Proc. of the Ninth Intl. Conf. on Advances in Bio-Informatics, Bio-Technology and Environmental Engineering - ABBE 2019
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN No. 978-1-63248-180-1 DOI : 10.15224/978-1-63248-180-1-07

A STUDY ON THE PAYMENT & SETTIMENT USING BIOMETRIC INFORMATION

[Yougjae Kim]

Department of Business Administration, Korea Polytechnic University, Prof. ph.D. Republic of Korea

Abstract.

The purpose of paper is to propose to standardize the international standard of the biometric Information on the payment & settlement using segregated biometric information for the distributed management technology of biometric data Research methodology is
review 2nd data analysis, conventional survey analysis and focus group interview (Government
agency officer, bank clerk payment & settlements officer, researcher and Professor) this paper
analyze international law, rule and system as follow

This paper intends to draw conclusion and malce implication as follows.

First, we must promote financial transaction

Second, we make to easy financial transaction by biometric Information(Fingerprint*)*

***Keywords*:Biometric,BiometricData, Authentication ,Certification, Trade, Financial transactions**

I. Introduction

Biometric information(Fingerprint) is a unique characteristic to identify individuals, such as fingerprints, faces and irises, that is used for authentication in a wide range of fields such as financial transactions, e-banking, fin-tech, e-business, distribution industry and etc.

Biometric information is convenient because it is inherent and does not need to be remembered or stored, but leakage or misuse of the information could bring about serious problems because of its unique property. It is becoming more and more important to manage the information safely without the possibility of misuse or leakage. To store the information safely, it is effective to segregate the information into fragments in an un-usable form. Accordingly, we propose to standardize the international standard for Management of Segregated Biometric Information.

II. Purpose and scope of Paper

A. *The Scope of Paper*

The proposed paper specifies in its scope the framework and process for management of segregated biometric information, including the definitions and terms, the management process and the authentication process.

First, the definitions and terms.

Second, the management process of segregated biometric information. Such as,

· Registration, deletion, inquiry and renewal process of segregated biometric information

Third, the authentication process of segregated biometric information.

· Financial Institution Server Method

· Segregation Management Center Server Method

III. Previous Studies

The earlier study analyzed the previous studies and current state of international standards such as ISO, IEC and ITU as follows.

First, ISO/TC68 SC2 standardized the international standards such as ISO 19092, Biometrics Security framework(2008).

Second, ISO/IECJTC1 SC27 standardized the international standards such as ISO/IEC 19790, Security requirements for cryptographic modules, ISO/IEC 24745, Biometric information protection, and ISO/IEC 19792, Security evaluation of biometrics.

Third, ISO/IEC JTC1 SC37 standardized the international standards such as ISO/IEC 19784, Biometric application programming interface (the component parts can be distinguished as follows).

·Part 1: Bio API specification

·Part 2: Biometric archive function provider interface

·24709-1R1, Conformance test for Bio API Part1 revision

·19794 -15, Biometric data interchange format - Part 15: Palm crease image data

·30106 -1AMD1, Object oriented Bio API - Part 1: Architecture - Amendment 1: Additional specifications and conformance statements

·30106 -4, Information technology - Object oriented Bio API - Part 4: C++ implementation

·ISO/IEC 30107, Biometric presentation attack detection

·ISO/IEC 30137 -2, Use of biometrics in video surveillance systems - Part 2: Performance testing and reporting (Biometrics base of CCTV security technology)

Fourth, ITU-T SG17 standardized the international standards such as ITU-T X.1086, A guideline to technical and managerial countermeasures for biometric data security

- ·ITU-T X.1087, A guideline to technical and operational countermeasures for telebiometric applications using mobile device (X.tam)
- ·ITU-T X.1085 ISO/IEC 17922, Telebiometric authentication framework using biometric hardware security module

IV. Previous Studies

Biometrics Information measurement and statistical analysis of physical characteristics and behavioral traits of individuals. Why is biometric data used for authentication?

