric components in the client computer is also implemented in these component programs, which combines the components together, conveys the data, and makes all components work as a biometric authentication system.

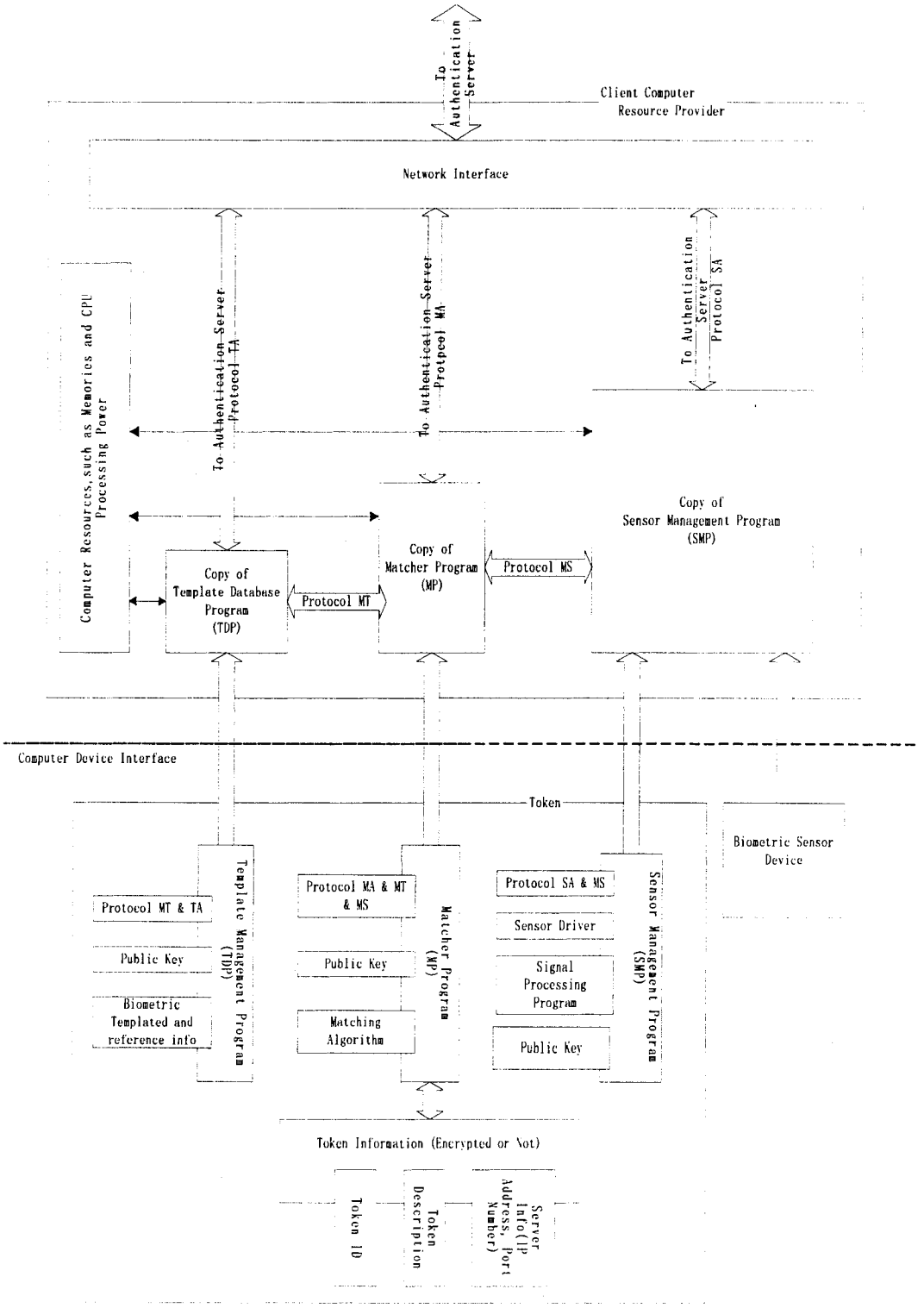

Figure6.3: Illustration of client and user's token

Besides the public key and the protocol implementations, each program contains functional data that depends on the program's function definition. The matcher program is defined to compare the incoming biometric samples with the stored templates, which results in the implementation of a matching algorithm in the program. The program that represents and manages the template management includes the biometric templates and their extended information, which is used to verify the user who provides the biometric sample. In the sensor management program, there is a functional part that controls and manages the attached sensor, which is treated as a sensor device driver that captures the biometric sample from the token holder.

6.4 Protocols and data format

In the system, only the application layer protocols that are designed to control the authentication in the secure mode are defined. These protocols are applied on internal communications and the communications between the biometric components and authentication server. Since the client computer only provides the necessary resources to the biometric-related programs, it will not involve itself in the authentication process, and there is no application communication between the client computer and any other element. According to the system architecture, the protocols are named as follows:

Protocol Name	Description
MA	The application protocol applied in the communication MA that is between the authentication server and the matcher program in the token
TA	The application protocol applied in the communication TA that is between the authentication server and the template management program in the token
SA	The application protocol applied in the communication SA that is between the authentication server and the sensor management program in the token
MT	The application protocol applied in the internal communication MT that is between the matcher program and the template management program
MS	The application protocol applied in the internal communication MS that is between the matcher program and the sensor management program

Table 6.1 Communication Protocols

All application protocols protect the transmitted data by the encryption mechanism, asymmetric and symmetric modes. Because of the larger resource consumption, the public-private keys are used to authenticate the component programs and protect the assigned symmetric keys. The symmetric keys are utilized to encrypt

the data in the channels after component authentication. They are all generated by the server and are applied to protect future data exchange in the communications that connect the biometric component and the authentication server. In the internal communications, the keys are created in the authentication server too, and the biometric component programs on the both sides of the channel are notified of this.

