Security Issues Related to Biometric Security

Sunghyuck Hong, JungsooHan, Guijung Kim

Abstract*: Biometric security is one of the promising methods. The purpose of this study is to provide a more systematic understanding of Biometric security. This study systematically summarizes the issues related to the biometric authentication method from the viewpoint of the non–professional, and suggests solutions on a policy level. The research methods were mainly based on the literature. Analysis of biometric types are being used, and there are pros and cons in each biometric type. Biometric authentication should use for authentication minimum two methods. Otherwise, each biometric method has its own vulnerability which could be attacked by malicious users. When developing policies, this study will be helpful. The fact that it does not reflect the latest trends abroad and the fact that it cannot present the technical supplementary measures more professionally and directly is the limit of this study.

Index Terms*: Biometric, Biometric security, FinTech, Information Security, Information protection.

I. INTRODUCTION

Biometric authentication technology, which is a security technology used in various devices, networks, and industries, is spreading. Especially, it is attracting attention worldwide with the development of FinTech (Fusion of IT and finance, Fintech). Especially in the financial sector. As an IT technology that adds security, biometric authentication technology is actively being introduced. However, paradoxically many experts say that it may be harder to keep personal privacy. Thus, what exactly is biometric technology, and why is biometric technology so hard to keep it private? This research question was derived from the interest in FinTech. We will also consider what measures are currently in place to overcome the security limitations of biometric technology. The composition of this study is as follows. Section 2 describes the overview of the biometric system, and Section 3 describes the principle of the biometric system. Section 4 describes the security limitations of the biometric system, and Section 5 describes the security measures of the biometric system. Finally, Section 6 concludes the conclusion of the study and future work.

II. BIOMETRIC SYSTEM OVERVIEW

A. Definition and type of biometric system

Figure 1 shows characteristics of biometrics. There are two types of biometric. A biometric system is a technology system that distinguishes biometric information (Fingerprint, iris, finger vein, face recognition, voice, hand shape, etc.) which are different for each person who is registered and registered in the storage device of the system, and the biometric information characteristic of the individual is measured through the biometric input device. In addition, user recognition is determined by comparing the registered information with the registered information.

Biometric methods are not only physical features but also they are behavioral features. Therefore, it can be classified into two types based on physical characteristics and behavioral characteristics. In the method based on the physical characteristics, it utilizes the part with little change in the individual body such as iris, fingerprint, and retina. Biometric methods that utilize behavioral features including the behavior of the mobile phone, voice or signature, keystroke, and gait. The biggest advantage of biometric technology is that it provides both convenience and security. Human fingerprints, irises, and faces are difficult to steal or forge. Also, they are easy to use because there is no need to remember or prepare them separately.

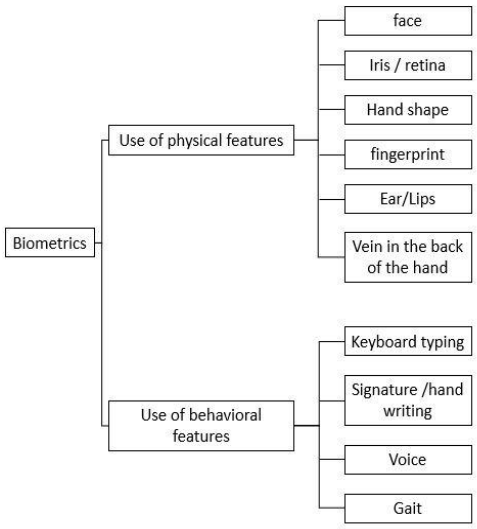

Figure 1. Biometrics using behavioral / physical characteristics

B. Utilization of biometric system

Since the 2000s, biometrics technology, which has been used in military and aviation, has been introduced as an authentication system for sensors and touch IDs of digital devices themselves (mainly for companies such as iPhone fingerprint touch

Revised Manuscript Received on May 23, 2019.

