International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.341-350
http://dx.doi.org/10.14257/ijsia.2016.10.10.30

The Data Processing Approach for Preserving Personal Data in FinTech-Driven Paradigm

Kyongjin Kim and Sengphil Hong[1]

School of Information Technology, Sungshin Women's University
{ kyongjin, philhong } @sungshin.ac.kr

Abstract

FinTech-driven paradigm shift in financial service poses challenges for financial sector in balancing the potential benefits of development with the potential risks. It is difficult to detect as advanced threats, so the extent of the damage cannot be foreseen in the financial sector. In this paper, we suggest the approach based on trust about processing data including personally identifiable information for preserving and protecting in the environment using FinTech.

Keywords: *FinTech, Financial Technology, Preserving Personal Information*

1. Introduction

The financial sector, which is evolving extremely rapidly, is facing a new paradigm to grow driven by technology. The government as well as major companies' responds to the development of new financial business models, known collectively as 'Financial technology' or 'FinTech' [1], will be importance in positioning for the growth of the financial sector. It is a term used to describe the business operating applied to any technology in the financial services. It has attracted the focused attention of the interested parties in the finance sector. According to another report [6], it was observed that the average value of investment in FinTech companies from 2011 to 2014, by round. This represents a large and rapidly growing FinTech industry.

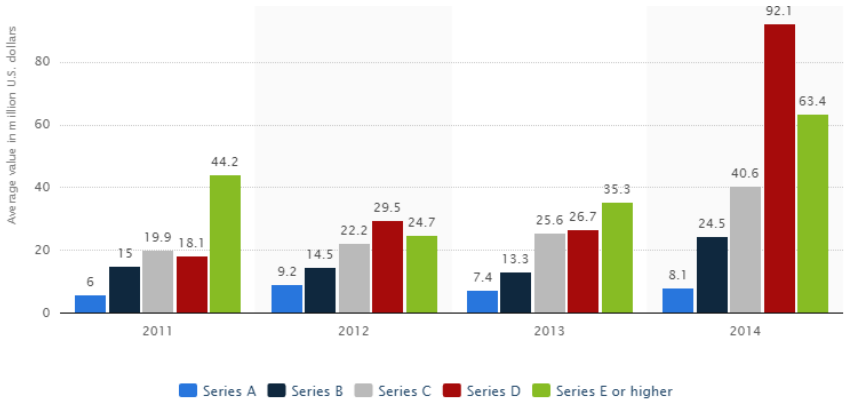

Figure 1. Average value of investment in FinTech worldwide, by round (in million U.S. $)

There are many good and bad things about FinTech-driven paradigm shift in financial services [19,20]. This new paradigm poses challenges for financial sector in balancing the potential benefits of development with the potential risks. Most of customers want to have the easiest and safest access to personalized finance services such as deposits, payments,

[1] Corresponding author

ISSN: 1738-9976 IJSIA

and wire transfers. But they are not used to handling such new technologies and services. They are also very concerned about the security problems. In trend of Korea particularly, the high penetration of smartphones and mobile payment services suggest significant potential demand for smartphone-based electronic payment services as shown in figure 2[23, 24]. With a new generation of FinTech companies who are leveraging the Internet, mobile and cloud computing, these continues that are changing the way financial services are increased. There is one challenge on how secure that we face in this environment. Key growth area of FinTech is in finding more efficient methods for ensuring privacy and security.