First, universality: It uses the same factors everybody shares.

Second, uniqueness: No one else has the identical biometric features as that of the principal.

Third, stability: The biometric data remains unchanged over time.

The biometric data can be distinguished into different types as follows.

First, physical aspects (characteristics) are classified into four categories including the fingerprints, palms, veins and faces.

Second, behavioral features(traits) are classified into four categories including the voices, keystrokes, signatures and gaits

V. Registration and Authentication

How does the Biometric Authentication Process work?

First, the registration process extracts the template of user’s biometric data several times and stores the extracted biometric data.

Second, the authentication process extracts the template of user’s biometric data during service and performs the authentication by comparing it with the registered biometric data.

V. Distributed Management of Biometric Data

A. *Management of Biometric Data*

The management of biometric data is reviewed in three major perspectives as follows.

First, vulnerability to hacking attacks and risk of misuse.

Second, how to store biometric data

Third, prevention of hacking and update of data

.

B. *ulnerability to Hacking Attacks and Risk of Misuse*

The issues in this perspective can be summarized into two categories as follows.

First, the massive biometric data in the server is vulnerable to hacking.

Second, hacking of the data can lead to a critical issue due to the stability of biometric data.

C. *Prevention of Hacking & Management of Data Updates*

The management of data in this perspective focuses on two distinctive points as follows.

First, due to distributed management, the fragmented data would be of no use any longer even if the data is penetrated and stolen.

Second, the stolen data can be refreshed by changing the way the data is split for distributed storage.

Ⅶ Process for Management of Segregated Biometric Information

A. *Composition of Process for Management Segregated Biometric Information*

This process is composed of five phases as follows.

First, the registration process of biometric information.

Second, the authentication process of biometric information.

Financial institution server method (proprietary authentication tasks)

Segregation management center server method (commissioned authentication tasks)

Third, the deletion process of segregated biometric information.

Fourth, the authentication module of segregated biometric information.

Fifth, the distribution management of segregated biometric information

B. *Registration Process of Biometric Information*

The registration process is implemented as follows.

The fragments of registration template are managed by the financial company and segregation management center in a distributed way. By splitting the biometric data into fragments, to preclude the possibility of unauthorized authentication, to be kept at different institutions for distributed management, the risks related to the hacking of information can be prevented

C. *Authentication Process of Biometric Information*

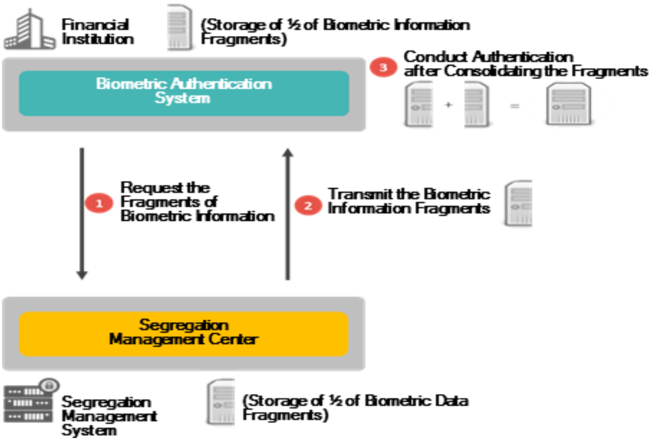
The authentication process can be distinguished between the financial institution server method and the segregation management center server method.

First, the Financial Institution Server Method (Proprietary Authentication Tasks).

After establishing the proprietary authentication system, the financial company conducts the consolidation and authentication of the biometric data with segregation management center assuming the role for storing the fragments of the biometric data.

Second, Segregation Management Center Server Method (Commissioned Authentication Tasks).

The financial company conducts the bio-authentication by using the shared authentication system offered by segregation management center, which assumes the role for consolidation and authentication of the biometric data.