SunghyuckHong, Div. of ICT, Baekseok University, Korea, Cheonan, Republic of Korea.
Jungsoo Han, Div. of ICT, Baekseok University, Korea, Cheonan, Republic of Korea.
Guijung Kim, Div. of ICT, Baekseok University, Korea, Cheonan, Republic of Korea.

authentication), recently, wearable devices, The development of information and communication technology, such as tech, has expanded the range of applications using biometrics technology. Therefore, the security using biometric technology is getting serious.

In particular, as the FinTech market, such as the launch of a professional bank in Korea, has become more active in Korea, biometric systems have become an innovative authentication technology because of the importance of self-certification in financial transactions.

Table 1: Biometric situation of Major banks in Korea

Bank name	Mobile Banking name	Biometric situation
Shinhan bank	Sunny bank, Shinhan S bank	Unmanned store kiosk vein, mobile iris recognition support
KB Kookmin bank	KB star banking, Liiv	While using palm vein authentication trial, electronic rental safe wi ll be used
KEB hana bank	1Qbank	Fingerprint information instead of a certified certificate
Wooribank	Webee platform	Kiosk Iris vein fingerprint authentication, voice recognition service launched
NH nonghyup	new NH smart banking	Fingerprint information instead of a certified certificate
Korea city bank	new city mobile	Using fingerprint information, you can transfer without limit betwe en your account

III. PRINCIPLES OF BIOMETRIC SYSTEMS

This section covers the more common iris recognition, finger vein recognition, and fingerprint recognition in biometric systems.

A. Iris Recognition

The iris recognition technology is based on a video signal processing algorithm based on Gabor Wavelet Transform which John Daugman of University of Cambridge in England can code the iris pattern to 256 bytes. It is used in places where high security is required because the recognition rate is lower than in other systems. It is statistically more accurate than DNA analysis and can be recognized even if wearing lenses or glasses for vision correction.

B. Finger vein recognition

The finger vein recognition technology maximizes the brightness contrast of blood vessels to the skin using infrared light and filters from the skin of the back of the hand and then extracts the vein pattern from the input digital image. Users who do not have fingerprints or fingers can also use it. In addition, the vein has more information than the fingerprint, so the recognition rate is high. There is a high possibility of application in the future, and security is very high because replication is almost impossible.

C. Fingerprint recognition

The most widely used biometrics, fingerprint recognition, began in England in 1684 when N. Grew discovered that people's fingerprints were different. It was first commercialized in a securities company in Wall Street, the USA in 1968. Fingerprint recognition is possible by a semiconductor, hybrid, and optical methods. The semiconductor method is to read the specific shape of the fingerprint that touches the chip surface by the electric signal when the finger touches directly to the surface of the silicon chip. The fingerprint information is obtained by reading the change of the capacitance of the chip installed on the chip surface and the fingerprint image obtained by using the ultrasonic wave or the electric field is converted into the electric signal to obtain the fingerprint. The optical system shoots the input light from the light source onto the prism and reflects the fingerprint shape of the fingertip placed on the prism. This reflected fingerprint image uses the principle that the fingerprint image inputted to the CCD through the high-diffraction lens is digitized by a special algorithm so that it is precisely focused on the CCD. The structure is the simplest and can prevent static electricity. The mixing method is a combination of an optical method and a semiconductor method.

D. Iris certification of Galaxy S8

Germany 's Chaos Computer Club (CCC) hackers have unveiled a video depriving the Galaxy S8 iris recognition security. The method was also simple. The male in the image was 1) taken a face photograph, 2) printed the corresponding photo, 3) put a contact lens on the pupil part of the output, and 4) exposed the Galaxy S8 iris recognition screen. By applying this method, a high-performance camera can capture a person's iris and disable security.

E. HSBC Bank's mobile certification

Although HSBC Bank has emphasized the safety of voice recognition services and promoted the excellence of biometrics, BBC's Dan Simms reported that his twin brother succeeded in verifying his mobile banking with his voice mimicked by his twin sister.