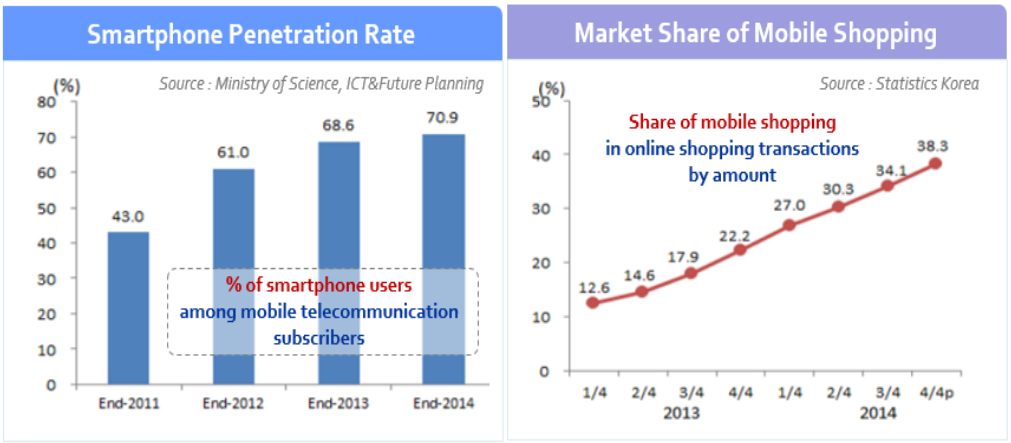

Figure 2. Using smartphone and mobile shopping in Korea

In this paper, we give an overview of the trends of the FinTech technology (Section 2), point out related security and privacy risks (Section 3). And then we discuss the approach method for processing data based on trust how a financial technology can be achieved for preserving and protecting data (Section 4).

2. FinTech Technology Trends

2.1. NFC Technology

Common technologies in the field of the financial sector have been developed. Near-field communication, or NFC [2, 3], that is the most representative technology of this, is earlier forms of mobile payments to handle transactions using scanning system such as a barcode and a QR code. In the financial sector, NFC is considered as an enabling technology and it has gained further legitimacy within FinTech. The concerns using NFC based mobile are also little less as in the process of payment. [4]

But, the important step in the mobile payment transaction is the secure element [3]. NFC can exchange various data including personal information, and this chip has to store any encrypted payment information. It can be accessible when it's activated at an NFC POS terminal or similar device. Obviously, we need for an extra layer of protection to prevent unwanted access and to protect critical payment information or sensitive personal data.

2.2. Security Authentications for FinTech

The key components of the FinTech in service of the Non-face to face transactions are user authentications system. These days, there are several authentication technology studies[15,16], such as the two major ones being certificate and SMS authentication. But to provide new services, it is essential to improve alternate authentication technologies.

Basically according to Gartner [5], it can be divided into the four categories by authentication factors.

Table 1. Categories by Authentication Factors

Category	Detail	Example
Knowledge authentication	The way to use what you know is one of the most common ways in security.	· Password based text · Image-based authentication · Virtual keypad
Authentication tokens	The method such as OOB (Out-of-band) authentication methods makes use of other channel.	· OOB – such as SMS, email · Utilizing the OTP tokens that stored in other device
Inferential authentication	The way is using the information based facts (it is not only what you know).	· Q&A methods to seek answers
Biometric authentication	It relies on the unique biological characteristics of users to verify identity.	· Using identified biological traits – such as fingerprint, hand geometry, iris patterns and voice waves – in smartphones

The best way to preserve the information is to use multi-factor technologies as mentioned above Table 1. Combined with the existing technology related to financial security, it will provide better FinTech infrastructure.

2.3. Cloud Computing Service

Many FinTech firms utilize a cloud service using cloud computing technologies [21,25], because it can offer the benefits of cloud such as an almost unlimited amount of computing power, storage space and fast speed. In the future, it may be expanded or reduced rapidly according to use levels. And the cloud has built in security capabilities. FinTech providers ensure protection of financial institutions by creating infrastructures for compliance. They put effort into developing integrated solutions to support financial technologies.

But there are many reasons to avoid the public cloud. Individual's data cloud be at risk, and people who are stored a cloud database are more susceptible to attacks. It is more efficient to develop a private or hybrid cloud or data storage system.

3. Security Issues and Requirements

Unfortunately, the speed and efficiency of new internet technologies is reflected in rising cybercrime [8,13,14]. The financial sector that security has enhanced is no exception on online platforms. No matter how convenient we provide a service, FinTech will be hard to expect if we don't keep important assets of clients safe[22]. In the financial sector particularly, it is very difficult to prevent and to detect as advanced threats, so the extent of the damage cannot be foreseen. In Korea, the domestic financial market is consistently expanding with micropayment and remittance market about FinTech, but concerns also would increase. According to a survey why do you not use mobile payments by [7], 78.3% of internet users who answered the survey are bothered about 'information leakage'.