6.4.1 Data format

The data format in these protocols is TLV, which defines a data in three fields – tag, length and value. The tag field defines the data type in the value filed; the length filed indicates the length of the data filed in byte. A PDU (protocol data unit) may contain several data defined by the protocol and a checksum that occupies two bytes at the end of the package.

Tag (1 byte)	Length (2 bytes)	Value (indicated by length)

Table 6.2 TLV Format

Data 1	Data 2	.....	Data N	CRC (16bit)

Table 6.3 PDU Format

6.4.2 Ticket data format

A ticket is a temporary credential produced by the authentication server to access the communication channels. When a component sends a message to another component via the internal channels or the server, the receiver has to verify the ticket at the head of the data packet.

Ticket serial Number (8 bytes)	Server Signature (16 Bytes)	Time stamp (8 bytes)	Duration (2 bytes)

Table 6.4 Ticket format

6.5 Authentication processes

6.5.1 Public key authentication

The system uses public key authentication for strong and secure authentication in the biometric component process. The authentication method utilizes asymmetric encryption to exchange information and verify the user and his or her identity.

Unlike symmetric encryption, asymmetric encryption uses a key pair to encrypt and decrypt messages. There are two keys in a key pair, a private key and a public key. A private key is kept by one entity in a secure and secret place and is not revealed to

others. A public key is the accompanying key to the private key and is spread to other entities that will communicate the private key holder. There are some important features of the key pair [31]:

(a) The key messages encrypted with the public (private) key can be decrypted only with its private (public) key.

(b) It is impossible to figure out the private key using the public key.

In the system, the public keys reside in the authentication server and are kept as secret as the private keys, and only the server owns the public keys. Therefore, the keys indicate the unique and valid entity in the authentication procedure. During the authentication in the system, a one-way hash function is used to generate the digest that indicates the entity to be authenticated. The function hides the secret and prevents tempering and spoofing attacks against the system. The digest is encrypted by the sender and verified by the receiver to perform component authentication.

6.5.2 Programs authentication and communication establishment

6.5.2.1 Principles

Although the protocols may vary in different environments and applications, some authentication principles should be applied in every authentication protocol.

In a protocol for authentication, there should be a mechanism that makes each

component verify the validity of the other side of the communication channel. The authentication server and the programs in the client computer verify each other by matching the shared secret that includes the key and the token description. If a program can recognize the encrypted information from the server and provide the required secret shared in enrollment, it is treated as an authenticated program. In addition to the biometric program, the authentication server is verified when it decrypts the message from a program correctly and sends the shared secret back.

In the protocols applied in the system, some temporary information is involved in the authentication processes. The information is used as the tags for the data exchanged in the communication channels and verifies the side where the temporary information is generated. In this system and its protocols, the temporary information, including the tickets and symmetric keys, is produced in the authentication server.

6.5.2.2 Authentication process

The authentication procedure starts when a user attaches a token to a client computer where there are enough resources to run the programs from the token and the copies of the biometric-related programs execute in the client computer. The token has to be verified at first before the biometric components are used, and it relies on the matcher to perform the verification. The matcher program is invoked after the token is connected to the client computer and tries to connect to the server using the network interface provided by the client computer after the program collects the necessary

information, such as a token ID, server address, and port number. It sends the text message "Hello" to awake the authentication server and waits for the response that indicates the existence of the service. At the same time, the matcher program sets a timer that controls how long the program will wait for the response. The authentication server returns the text string that describes the status of the server, ready, busy, or unavailable. If there is no response received until the timeout is triggered, the matcher program will close the connection automatically.

M → A: "Hello"

A → M: "Ready" / "Server busy" / "Service unavailable"

When the program obtains the response message of "Ready" from the server, the authentication continues to verify the matcher program by sending the plaintext token ID. In addition to the ID, the digest of the token description and matcher program ID encrypted by the private key of the matcher program are submitted to verify the validity of this token and its ID. The authentication server decrypts the token digest and matcher program ID and checks them with the stored information retrieved by the token ID. If the submitted information is recognized by the server and matched to the stored reference, the token and the matcher program are successfully verified. The authentication server then generates a ticket for the matcher program and two symmetric keys, SYMK1 and SYMK2, for future communication with the matcher program. They are then encrypted and sent to the matcher with the digest of the token description.

M → A: {Token ID & {Digest(Token Description) & Matcher Program ID}MatcherPrv }

A → M: {Tickets for Matcher program & SYMK1 & SYMK2 & Digest(Token Description) }MatcherPub