F. Biometric system security vulnerability

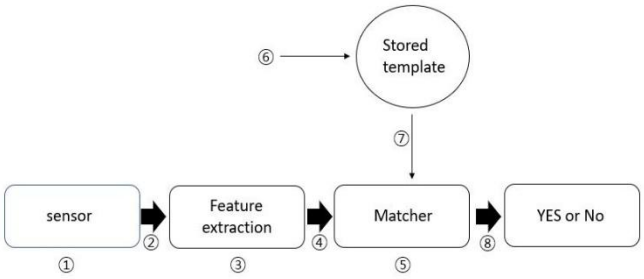

Figure 2. Points that can be attacked

Figure 2 shows the points that can be attacked in the biometric system. Here is a simple example.

①A part for obtaining a signal from a user is a case where a false fingerprint, a copied signature, a face mask, or the like is used in the sensor.

②In case of using the bio-signal which is previously stored again, the (bypass) by-pass the sensor and sends a copy of a fingerprint or a voice signal.

③ The attacker attacks a feature extraction node using

a Trojan horse or the like to create a desired feature.

④ If you know a specific way of expressing a biometric system, you can arbitrarily change it. If feature extraction and matching are done in one step, you can solve it to some extent. But if a feature point is transmitted to the Internet, snoop on TCP / IP You can also change the packet through.

⑤Attacking the matching unit itself to get a preselected matching result, no matter how accurate the matching algorithm is, results in unwanted results.

⑥In the case of changing the stored template by attacking the database in which the template is stored, in particular, when the template is stored in a distributed manner, some or all of them may be changed, and thus the rate of acceptance of other persons or the rejection rate may be increased.

⑦When the stored template is transmitted to the matching end through the transmission channel, it attacks the channel. In this case, the transmitted data is intercepted and changed into another form, resulting in different matching results.

⑧Even if the actual system is excellent and accurate, there is no meaning if the match result is attacked.

IV. BIOMETRIC SYSTEM SECURITY MEASURES

A. Legal and institutional measures

In the current Electronic Financial Transactions Act, if a consumer is harmed by forgery or alteration of security authentication means including biometric information, the consumer can be compensated for damages only by proving the specific situation. In the case of the United States, financial institutions are responsible for making repayment easier. However, as described earlier, the leakage of biological information once does not stop the damage once, so even if compensation is given, the long-term damage may be repeated. More careful attention is needed to prevent this. Therefore, it is necessary to establish appropriate laws, regulations, and social agreements that do not lag behind the speed of technological development.

First of all, it is necessary to investigate the subject of management of biometric authentication information for biometric authentication, system construction and activation measures for a development project.

In addition, biometric-based user authentication technology should be developed as well as security technologies for data archiving and transmission. In addition to promoting in-depth research for industry-academia-industry researchers, biometrics industry participants should be obliged to self-evaluate and forecast security by law. In addition, not only self-evaluation, but also domestic and foreign experts should be verified by mobilization.

Finally, even if hacking technology develops, it should invest in the field of data security R&D in order to prepare countermeasures.

B. Technical measures

First, encryption of biometric data for improving the security of the user authentication system when it is desired to transmit binaries biometric information to the server with using the MD5 and RSA algorithms for secure transmission using. It is a solution for secure transaction.

Second, multiple biometrics can be mentioned. It can improve security performance through multi-biometrics-based real-time authentication and authentication technology in Multi-biometrics-based authentication technologies and tasks. For example, even though, one of biometric methods passed, but the system requires an additional channel to finish the process such as OTP.

Finally, the last technical measure is discriminating a counterfeit fingerprint which is proposed an effective learning data enhancement method based on the forcible fingerprint discrimination difficulty and confirmed the validity through experiments.