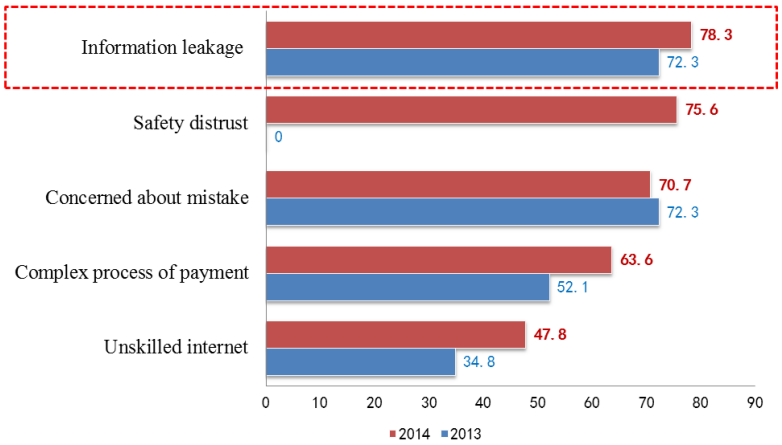

Figure 3. The Reasons for not Using Mobile Payments (% of respondents)

Therefore, the strong security is essential for growth of FinTech industry[10,12]. Figure 3 shows the overview process for FinTech service-provision environment. In fact, the existing network environment and the FinTech environment are not significantly different[9,11]. The important thing to consider is the financial platform including the bank server. So it should include not only high performance but also strong security.

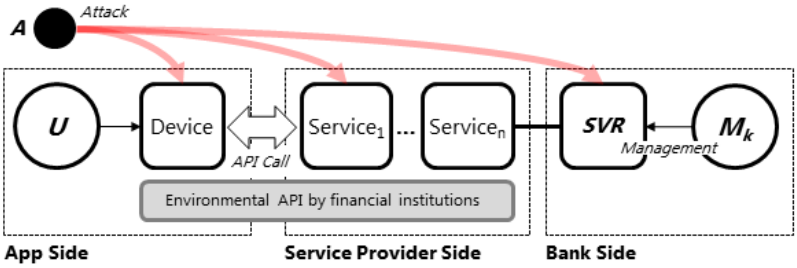

Figure 4. Overview of the basic FinTech Service-Provision Platform

These confidence measures could be the key to success in the open network environments. We introduce new or existing sets of risks for the financial security (see Table 2): ***A*** defines an attacker who hacks into systems, i.e., a financial computer system, network, and an app in smartphones; ***U*** means a customer who ultimately uses an app or is intended to ultimately get a service; and a person or a program that has a system of administration authority expresses M_k.

Table 2. Sets of Risk Impact about Applying FinTech

Possibility of attack	Distribution of vulnerable points	Possibility of detection	Impact
Difficult	**Limited**	**Average**	**Dangerous**
· ***A*** puts a malicious server, or attacks DDoS at ***SVR.*** · ***A*** steals the certificate key of a financial computer. · ***A*** hacks user app, and then he can control it.	· ***U*** ignores encryption for their data in smartphone. · M_k doesn't discover potential threats and vulnerable points. · ***A*** executes a man-in-the middle attack (and phishing, SMS phishing, etc.) · ***A*** steals the phone, but it is secured with locks.		· ***A*** hacks into a financial computer to get the high transactional results of financial services. · ***U***'s confidential data to create high valued services for ***U*** can be leaked.

