Journal of Engineering and Applied Sciences 13 (5): 1118-1123, 2018
ISSN: 1816-949X

Non-Face-To-Face Digital Signature Using Fingerprint in FinTech Environment

[1]Yonghoon Jung and [2]Jinhee Song
[1]Department of Computer Sciences, Soongsil University,
369 Sangdo-ro, Dongjak-gu, Seoul, Korea
[2]School of IT Convergence Engineering/Computer Science and Engineering,
Shinhan University, 30 Beolmadeul-ro, 40 Beon-gil, Dongducheon-si,
Gyeonggi-do, Republic of Korea

Abstract: The advent of FinTech industry had to requiring triggered vibrant research of the biometrics-based non-face-to-face identification and digital signature technologies, especially in the financial industry. The biggest problems of the digital signature technologies are delegation/lending/duplication. In this study, we propose a new approach method which use the TEE area in the smart phones and it based on non-face-to-face identification and digital signature method. Suggested method is requiring no specific device except smart phones. The biometric information and personal data of the user are stored in the safe TEE within the smart phone. In our method, the key generation and digital signature are also, conducted in TEE, we can prevent to various types of attack including sniffing and man-in-the-middle attack. Also, because all of the processes are conducted in TEE, the all transactions can be protected against malicious users.

Key words: Biometrics, fingerprint, digital signature, FIDO, TEE, transactions

INTRODUCTION

Recent development of IT technologies enables individuals as well as companies to accumulate various types of data and to easily distribute them over the network. The environment under which the data can be shared on a large scale has been already implemented. With considerable growth of e-Commerce triggered by development of internet, research on biometrics is being conducted vibrantly in various fields. Biometrics is a new type of identity verification method which overcomes the limits of the existing simple verification method and minimizes the risk of illegal use or fabrication through loss, theft or leakage. Biometrics is a field of studying measurable physical or biological features to automatically verify or identify individuals. The bio-data are classified into passive and active biological features. The passive biological features include fingerprint, iris, face, hand vascular pattern, retinal vascular pattern, palm, ear and DNA. The active biological features include voice, online signature, walking pattern and key stroke (Korea). Generally, the biometric information is used only for the authentication of the user and only the method using the certificate is used as the digital signature. In order to solve the problem of certificate, it is necessary to study identity verification and digital signature method using biometric information that can not be delegated/lending/duplicated. Research on biometric information is actively underway in the financial sector. While adopted in various fields for protection of information, the biometrics system is controversially infringing the personal physical data. A university had adopted the fingerprint recognition system for gate control but had to remove the system in the controversy of infringement of personal data. Protection of personal data might not be a critical issue in the community of small number of people established on a wide area but has become an important personal value, since, the industrial revolution. Personal data was first defined by the judges of USA late in the 19th century and has become a right of citizens. Each state has separate legal or social system to protect personal data. Scholars tend to consider it as a matter of interest or concern, rather than a right (Park, 2015).

Literature review

Weak points of the biometrics system: The biometrics system has the following weak points: one can acquire the bio-signal from the user. He/she may use forged fingerprint, copied signature or a picture of the face. If the stored bio-signal is reused, one can bypass the sensor and send the copied fingerprint or the audio signal. One can attack the feature extractor by using Trojan Horse in order to create the desired feature.

When one knows the method of expression of features used by the biometrics system and changes it

Corresponding Author: Jinhee Song, School of IT Convergence Engineering/Computer Science and Engineering, Shinhan University, 30 Beolmadeul-ro, 40 Beon-gil, Dongducheon-si, Gyeonggi-do, Republic of Korea

you can solve the problem to some degree if the feature extraction and matching are performed in a single step. If the feature is transmitted over internet, one can change the packet through snooping of TCP/IP.

If one attacks the matcher and makes the system to provide the preselected matching result, however, accurate the matching algorithm is you will receive the unwanted result. If one attacks the database and changes the entire or a part of the stored template, the False Accept Rate (FAR) or the False Reject Rate (FRR) grows.