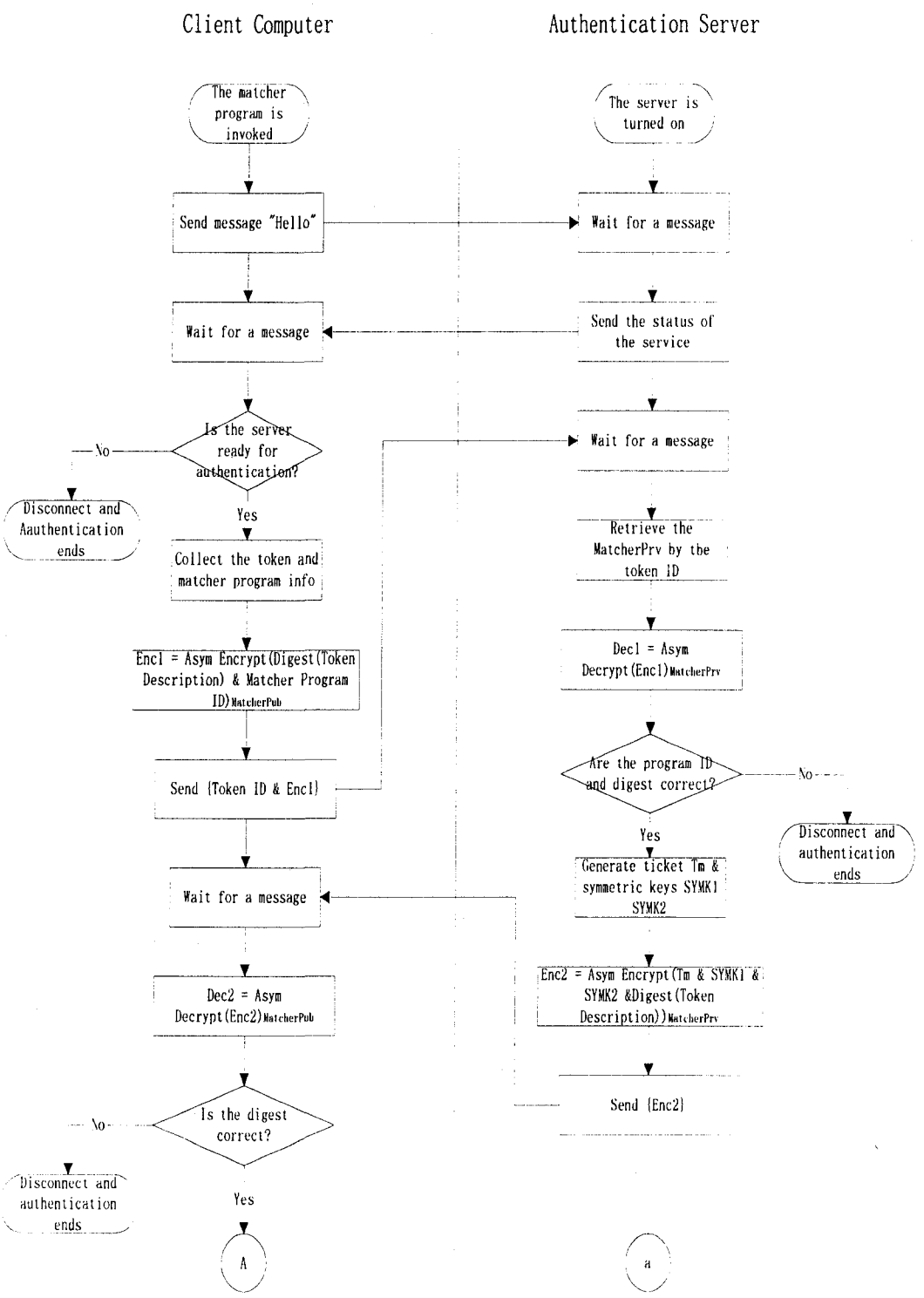

Figure6.4: Program authentication process part 1

The matcher program obtains the tickets and the encryption key for the future

communication when it successfully decrypts the response message from the authentication server using the public key. This transaction makes the server and the token trust each other by using the public-private key encryption mechanism and checking the shared information – the digest of the token description and matcher program ID.

The matcher program invokes the authentication process of the template management program and the sensor management program by passing the encrypted tickets that indicates who activated the programs. The program authentication is similar and starts when the program sends the encrypted messages that contain the encrypted ticket from the matcher program and their program ID. The responses are tickets and the symmetric key for the internal communication channels where the data is exchanged in the client computer. In these transactions, the authentication server and the biometric programs verify each other using the public-private key encryption mechanism. Moreover, the encrypted matcher program ID proves the relationship between the matcher program and each of the two programs. After the authentication process, the two programs send their encrypted tickets to the matcher program, which is ready to retrieve the channel encryption key.