Most dangerous thing in a table is that handling sensitive or confidential data, such as non-public personal information and personally identifiable information, in financial services comes with a large risk[17,18]. We address the privacy concerns when using FinTech services:

- **Difficulties of the Non-face to face transactions.** To provide new financial services, it is important to solve this problem in the system what we now call financial services. Many people believe it is under-invested and less safe than face to face.
- **Possible re-identifying individuals for high valued financial services.** Even if the system collected tenuous related public information, the process of re-identifying individuals refers to using anonymized data to match individual or sensitive information in public datasets.
- **Leaking of creating sensitive and identifiable information.** The system for FinTech is becoming new forms of social interaction. And to provide individual customized services, the system needs to collect non-public personal information and to analyze gathered data. If an accident occurs, it is expected to have a huge impact because related financial information includes.

In light of this, the privacy is an important security requirement in FinTech.

4. Data Processing Approach for Preserving Privacy

4.1. Proposed Data Processing System

The most important objective of financial systems is safety probability, which should protect any financial information in transaction. Absolute availability is important for trade of financial services as well. To achieve this objective, the data processing system for FinTech must be preserved safely, and in particular privacy aspects must be protected during the lifetime of systems for financial services, i.e., a smartphone, a reader, sensors, and a financial server. We focus on a solution for protecting personal critical information which is processed at core of financial systems.

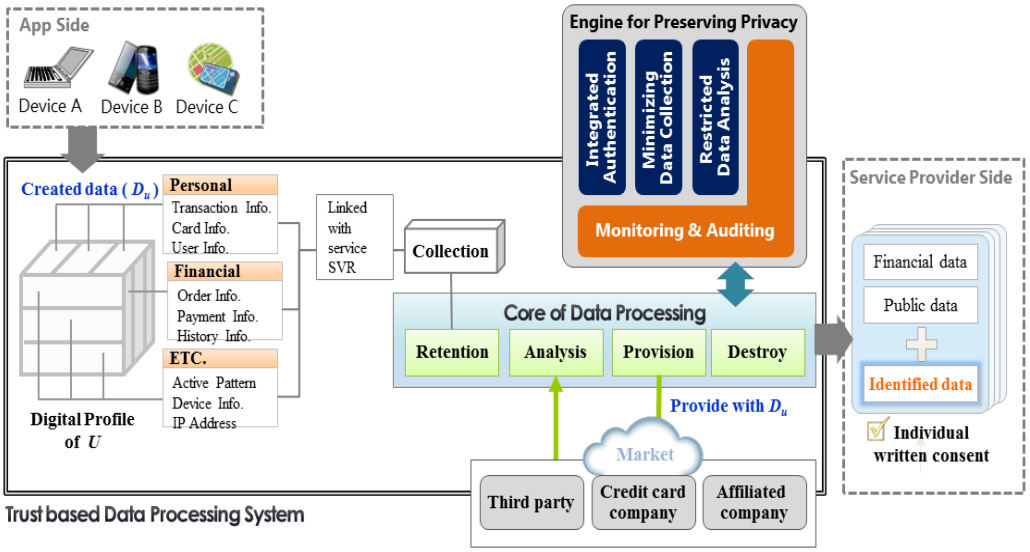

Figure 5. Data processing approach to preserve and protect for privacy

1) Integrated authentication: *Applying the certificated token*

It is important to prevent access to unauthorized parties because an authentication is a primary protection. For example, when ***U***, that is the user, uses it for financial services such as a payment and a transfer, our mechanism provides a public key to ***U*** and encodes it. The system then generates the certificated token C_k which can verify ***SP***, that is the service provider. It will confirm transactions based on trust among the interested parties (i.e., ***U***, ***SP***, and financial organizations) for FinTech services.

2) Minimizing Data Collection: *Access permission with informed consent*

Among the collected information of ***U***, the personal information including a financial statement is especially important to preserve confidential in such environments. The personal information, that is D_u, on FinTech related servers can be encrypted, and the system holds D_u, and ***U*** holds the certificated token C_k. Nobody can access it without ***U*** permission, and Authorized ***SP*** can access stored data or for what purposes. Basically, the system can obtain the collection of all personal information with the prior informed consent. It has to minimize data collection or retention.