If one attacks the channel through which the stored template is transmitted to the matcher and changes the data being transmitted, you will acquire a unexpected matching result. If one attacks the final judgment, however, excellent and accurate the actual system is you cannot solve the problem.

There are numbers of attack points and you should consider the plan to avoid attacks. In Japan, regarding the question of how to identify copied fingerprint they suggest two different approaches. Software-wise approach and hardware-wise approach. The software-wise approach includes sweat gland for the fingerprint reader, movement of head for the face reader and movement of eye for the iris reader. The hardware-wise approach includes temperature and pulse measured at the finger for the fingerprint reader or utilization of electric feature. If you can use these approaches, you can avoid attacks to the sensor to some degree. Or you can use encryption method or encrypted channel or install the matcher and the database in a safe place (Park, 2015; Inyeob and Chun, 2016; Lee and Park, 2010; Jeong-Hyo, 2016; Srinivas *et al*., 2015; Lindemann *et al*., 2014).

Digital watermarking: Use of watermark goes back to the ancient Egypt. In the process of making study from papyrus they dissolved fiber in water and put it on an expeller. In this course a unique pattern called watermark is generated. Watermark indicates the pattern you can find through light without change or damage. The watermarking technology is used in bills. In order to make watermark on bills, they print the unique watermark on wet bills. You can view the unique watermark through light to detect counterfeit bills. In general, watermarks are made such that they should not be seen easily with the naked eye. With the development of digitalization technology, printed matters or contents are distributed over internet. In this course, the watermarking technology is developed to hide the copyright information in the researches (Inyeob and Chun, 2016). Figure 1 shows the watermarking flow.

The watermark data specifying the digital content and the copyright to be protected generates the water marked digital content at the watermark embedding module. The water mark detection module checks if there is any water mark and only the appropriate user is allowed to detect, recover or modify water marks. For this purpose, a publicly shared watermark key is used.

Embedding data in bio-data: In order to prevent forgery of bio-data, you may consider embedding additional information in the bio-data (watermarking). Unless the embedding algorithm is known, the service provider can guarantee safety of the fingerprint image transmitted with the standard watermarking technology. The water mark protects the finger print image stored in DB from forgery and enables users to send the finger print image safely by embedding a water mark before transmission and detecting the water mark at the receiver side. The technology of hiding data by embedding a water mark in an image is well known. But most of the studies on water marking technologies were to protect the copyright and not provide authentication. The study on embedding a water mark before and after extraction of finger print feature suggests that the embedded water mark should not change the feature of the finger print image. Recently, a study has suggested the multi-modal biometrics system where the finger print/face host image is protected with the finger print feature embedded in the face image or the face feature embedded in the finger print image and at the same time, the embedded face/finger print feature is used additionally (Park, 2015).

Digital signature: Digital signature is used with the public key encryption technology and the hash function. Digital signature operates in the following procedure: Generation and verification of digital signature (Murukutla and Shet, 2012; Li and Mitchell, 2014; Anonymous, 2016a, b).

The signer generates a private key and a public key. e-Document is contracted with the message digest using a hash function. The sender encrypts the message digest by using his/her private key to generate a digital signature (Fig. 2). The sender combines the digital signature with the original e-Document and sends it with the certificate to the receiver.

The receiver separates the digital signature from the original e-Document sent by the sender. The receiver decrypts the received digital signature by using the public key included in the receiver certificate. The receiver generates the message digest from the