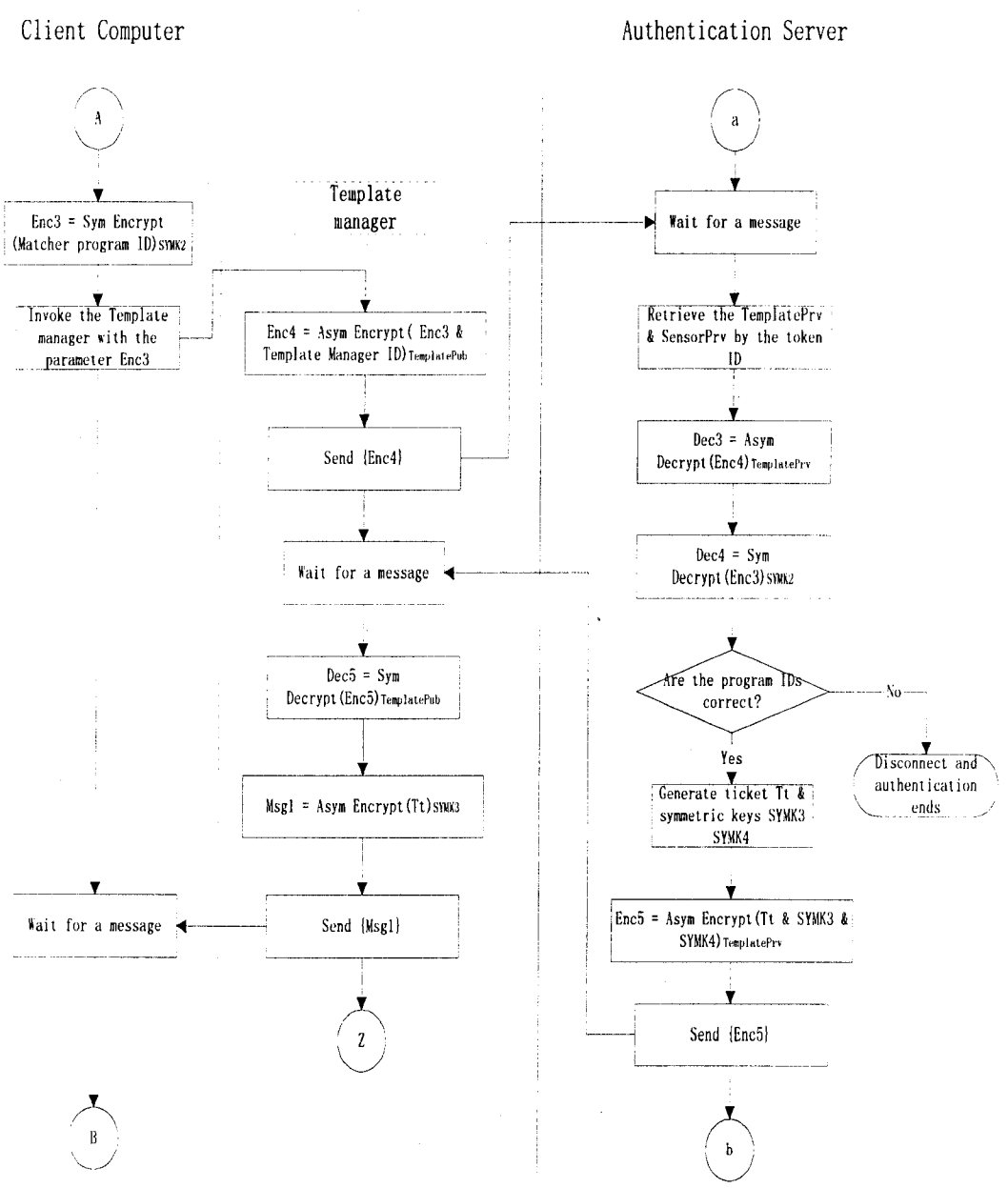

Figure6.5: Program authentication process part 2

T → A: {{Matcher program ID}SYMK2 & Template management program ID}TemplatePrv

A → T: {Ticket for the template management program & SYMK3 & SYMK4}TemplatePub

T → M: Msg1 = {Ticket for the template management program}SYMK3

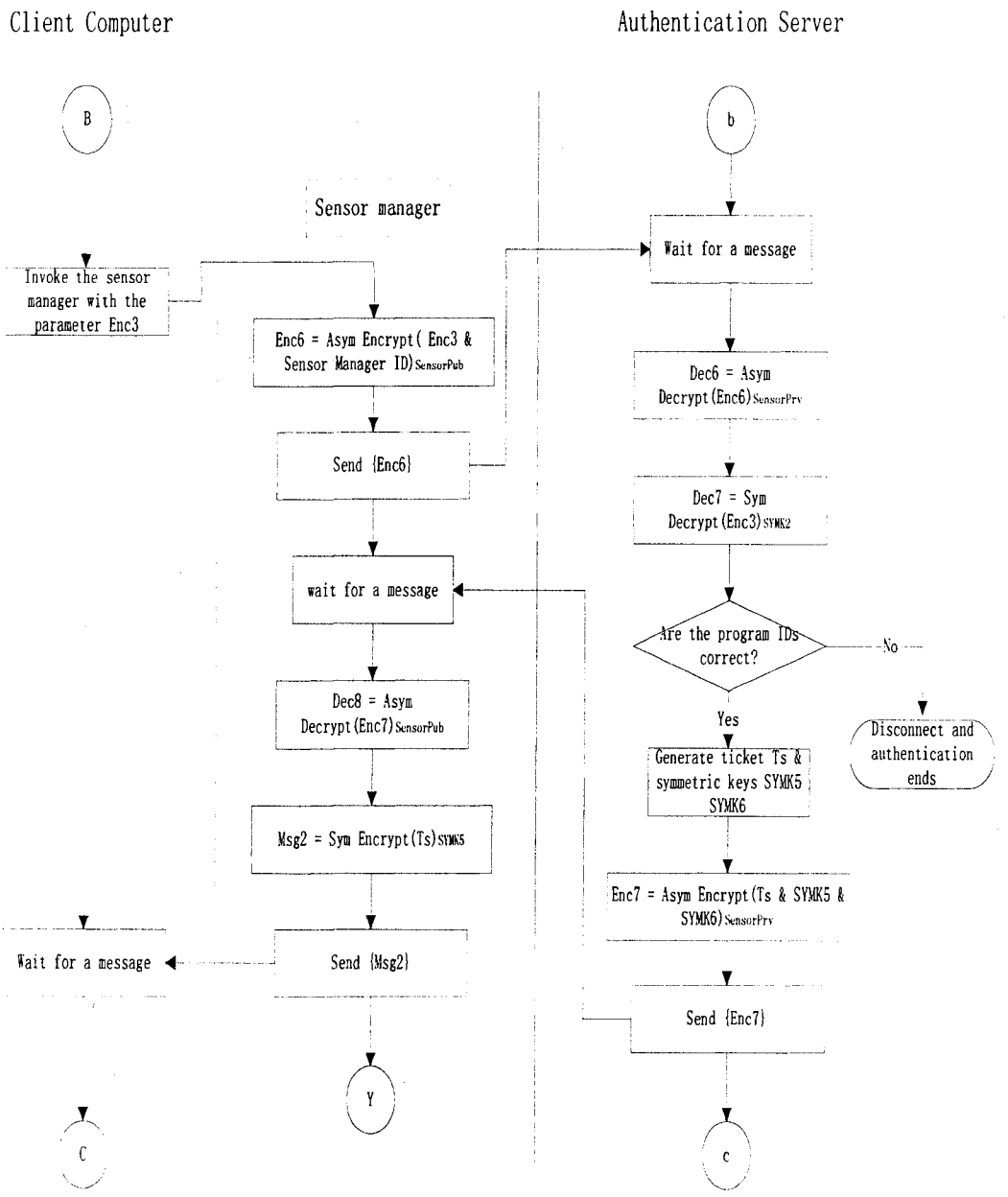

Figure6.6: Program authentication process part 3

S → A: {{Matcher program ID}SYMK2 & Sensor management program ID}SensorPrv

A → S: {Ticket for the Sensor management program & SYMK5 & SYMK 6}SensorPub

S → M: Msg2 = {Ticket for the sensor management program}SYMK5

The matcher program obtains the encrypted tickets of the other two programs, and transmits them to the authentication server with its own ticket. The message ensures that the necessary and proper components are combined together and are ready to build up the communications. That response from the authentication server is a new ticket for the biometric authentication results and the channel encryption keys used to protect the internal communications channels – MT and MS.