3) Restricted Data Analysis: *Additional verification if necessary*

Usually in order to FinTech services to customize for ***U***, ***SP*** need to use massive data independently gathering and analyzing a wide range of data to help personalize ***U***'s online experience. Therefore the system preserves analyzed information for confirmation and verification of transactions, and stores them using strict cryptographic rules. There are ways to protect that D_u that supports them that limit the level of confidential that we entail. So the high confidential information of D_u is hided, it should not be shared. With that, we should have multiple options for additional verification in order that newly created apps and services in the FinTech environment can only be used within certain system. In representative example, a blockchain-based solution can apply to integrate into any platform or system, and it is more secure than that used one central authentication system, because this solution distributes verifying authority by using a digital token among all peers in the blockchain[2]. In peer-to-peer network on the blockchain, it can check and verify whether ***U*** belongs to a suitable participant or not. Generated transactions would be validated and recorded on the blockchain.

4) Monitoring and Auditing

The system has complete transparency over what data is being collected and used about ***U*** and how ***SP*** are accessed. Monitoring is detecting and observing about the process for abnormal behaviors between different transactions. And auditing performs the role of grasping situations that are found as system violations. This mechanism involves audits for various types of system violations based on the gather finding of inside the system.

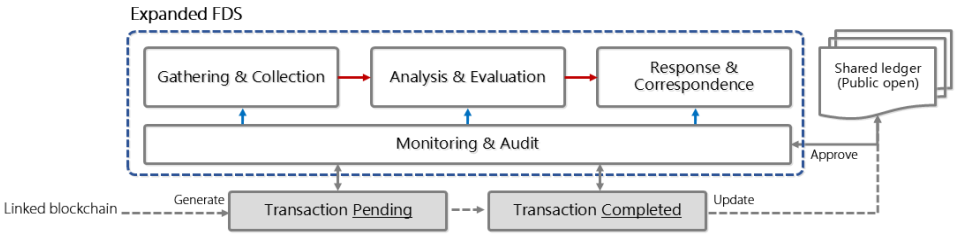

Figure 6. Expanded FDS for Monitoring and Auditing

In order to perform with this system, a key function is the expanded FDS (Fraud Detection System) that is collected data about accidents that occur. And it is detected abnormal behaviors by examining patterns and required additional verification when fraud is detected.

[2] A blockchain technology concepts a transaction database shared by all nodes participating in a system, and it has peer-to-peer distributed technology characteristics. (For more details, please check 'Blockchain' written by Swan and Melanie)

4.2. Analysis Protocol

Based on our proposed system described in the previous section, we introduce a key algorithm for the authentication and the additional verification using the certificated token.

This illustrates the implementation for the user and the service provider. As illustrated, the creation of the certificated token C_k can be accomplished using several options such as user's individual information. C_k is U's identity that is comprised of key-pairs such as public and private. And C_k of U specified should match the public key what SP retains. In this, it is using *Match computes* algorithm.