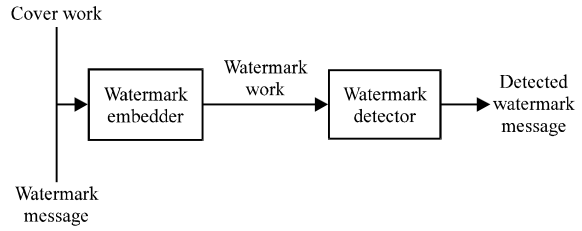

Fig. 1: Watermarking flow

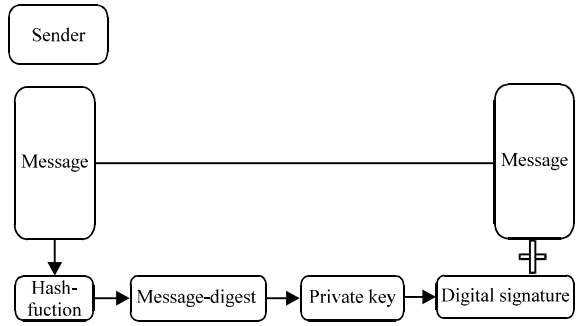

Fig. 2: Generation of digital signature

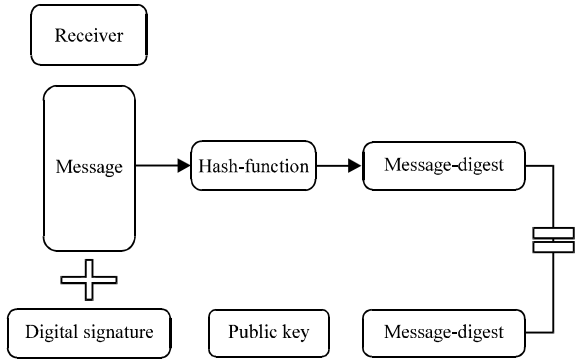

Fig. 3: Digital signature verification

original e-Document by using the hash function. The receiver compares the values of the two message digests, verifying if the signer has signed the e-Document (Fig. 3).

MATERIALS AND METHODS

Secure digital signature using fingerprint: Digital signatures using public certificates are vulnerable to delegation/lending/duplication and many studies are under way to solve them. Digital signature method using fingerprint is an electronic signature method using biometrics information which is a method of measuring similarity. Since, biometric information can not be the same every time, it is confirmed by using similarity. Therefore, biometric information can be easily distinguished when it is copied and used.

Digital signature utilizing the FIDO TEE technology on the mobile environment: In the suggested system, a user can identify himself/herself and make the digital signature by using own bio-data. In the suggested system, the bio-data are only executed and managed in TEE for the safety reason.

Composition of the overall system: The suggested system supports users with the smart phones or smart devices with the finger print sensor and the NFC function to identify themselves and to make digital signature on the mobile environment. Figure 4 shows the suggested system.

Face-to-face contractor: In a face-to-face contractor, after the user prepares the contract, the agent reviews the contract and requests the user to make a digital signature. On receiving a request from the agent, the contractor registers his/her bio-data through the finger print sensor embedded in the mobile device. The bio-data is stored in a safe area and the key for authentication of the device is generated in the safe area.

In the TEE (Hardware-based independent execution area) area, digital signature is made with the bio-data, device authentication key and the time stamp value (Fig. 5). The following formula is used to generate the device authentication key and the digital signature:

Device authentication key = (IMEI || MACaddress)
Encryption key = DAK⊕RN
Sign = E (UUID || DAK), TS
(DAK: Device Authentication Key

The digital signature information generated in this way is delivered between mobile devices through NFC communication. The delivered digital signature information is combined logically with the e-Document in the server.

Agent: The agent signs the contract with the contractor in a face-to-face manner and requests the contractor to sign the contract and to make the digital signature. The agent also, reviews the e-Contract. In order to receive the digital signature of the other contractor in a remote place, the agent requests the mobile number of the remote contractor from the face-to-face contractor. The agent sends the mobile number of the remote contractor to the server (Fig. 6).