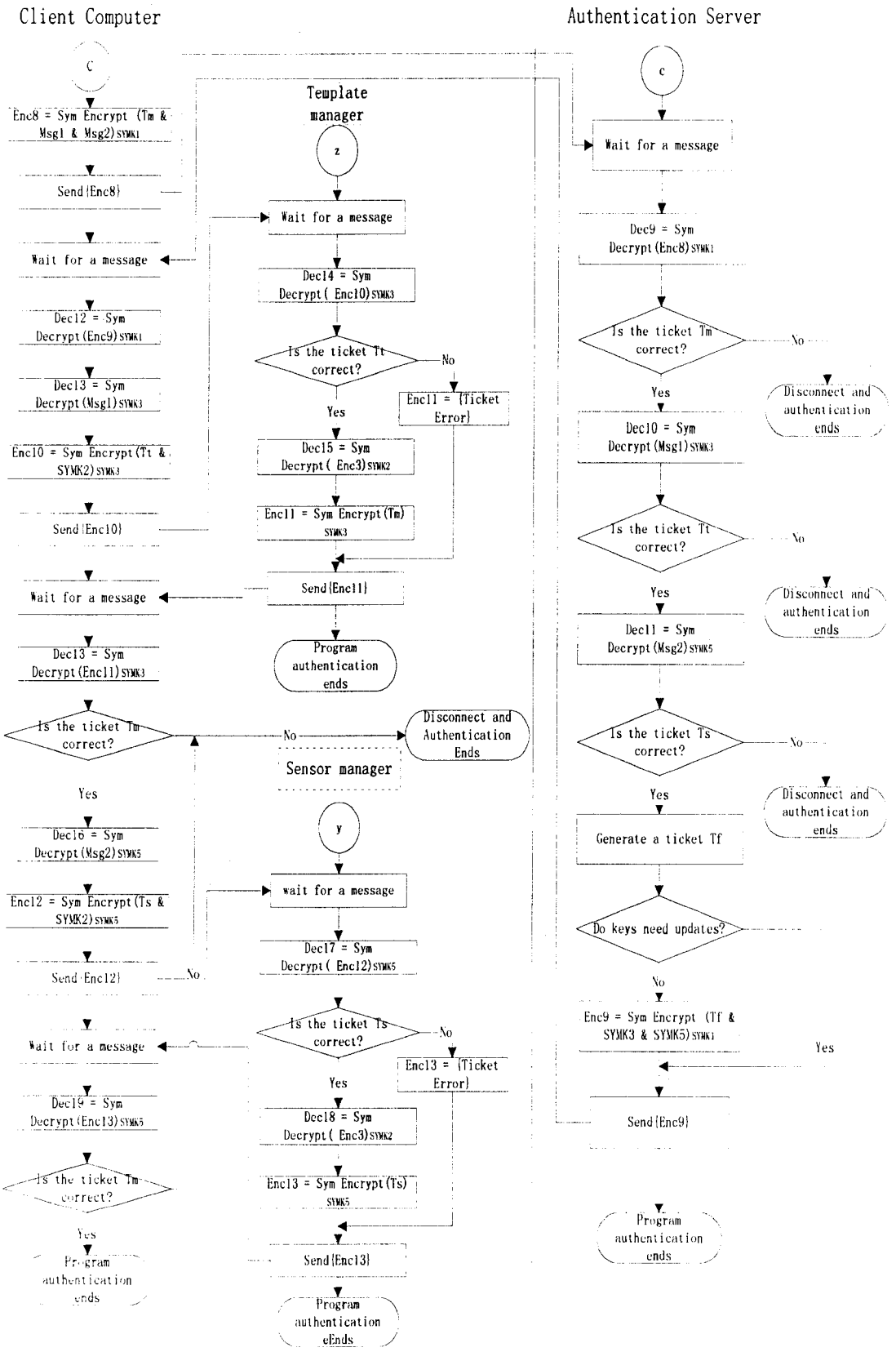

FIGURE6.7: PROGRAM AUTHENTICATION PROCESS PART 4

M→ A: {Ticket for the Matcher program & Msg1 & Msg2}SYMK1

A → M: {Ticket for the final result & SYMK3 & SYMK5}SYMK1

The returned channel encryption keys help the matcher program to establish the connections with other two programs, in which the data in the channels are encrypted and are only recognized by the program that has the same encryption key. Until this transaction, the channel keys are distributed to all programs and the last step in the components authentication process is to create the internal communication channels using these keys.

M → T: {Ticket for the template program & SYMK2}SYMK3

T → M: {Ticket for the matcher}SYMK3

M → S; {Ticket for the Sensor management program & SYMK2}SYMK5

S → M: {Ticket for the matcher}SYMK5

6.5.3 Biometric authentication and internal communications

The following phase after the component authentication and key exchange in the authentication procedure is to verify the token holder's identity using the local biometric authentication system. At the beginning of the biometric authentication that occurred in the client computer, the internal communication channels where the

biometric related data is conveyed to the matcher program are established. The matcher program compares the captured biometric sample from the sensor management program with the templates from the template management program via the secured internal communication channels until a proper one is found or they are not coincident.