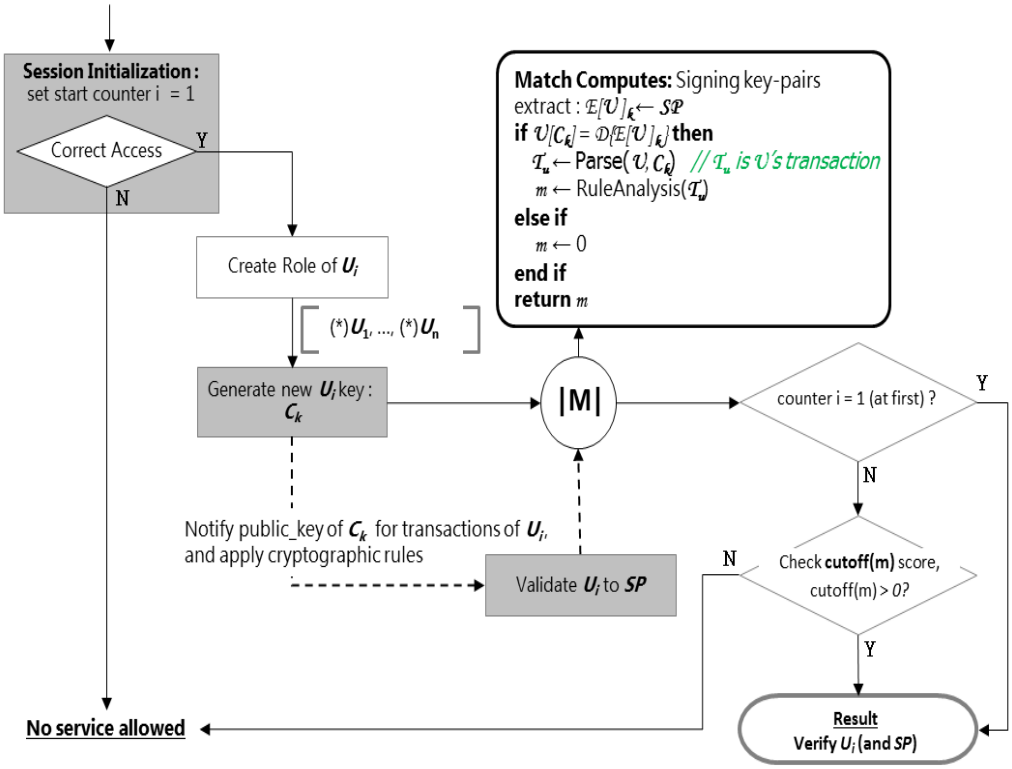

Figure 7. The Key Algorithm for Authentication and Verification

5. Conclusion

Financial technology (FinTech) is an emerging key technology that provides simplifying finance and high transaction value services for the users. These situations generated by FinTech come with risks, and a myriad of FinTech companies do not even need to abide by financial regulations or related laws as yet. That is FinTech is not sufficiently enhanced to bear security and privacy risks.

In this work, we proposed the approach method for processing data based such as strong authentication function. This approach has been detailed in scenarios of various attacks, where the user generates non-public information such as financial in an environment using FinTech. It provides a strong alternative to the currently used methods, and suggested requirements are essential in protecting and ensuring user's personal information. Further research is required to develop a trust-based financial system, including overall and scalable security mechanisms.

Acknowledgments

This work was supported by the Sungshin University Research Grant of 2016.