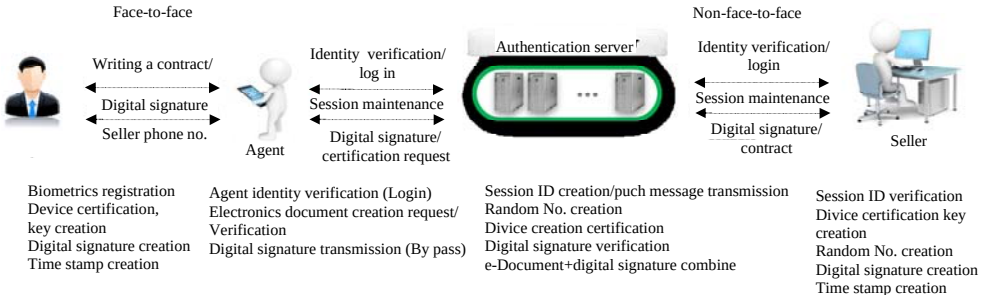

Fig. 4: The suggested flow of digital signature and authentication

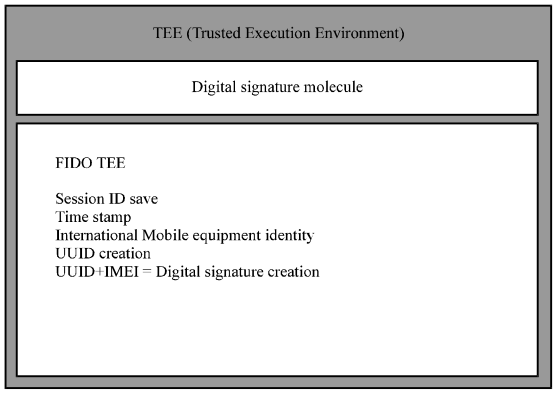

Fig. 5: TEE area (Trust Execution Environment)

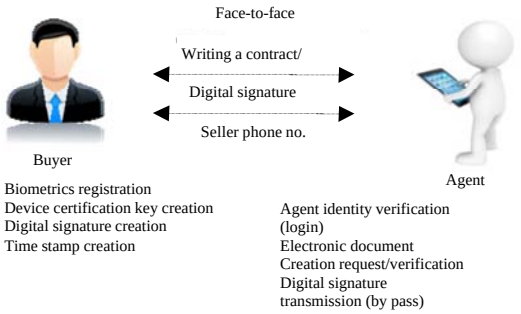

Fig. 6: Face-to-face transactions

After the remote contractor signs the contractor and makes a digital signature, the agent reviews the contract and completes the contract with the accredited digital signature through the accredited certificate. The accredited digital signature plays the role of offline notarization.

Server: The server provides the face-to-face contractor, the remote contractor and the agent with the e-Contract and logically combines the e-Contract with the digital signatures. The server also, sends the authentication code to the remote contractor through the push message and authenticates the user with the received authentication code. After user authentication, the server sends the dedicated app. URL to be used in digital signature to the remote contractor and the remote contractor installs the app. URL in his/her mobile device. The reason to use a dedicated app. is to use safer environment and area. After authentication of users, the server provides the safer environment for digital signature through the session connection. The session ID is created in the server and transmitted to the remote contractor with a random value.

Remote contractor: In order to perform non-face-to-face authentication and digital signature on the mobile environment, the remote contractor receives a user authentication code from the authentication server and returns it to the server for authentication. After completion of authentication, the remote contractor downloads the dedicated app. required for digital signature from the URL received from the server. The digital signature value of the remote contractor is created as following:

$$Sign = E\ (UUID \parallel DAK, Auth\text{-}Code), TS$$

The reason to use a dedicated app. is to maintain the session for safe transaction environment and to use a safe area for safe management of bio-data.

RESULTS AND DISCUSSION

Performance evaluation: To check the safety of the suggested digital signature system, this study has compared safety between manual signature, general digital signature and accredited digital signature. Table 1 shows the result of the comparison.

Safety of bio-data: A smart phone is roughly divided into the general area and the secured area. The general area can be accessed by all users. If any app. with a malicious cord is installed from the Google market or the mobile device is infected by a malicious cord, all information in

Table 1: Safety comparison

Variables	Handwritten	Certificate	Proposal system
Safety	Weak	Usually	Strong
Fake	Weak	Usually	Usually
Lost and rental	Weak	Weak	Strong
MITM	Weak	Safety	Safety
Advantage	Simplicity	Manageability	Lightweight long-term verification
Disadvantages	Copy/imitation	Delegation/lending/duplicated	Non-standardization

the general area can be leaked. In the suggested system, bio-data and other personal data are processed safely in TEE (Trust Execution Environment) of the android smart device.