Financial Institution
(Storage of ½ of Biometric Information Fragments)
Biometric Authentication System
3 Conduct Authentication after Consolidating the Fragments
+
=
1 Request the Fragments of Biometric Information
2 Transmit the Biometric Information Fragments
Segregation Management Center
Segregation Management System
(Storage of ½ of Biometric Data Fragments)

Ⅷ The Expected Effects

The expected effects of this paper are summarized in Table 1-1

Table 1. The Expected Effects of This Paper

	Benefits/impacts	Examples of organizations /companies to be contacted
Industry and commerce — large industry	All large industry (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)	Private company (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)
Industry and commerce — *SMEs	All SMEs (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)	Private company (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)
Government	Public area	Standard application business area
Consumers	End user	End user
Labour	Be increased in SME	Be reduced by apply standards and standards application
Academic & research Bodies	All academic & research bodies	All standard application business
Standards application businesses	All industry (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)	All industry (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement

Ⅷ Conclusion

This study intends to draw its conclusion and make policy implications as follows.

First, we must promote management of segregated biometric information.

Second, there is no international, regional or national standard of distributed management technology of biometric data. Accordingly, this proposal is to propose to standardize international standard for the distributed management technology of biometric data.

Third, biometric information is a unique characteristic to identify individuals, such as fingerprints, faces, veins and irises, that is used for authentication in a wide range of fields such as financial transactions, e-banking, fin-tech, e-Business, distribution industry and etc. Biometric information is convenient because it is inherent and does not need to be remembered or stored, but leakage or misuse of the information could bring about serious problems because of its unique property. It is becoming more and more important to manage the information safely without the possibility of misuse or leakage. To store the information safely, it is effective to segregate the information into fragments in an un-usable form.

Fourth, by ensuring the safety of the biometric information stored in a distributed way, the financial institutions are not allowed to infer the sound biometric information of customers and the fragmented biometric information is not available for use even if the fragments are leaked.

Fifth, the convenience can be enhanced in financial transactions. Because the customer can use the financial services at the other financial institutions without additional registration if the customer has registered the biometric information with one financial institution, convenience in financial transactions could be enhanced.

References

[1] *A study of Biometric Approach Using Fingerprint Recognition Lecture Notes on Software Engineering Vol.1 No.2, May 2013 Ravi Subban and Dattatreva P.Mankame page 211-213*

[2] *Biometrics Management Guidelines for the financial security, TTA(Telecommunications Technology Association) 2016.12.02*

[3] *Ensuring Quality in Biometric Systems Md. Mahbubur Rahman, Amit Karmaker, Md.Mahmudul Hasan, Samsuddin Ahmed international Journal of Security and Its Applications 2015 September Vol.9 No4*

[4] *ISO 19092, Biometrics Security framework, ISO/TC 68 SC2, 2015*

[5] *ISO/IEC 19790 Security requirement for cryptographic module. ISO/IECJTC1 SC27. 2015*

[6] *ISO/IEC 24745, Biometric information protection, ISO/IECJTC1 SC27. 2015*

[7] *ISO/IEC 19792, Security evaluation of biometrics, ISO/IECJTC1 SC27. 2015*

[8] *ISO/IEC 19784, Biometric application programming interface, ISO/IEC JTC1 SC37.2015*

[9] *ITU-T X.1086, A guideline to technical and managerial countermeasures for biometric data security, ITU-T SG17*

[10] *Segregated management of biometric data information, Korea payment settlement association Park Jung Gook 2016.12.05*

[11] *Standard of segregated management biometric data , ISO/TC 68 SC2 Presentation, 2018.04.25*

[12] *"A novel way of ICON based authentication methods", Advance Computing Conference (IACC) 2015 IEEE International, P Devaki, Raghavendra Rao, pp. 449-453, 2015.*

[13] *Use of biometric data Information and protection of privacy. Korea institute of Information security December 2005 Cryptology vol.15, No.6 Jeon Myung Geun, Moon Ki Young page 14~16*