This is a method of protecting biometric information using a smart card. Store biometric templates on a smart card instead of an attack-prone database, and delegate management to users (store-on-card). If so, we can block attack point ⑥in Figure 2 and solve the privacy problem. However, this method may be exposed when the stored biometric template is transmitted out of the card for comparison with the inputted biometric information that is, exposed at the attack point ⑦. The most complete scenario using a match-on-card smart card is a sensor-on-card method in which a fingerprint sensor is mounted on a card, to be. The entire process from acquiring biometric information to processing can be processed inside the smart card, which makes perfect security possible. However, since most of the feature extraction stages include a signal processing process requiring a large amount of computation for processing by a processor in the smart card, there is an economic burden that the hardware for the exclusive use of feature extraction must be installed separately in the smart card. Figure 3 shows multi biometric authentication process. Each biometric authentication has its own weakness which could be a possible target from malicious users or hackers.

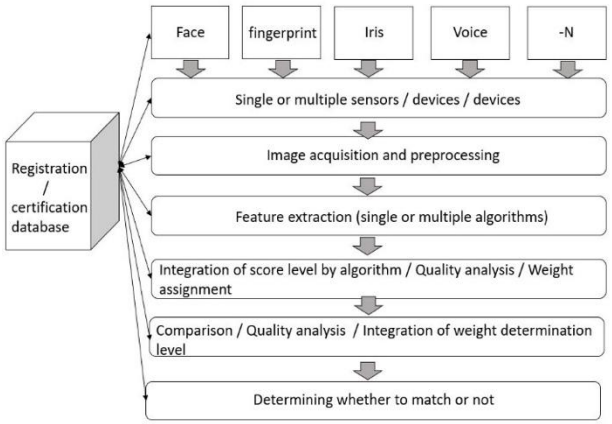

Figure 3. Multi Biometric Authentication Process

V. CONCLUSION

Biometric information cannot be arbitrarily changed unlike a password, so once leaked, it can be permanently exploited for various crimes. Therefore, it is very necessary to establish a regulatory policy that follows the speed of IT development. Through continuous R & D support, countermeasures should be taken to completely block the existing security holes. In the past, we have to recognize that a single piece of a picture can be a preparation for hacking, as opposed to the fact that personal face information has been regarded as public information. Biometric technology should not be blamed for the fact that no major damage cases have yet emerged. In this regard, the latest technological research trends were also examined. In order to prepare for the new biometric hacking that will appear in the future, it is necessary to concentrate on security throughout the whole process including data collection, network transmission, utilization in Fintec, database management.

REFERENCES

1. JaepilYoo and Sekyoung Huh, "Fintech security issues and fundamental strategy", Communications of the Institute of Information Scientists and Engineers. 2015 May, 33(5), pp. 33-36.
2. Sanghwan Park, “Requirement of Fintech”, The Journal of The Korean Institute of Communication Sciences .2017 Feb, 34(3), pp. 15-22.
3. Jeongkuk Park, “Fintech and Information Security”, Communications of the Korean Institute of Information Scientists and Engineers, 2015 May, 33(5), pp. 23-32.
4. Hyo-beomAhn, “Analysis on Trend of Domestic Fintech technology”, Communications of the Korean Institute of Information Scientists and Engineers. 2016 April, 34(4), pp. 29-33.
5. Cho, Byungchul& Park, Jong-Man,“Technology Review onMultimodal Biometric Authentication”, The Journal of Korean Institute of Communications and Information Sciences, pp. 132-141.
6. Park, Wooshin. “Encryption of Biometrics data for Security Improvement in the User Authentication System,” 2005.
7. Dong-yoon Kim and Jae-seon Lee and MinguKang, “Application of Biometric Sensors based Fintech Identification“, internet information journal. 2015, 16(2), pp. 57-63.
8. J. Galbally-Herrero, J. Fierrez-Aguilar, J. D. Rodriguez-gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia and M. Tapiador, "On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks," Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology, Lexington, KY, 2006, pp. 130-136.
9. R. E. O. Paderes, "A Comparative Review of Biometric Security Systems," 2015 8th International Conference on Bio-Science and Bio-Technology (BSBT), Jeju. 2015, pp. 8-11.
10. P. K. Saralaya, R. Anjali, G. Shivaprasad and N. V. S. Reddy, "Biometric authentication usage for internet banking," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore. 2017, pp. 1810-1814.
11. K. Saeed, "A Note on Problems with Biometrics Methodologies," 2011 International Conference on Biometrics and Kansei Engineering, Takamatsu, Kagawa, 2011, pp. 20-22.
12. Weonjin Kim and Cheng-Bin Jin and Jinsong Liu and Hakil Kim, “Data Mixing Augmentation Method for Improving Fake Fingerprint Detection Rate“, Journal of The Korea Institute of Information Security & Cryptology. 2017 Apr.
13. M. Gomez-Barrero, C. Rathgeb, U. Scherhag and C. Busch, "Predicting the vulnerability of biometric systems to attacks based on morphed biometric information," in IET Biometrics. 2018 July, 7(4), pp. 333-341.