6.5.3.1 Internal communications

In the system, there are two internal communication channels that connect two biometric components in the client computer. When the token and biometric components are authenticated, the channels are responsible for delivering the data to the matcher from the other two components.

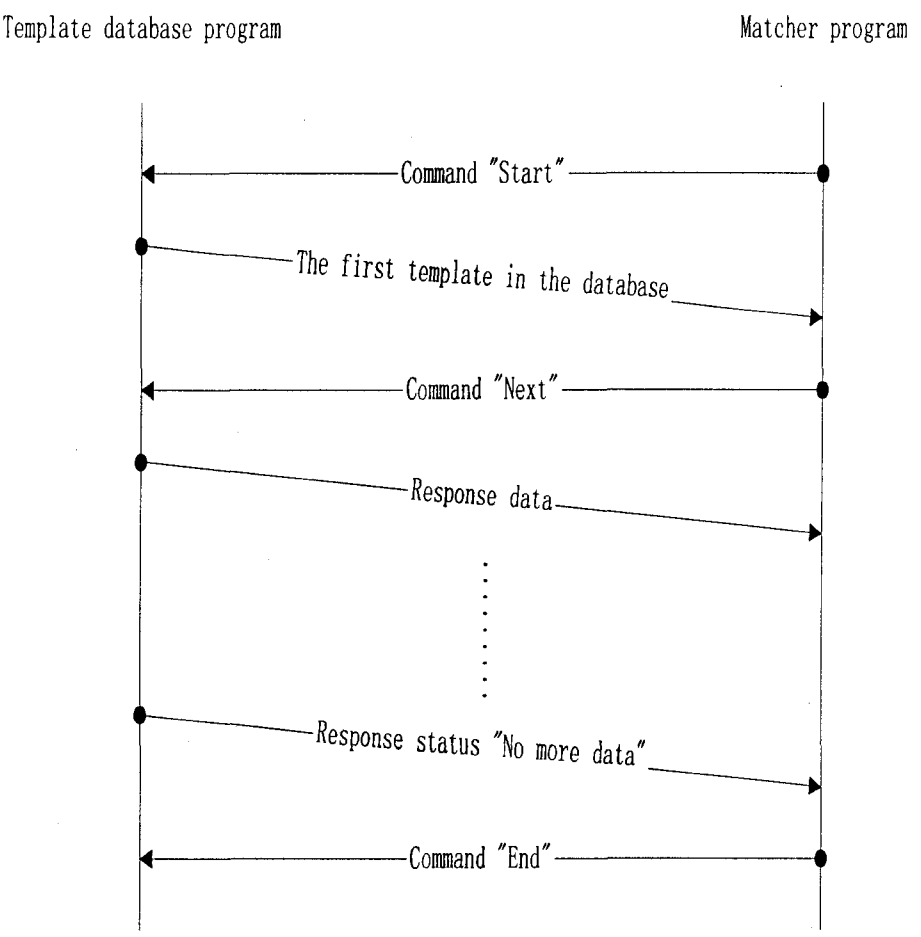

Figure6.8: Transactions in the biometric authentication process part 1

Communication channel MT is located between the matcher program and the template management program and is responsible for delivering the stored templates upon the demand of the matcher program. When the incoming biometric sample is recognized and is matched to one of the stored templates, the matcher program requests the matched template's reference information, which is also transmitted via communication channel MT. As a result, protocol MT that is applied in communication channel MT is based on the request-response mode, and the matcher program generates a request to a template and the template management program

returns the corresponding data, template, or reference information.

The matcher program asks for the first template by sending a PDU (protocol data unit) with the command "Start" when the biometric authentication begins. If the matcher program needs more templates, the command of "Next" is submitted to the template management program to obtain another template. The data exchange process terminates in two cases – the matcher program found a matchable template, or the matcher program could not find a matchable one until all templates had been tried. In the first case, when the matcher program finds a proper template successfully, the template program provides the extended information of the suited template to the matcher program as the response to the command of "OK". In the second case, the biometric authentication fails, and the matcher program ends the template request after it receives the reply that indicates that no more templates can be transmitted.