Forgery: Manual signature generally means the signature made with a hand on the pad after making payment with a credit card. Manual signature can be copied and it is very difficult to analyze handwriting with the stored image. For example, payments made by credit cards are mostly signed by the sales clerks. The suggested system adopts the bio-data-based digital signature which cannot be rent to other person or signed by other person. The bio-data used in digital signature are stored in TEE (Trust Execution Environment), the secured area in the smart phone. The bio-data used in digital signature are controlled and managed by the user himself/herself.

Loss and rent: The digital signature using the accredited certificate has the risk of malicious cord distributed through active X. To use it in a smart phone, you need to move and copy the accredit certificate. One can copy the accredited certificate and delegate or lend it to other user or it can be lost. These kinds of accident occur, so, frequently. By using the bio-data which cannot be delegated, lent or copied, the suggested system solves the problems of the accredited digital signature system. Because all the processes of digital signature are conducted in TEE, it is protected from leakage or online attack.

Man-in-the-middle attack: Attackers can seize the biometrics-based digital signature value to forge or reuse it. The biometrics-based digital signature system authenticates users by comparing similarity because no identical value can be acquired due to the characteristics of the bio-data. In the suggested system because digital signature is generated and managed in TEE, the bio-data is protected safely against attacks. When a man-in-the-middle steals the digital signature value and attempt to reuse it, the same digital signature value shows that it has been forged or copied, since, it is not possible for the bio-data to generate the same value.

CONCLUSION

Recently, growing number of financial institutes has declared disuse of accredited certificate and are considering and adopting the biometrics-based authentication and the digital signature technology as the alternative means. Because you cannot easily change the bio-data when it is lost, you need to store and manage it safely. This study suggests the method for safe storage and management of bio-data on the mobile environment and the biometrics-based user authentication and digital signature. The suggested digital signature system prevents the problems of the existing system caused due to delegation or lending of signature. The suggested system also, solves the problem of leakage of bio-data because it is stored and managed safely in TEE. Recently, research is being conducted actively on the biometrics-based non-face-to-face authentication and digital signature technology. Further, research is required for the method of managing the bio-data more safely.

REFERENCES

Anonymous, 2016a. Excavating research areas of FinTech through the analysis of its relevant technologies and policy trends at home and abroad. Korea Internet & Security Agency, South Korea.

Anonymous, 2016b. Implementation guideline for safe usage of accredited certificate bio information in smart phone. Korea Internet & Security Agency, South Korea.

Inyeob, J. and K.M. Chun, 2016. Digital currency and inflation hedge: Evidence from Bitcoin. Korea Assoc. Telecommun. Policies, 1: 31-51.

Jeong-Hyo, P., 2016. A non-password secure biometric digital signature method for mobile device. Master Thesis, Soongsil University, Seoul, South Korea.

Lee, H.W. and Y.J. Park, 2010. A design and implementation of user authentication system using biometric information. J. Korea Acad. Ind. Cooperation Soc., 11: 3548-3557.

Li, W. and C.J. Mitchell, 2014. Security Issues in Oauth 2.0 SSO Implementations. In: Information Security, Chow, S.S.M., J. Camenisch, L.C.K. Hui and S.M. Yiu (Eds.). Springer, Switzerland, ISBN: 978-3-319-13256-3, pp: 529-541.

Lindemann, R., D. Baghdasaryan and E. Tiffany, 2014. FIDO UAF protocol specification v1.0. FIDO Alliance Proposed Standard, USA.

Murukutla, P. and K.C. Shet, 2012. Single sign on for cloud. Proceedings of the 2012 International Conference on Computing Sciences, September 14-15, 2012, IEEE, Washington, USA., ISBN:978-0-7695-4817-3, pp: 176-179.

Park, J.G., 2015. Fintech and information security. Commun. Korean Inst. Inf. Sci. Eng., 20: 23-32.

Srinivas, S., D. Balfanz, E. Tiffany and A. Czeskis, 2015.. Universal 2nd Factor (U2F) overview. FIDO Alliance Proposed Standard, USA.