AUTHORS PROFILE

Sam 'Sunghyuck' Hong received his B.A. degree from Myongji University, Korea in 1995. After graduation, he worked at Hyosung Inc. in Seoul, Korea from 1995 to 1999 as a computer programmer and ERP consultant. He received a Ph.D. degree from Texas Tech University in August, 2007 major in Computer Science.

After graduation, he worked at International affairs in Texas Tech University as a senior programmer/analyst from 2007 to 2012, and his jobs were development of ASP.NET web applications and maintenance of PC/Server.

Currently, he is an associate professor in Division of Information & Communication at Baekseok University, and he is a member of editorial board in the Journal of Korean Society for Internet Information (KSII) Transactions on Internet and Information Systems. His current research interests include Blockchain, Secure Crypto-currency, Secure Mobile Networks, Secure Wireless Sensor Networks, Key Management, Networks Security, Information Security, Embedded Networked Systems, Embedded Software, Wireless LAN, Distributed Systems, Computer Networks, Hybrid Wireless Network Architecture Design, and Mobility Design/Modeling/Simulation. He published 53 referred journals papers and 28 referred conference papers which are related to Blockchain and Secure protocols since 2004. Total research grants is $928,578 from 2013 to present. Contact email is shong@bu.ac.kr. Mailing address is Munam-ro 76, Dongnam-Gu, Chenan, Chungnam, Republic of Korea, 31065.

Jung-Soo Han received a BS, an MS, and a PhD in Computer Engineering from Kyung Hee University, Republic of Korea. Since 2001, he has been a Professor in the Division of Information & Communication Technology, Baekseok University, Cheonan City, Chungnam, Republic of Korea. In 2014, he researched Convergence IT and Creative Education Methodology at California State University Fullerton as an Exchange Professor. His research topics include Data Mining, Contents Planning, 3D Modeling and CBD, Telemedicine, Knowledge-based Decision Support Systems, Intelligent Systems, Convergence, HCI, and Recommendation Systems. He has edited books on computer science and convergence technology. He serves as Executive Editing Director of the International Conference on Convergence Content (ICCC), as General Co-Chair of the International Conference on Digital Policy & Management (ICPDM), as General Co-Chair for steering committees of the International Conference on Convergence Technology (ICCT), as Workshop Chair of the International Conference on Information Science and Application 2013, as Workshop Chair of the 2nd International Conference on IT Convergence and Security 2012, as Vice President of the Korea Contents Association, as Vice President and a member of the Editorial Committee of the Society of Digital Policy & Management, and as Vice President of the Editorial Committee of the KoreaContents Association.

GuiJung Kimreceived the B.S. degree and the M.S. degree in computer engineering from Hannam university, Republic of Korea, and the Ph.D. degree in computer engineering from Kyunghee university, Republic of Korea in 2003. Since 2001, she has been a professor in department of Biomedical Engineering, Konyang University, Chungnam, Republic of Korea. Since 2017, has been a Professor in the Division of Information & Communication Technology, Baekseok University, Cheonan City, Chungnam, Republic of Korea.Her main research interests include Medical Information System and 3D e-Learning, security programing, Big data, Intelligent Systems, Convergence System. She has edited books on computer science and convergence technology.