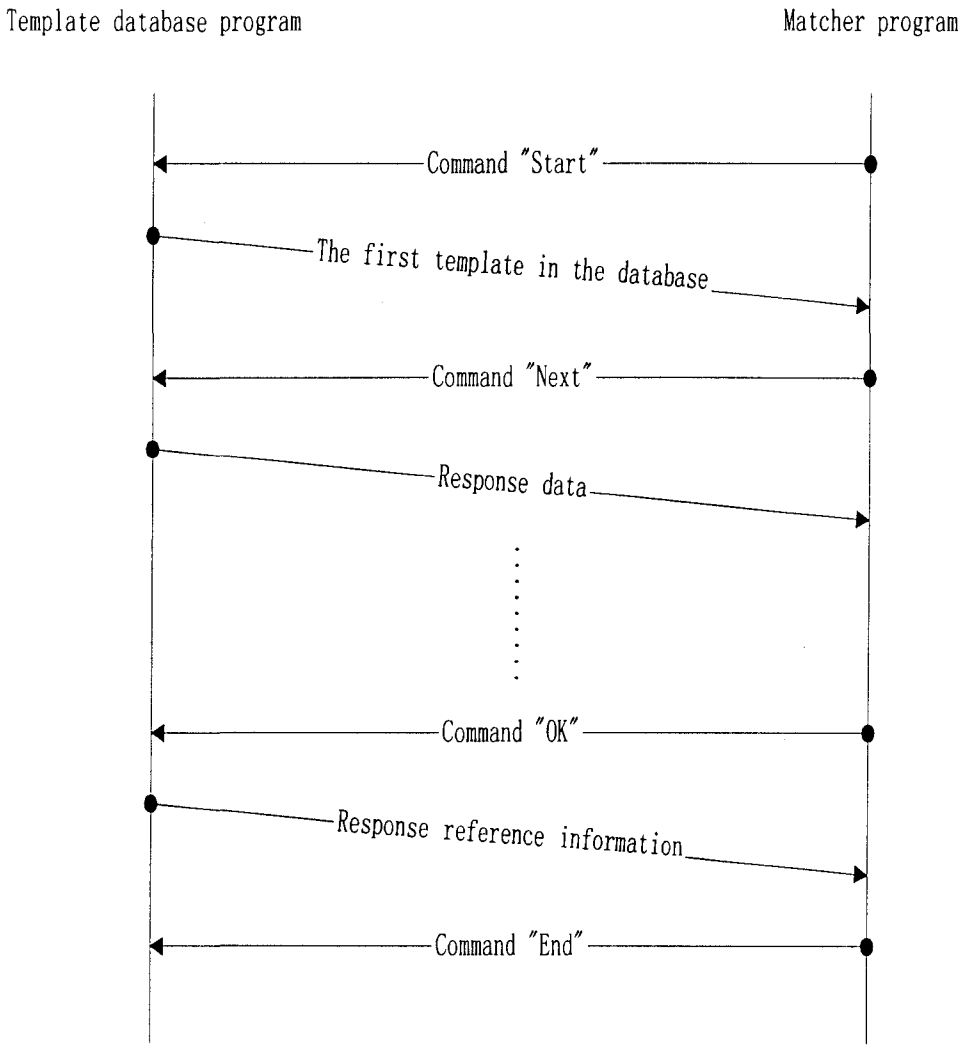

Figure6.9: Transactions in the biometric authentication process part 2

Another internal communication channel, MS, is designed to deliver the captured biometric sample from the sensor to the matcher program. It has a data exchange process that is similar to the process in communication channel MT, except that only one biometric sample is provided by the sensor management program. The data exchange originates with the "Start" command from the matcher program and ends in

the sensor management program's response, which is the data stream or the status of the program.

6.5.4 User authentication

The last stage in the authentication procedure is to verify the information on the user who has provided the biometric sample and succeeds in being authenticated by the internal biometric authentication system in the client computer. The matcher program submits the extended information obtained to the authentication server, where the information is compared with the stored reference. The comparison results lead to the termination of the authentication procedure and affect the resource accessibility and service availability to the user who holds the token and presents his or her biometrics.

M → A: {Ticket for the reference information, {reference}SYMK4}SYMK1

A → M: {Finish}SYMK1

The reference is encrypted by the symmetric key distributed in the component authentication process and is sent with the ticket. The returning message "Finish" indicates the authentication server has obtained the reference and the authentication procedure is finished. The matcher program releases the resources admeasured to all biometric-related programs in the client computer.

6.5.5 Key update

Since time makes the keys insecure, the keys assigned to each biometric program have to be updated after a period of usage. The attackers cryptanalyze the captured data that is protected by the keys to obtain the plaintext, but the process takes lots of time. Therefore, encrypted data transmitted via the communication channels is less secure when the keys to the channels have been used for a while. It is necessary to update the keys so that new keys can recover the high security of the communication. Only the public-private key pairs for the biometric programs need to be updated because the symmetric keys are generated and maintained during the authentication procedure.

The authentication server decides whether the keys should be updated or not when it receives the last message from the matcher program in the biometric program authentication process. The response may contain the new public keys for each biometric program and encrypt the public keys using the distributed symmetric keys respectively.

M→ A: {Ticket for the Matcher program & Msg1 & Msg2}SYMK1

A → M: {Ticket for the final result & SYMK3 & SYMK5 [& {New public key for matcher}SYMK2 & {New public key for template manager}SYMK4 & {New public key for sensor manager}SYMK6]}SYMK1

If the matcher program receives the response containing the public keys for

updates, it dispenses the keys to a corresponding program that can decrypt new public keys correctly. The new public keys are sent to the template manager and the sensor manager after the internal communications has been established.

M → T: {{New public key for template manager}SYMK4}SYMK3

T → M: {{Result of Update}SYMK4}SYMK3

M → S; {{New public key for sensor manager}SYMK6}SYMK5

S → M: {{Result of Update}SYMK6}SYMK5

The matcher submits the collected results of the updates to the authentication server and waits for the response message that makes the internal biometric authentication start.

M → A: {{Update result of matcher}SYMK2 & {Update result of template manager}SYMK4 & {Update result of sensor manager}SYMK6}SYMK1

A → M: {Updates Finish}SYMK1

Chapter 7: Conclusion and Future Works

7.1 Conclusion

In this thesis, the composed distributed architecture (CDA) is proposed. Compared to traditional architecture, the proposed architecture enhances performance in the aspects of security, privacy protection, and usability. The new architecture is the synthesis method to resolve the challenges that biometric authentication systems have to face. The most important enhancement to system performance is the improvement of system security, as the CDA prevents widely used attacks and threats effectively, according to the analysis. It also has mechanisms to protect the user's biometric information and provides convenience of usage, maintenance, and management of the systems. Therefore, it provides a flexible framework for biometric authentication systems with high security, reliable privacy protection, and convenient usability.

A scoring system is used to measure the performance of a system when it is hard to find a quantitative method to evaluate the system. The scores on vary biometric authentication systems shows that a system based on the CDA has the best performance in each aspect and in the total evaluation, which is compared to commonly used and newly developed biometric authentication techniques and systems.