References

[1] Susanne Chishti and Janos Barberis, The FINTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries, John Wiley & Sons, **(2016)**.
[2] Vinod Sharma, NFC based Mobile Payments, Linked in, Available at https://www.linkedin.com /pulse/nfc-based-mobile- payments-vinod-sharma, **(2015)**.
[3] Seokhoon Kim and Ha-Min Kwak, A Study on the Countermeasure Technology for Fin-Tech Optimized Financial Security, Journal of Convergence Society for SMB, 5 **(2015)**, pp. 25–30.
[4] Shishir Kumar Singh, New Trends in Payment Security: NFC and Mobile Payments, ISACA Manila Professional Development Center, **(2016)**.
[5] Ant Allan, A Taxonomy of User Authentication Methods, Gartner, **(2014)**.
[6] The Statistic Portal, Average value of investment in Fintech worldwide from 2011 to 2014 by round, Statista, Available at http://www.statista.com/statistics/380147/average-fintech-investment-by-round/, **(2016)**.
[7] Kyu-Soo Kim and Seul-Kee Lee, Research and implications of payment behavior for Korea in 2014, Report on Payment and Settlement, **(2015)**.
[8] Vittorio P. Illiano and Emil C. Lupu, Detecting Malicious Data Injections in Wireless Sensor Networks: A Survey, ACM Computing Surveys (CSUR). 48, 2 **(2015)**.
[9] Jesse Elwell, Ryan Riley, Nael Abu-Ghazaleh, Dmitry Ponomarev and Iliano Cervesato, Rethinking Memory Permissions for Protection Against Cross-Layer Attacks, ACM Transactions on Architecture and Code Optimization (TACO). 12, 4 **(2016)**.
[10] Raef Mousheimish, Yehia Taher and Béatrice Finance, Towards smart logistics processes: a predictive monitoring and proactive adaptation approach, Proceedings of the 2015 International Conference on Software and System Process, **(2015)** August 24–26, Tallinn, Estonia.
[11] C.L. Philip Chen and Chun-Yang Zhan, Data-intensive applications, challenges, techniques and technologies: A survey on Big Data, Information Sciences, 275 **(2014)**, pp.314–347.
[12] Matthew Marshall, David S. Kirk and John Vines, Accountable: Exploring the Inadequacies of Transparent Financial Practice in the Non-Profit Sector, Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, **(2016)** May 7–12, San Jose, CA, USA.
[13] Youngran Hong and Dongsoo Kim, A Study on the Information Technology Security Review Process in Finance, Proceedings of the 17th International Conference on Electronic Commerce, **(2015)** August 03-05, Seoul, Korea.
[14] Sufatrio, Darell J. J. Tan, Tong-Wei Chua, Vrizlynn L. L. Thing, Securing Android: A Survey, Taxonomy, and Challenges, ACM Computing Surveys (CSUR). 47, 4 **(2015)**.
[15] Chandra K. H. Suresh, Sule Ozev and Ozgur Sinanoglu, Adaptive Generation of Unique IDs for Digital Chips through Analog Excitation, ACM Transactions on Design Automation of Electronic Systems (TODAES). 20, 3, **(2015)**.
[16] Stefano Calzavara, Gabriele Tolomei, Andrea Casini, Michele Bugliesi and Salvatore Orlando , A Supervised Learning Approach to Protect Client Authentication on the Web, ACM Transactions on the Web (TWEB). 9, 3, **(2015)**.
[17] Kyong Jin Kim and Seng Phil Hong, The Sensitive Information Management System for Merger and Acquisition (M&A) Transactions, International Journal of Applied Engineering Research (IJAER). 10, 13, **(2015)**, pp.33623-33625.
[18] Kyong Jin Kim and Seng Phil Hong, A Study on the Trusted Verification Process for Protecting Assured Privacy from Big Data Analytics, International Journal of Applied Engineering Research (IJAER). 10, 21, **(2015),** pp.41790-41793.
[19] Sangsu Jeong, A Discussion to the Effects of FinTech on Information Security, Internet and security focus, **(2015)**, pp. 4-32.
[20] Sungbok Lee, Fintech and Korea's Financial Investment Industry, Korea Capital Market Institute, Capital markets WEEKLY. 2 **(2015)**.
[21] LG CNS Report, Differences between Korean and Global Financial Security Technology through FinTech!, Available at http://www.lgcnsblog.com/inside-it/differences-between-korean-and-global-financial-security-technology-through-fintech/, **(2015)**
[22] Seung-Soo Shin, Yoon-su Jeong and Ju-Jin An, A Study of Analysis and Response and Plan for National and International Security Practices using Fin-Tech Technologies, Jornal of Convergence Society for Small and Medium Business, 5, 3, **(2015)**, pp.1-7.
[23] KISA Report, Excavating research areas of FinTech through the analysis of its relevant technologies and policy trends at home and abroad, Korea Internet & Security Association, **(2016)**.
[24] Yonghee Kim, Jeongil Choi, Young-Ju Park and JiyoungYeon, The Adoption of Mobile Payment Services for "Fintech", International Journal of Applied Engineering Research, 11, 2, **(2016)**, pp.1058-1061.

[25] Seong-Hoon Lee and Dong-Woo Lee, A Study on Fintech Based on Actual Cases, International Journal of u- and e- Service, Science and Technology, 9, 8, **(2016)**, pp.439-448

Authors

Kyong-Jin Kim, she graduated with a B.S. in 2007, with a M.S. in 2009 and with a Ph.D. in 2013 from the Sungshin Women's University. She joined the Information Security lab as a postdoctoral fellow in March 2013. Her research interests focus on privacy protection, security framework, and access control.

Seng-Phil Hong, he received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for Ph.D at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree in computer science from KAIST University in Korea. He is actively involved in teach and research in information security at Sungshin Women's University, Korea. His research interests include access control, security architecture, Privacy, and e-business security.