The system design of the application in this thesis is a sample that represents how to design a biometric authentication system according to composed distributed

architecture. And the system prototype design and the protocol design prove That it is possible to implement a system that utilizes the proposed architecture.

7.2 Future works

Although this thesis provides a system prototype based on the token, the future work is to design more systems that are based on the proposed architecture, have various platforms, and use different security techniques. The architecture achieves security on a systemic level, and the production designs need more attention to the details of the system to avoid degradation of the system security.

References

[1] Patrick McDaniel, "Authentication", AT&T Lab - Research, May 31, 2002

[2] M. Bishop, *"Authentication"*, chap.12 in Computer Security, Boston, MA: Addison-Wesley, 2003

[3] Claus Vielhauer, *Biometric User Authentication for IT Securiyt: From Fundamentals to handwriting*, New York: Springer, 2006, pp. 11-33.

[4] Richard Duncan, "An Overview of Different Authentication Methods and Protocols", SANS Institute, 2000

[5] "Introduction to Public-Key Cryptography" [Online], Sun Microsystems, Inc., Oct 1998, available from World Wide Web: http://docs.sun.com/source/816-6154-10/contents.htm#1051881

[6] "Biometrics" [Online], National Institute of Standards and Technology, Jun. 2002, available from World Wide Web: <http://www.nist.gov/srd/biomet.htm>

[7] Jamee.L. Wayman(Ed.), "Collected Works Version 1997 – 2000", National Biometric Test Centre, San Jose State University, August. 2000

[8] Julian Ashbourn, *Biometrics: Advanced Identity Verification*, London: Springer, 2000

[9] Emma Newham, Calum Bunney, Carolan Mearns, *The Biometrics Report; SJB Services*, Langport, UK 1998

[10] "Biometrics Market Report 2003-2007" [online], International Biometrics Group, 2002, available from World Wide Web: http://www.biometricgroup.com/reports/public/market_report.html

[11] Anil K. Jain, Arun Ross, Salil Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, Vol. 14, No. 1, January 2004

[12] Václav Matyáš and Zdeněk Říha, "Biometric Authentication – Security and Usability", Masaryk University Brno, Czech Republic, 2002

[13] J.L. Wayman, "Technical Testing and Evaluation of Biometric Devices", chap.17 in *Biometrics – Personal Identification in a Networked Society*, by Anil K. Jain(Editor), Ruud Bolle, Sharath Pankanti, Kluwer Academic Publisher, 1999

[14] Nanavati, Samir, *Biometrics: Identity Verification in a Networked World*, New York: Wiley Computer Publishing, 2002

[15] Diana Kalenova, *Personal Authentication Using Signature Recognition*, Laboratory of Information Processing, Lappeenranta University of Technology

[16] A.Ross, A.K. Jain, "Multimodal Biometrics: An Overview", in *Proc the 12th European Signal Processing Conference*, Vienna, Austria, 2004

[17] R. Frischhholz, U.Dieckmann, "BioID: A Multimodal Biometric Identification System", *IEEE Computer*, Vol. 33, No. 2, 2000

[18] Luca Bechelli, Stefano Bistarelli, and Anna Vaccarelli, "Biometrics authentication with smartcard", Istituto di Informatica e Telematica (IIT), CNR Pisa, Italy, 2002

[19] "Introduction to FIU-810 Fingerprint Token" [online], SONY Corp, available from World Wide Web:

http://b2b.sony.com/Solutions/subcategory/security/biometrics/Fingerprint_Identity_Token

[20] "Introduction to BioPass3000" [online], RS-Computer, Langenhagen Germany, available from World Wide Web:

http://www.rs-computer.com/hardware_e/usb-security-token/biopass3000.php

[21] Yoshiaki Isobe, "ISO/IEC JTC 1/SC 37: Request for Comments on Telebiometrics System Mechanism", ITU-T Study Group 17, Moscow, 2005

[22] S.Y. Kung, M.W. Mak, S.H. Lin, *Biometric Authentication – A Machine Learning Approach*, New Jersey: Prentice Hall, 2005

[23] N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing the security and privacy in biometrics-based authentication systems", *IBM systems journal*, VOL 40, NO 3, 2001

[24] Ileana Buhan, Asker Bazen, Pieter Hartel, Raymond Veldhuis, "A False Rejection Oriented Threat Model for the Design of Biometric Authentication Systems", presented at Advances in Biometrics, International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006

[25] U. Uludag and A.K. Jain, "Attacks on biometric systems: a case study in fingerprints", in *Proc. SPIE-EI 2004*, San Jose, Canada, January 18-22, 2004, pp. 622-633.

[26] P. Tuyls, E. Verbitskiy, J. Goseling, D. Denteneer, "Privacy Protecting Biometric Authentication Systems: An Overview", Philips Research, Eindhoven, Netherlands

[27] Rick Smith, "The Biometric Dilemma" [online], available from World Wide Web:

http://www.smat.us/crypto/docs/bh-us-02-smith-biometric.ppt

[28] IETF, *RFC 3039 - Internet X.509 Public Key Infrastructure Qualified Certificates Profile*, January, 2001.

[29] H. C. Lee and R. E. Gaensslen, *Advances in Fingerprint Technology*, New York : Elsevier, 1991.

[30] M. Young, S. Modi, C. Tilton, A. Triglia, "Contribution on Biometric Architectures to AHGBEA", Purdue University, 2006

[31] "HP-UX Secure Shell Getting Started Guide" [online], Hewlett-Packard Development Company, 2006, available from World Wide Web: http://docs.hp.com/en/5991-7493/5991-7493.pdf

[32] Zdeněk Říha, Václav Matyáš, "Biometric Authentication Systems, FI MU Report Series", Faculty of Informatics, Masaryk University, 2000