International Journal of
Emerging Multidisciplinary Research

ISSN : 2546-1583
Volume 1, Number 1, September 2017
https://doi.org/10.22662/IJEMR.2017.1.1.043

Trends and Implications of Mobile and Online FinTech

Sunghyuck Hong[1], Sanghee Park[2] and Noe Lopez-Benitez[3]
[1,2]Div. of Information Communication, Baekseok University, KOREA
[3]Department of Computer Science, Texas Tech University, USA

Abstract

Background/Objectives: With the advent of the FinTech era, which is an IT technology-based financial service, the service has been transformed into a service emphasizing user-friendly convenience, and new and innovative services are always pouring out. **Methods/Statistical analysis:** However, due to the nature of FinTech, personal information, financial information, and physical information can be easily exposed, so countermeasures against security threats are essential. Even if we provide innovative services, if we can not provide reliable service and do not get customer's trust, **Findings:** we will not only lose customers but also result in the decline of brand value. **Improvements/Applications:** Therefore, this paper examines the security threats of the FinTech market, domestic and overseas industries, and proposes countermeasures to protect consumers from increasingly intelligent and organized security.

Index Terms

FinTech, Mobile Security, Trend of Online, Market Analysis.

Corresponding author : Sunghyuck Hong
sunghyuck.hong@gmail.com

• Manuscript received July 18, 2017.
• Revised August 8, 2017; Accepted September 1, 2017.
• Date of publication September 30, 2017.

I. INTRODUCTION

A. FinTech

FinTech, as shown in Figure 1, is a combination of finance and technology and refers to a new form of financial services based on IT technology. It means providing new forms of financial services regarding structure and delivery system and technique, using IT[1]. These days, it is recognized as a useful payment service regarding payments such as Kakao Pay, Apple Pay, and PayPal Co.

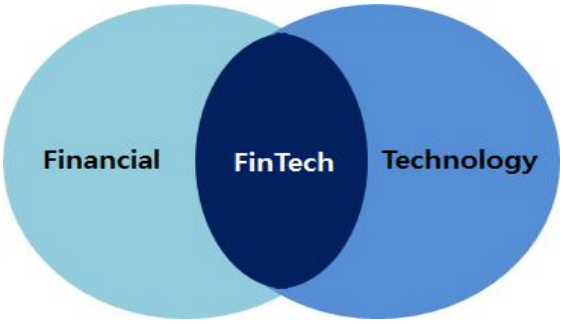

Fig. 1. The concept of FinTech

According to research by the Korea Internet Development Agency, With the proliferation of mobile markets, as shown in Figure 2, the financial transactions have increased through not only mobile channels but also online. Under this are witnessing a glimpse of the possibility of development of the FinTech industry[2].

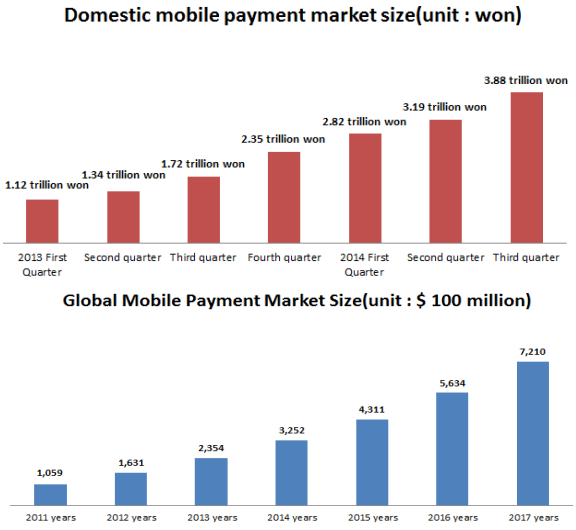

Fig. 2. Mobile payment market scale

As the FinTech market grows, there is also a growing concern about security threats. Services that simplify or omit authentication procedures are often introduced. Because it is focused on convenient. When information leaked to a hacker who has special intentions, Online FinTech that are used accredited certificate can suffer secondary damage to the information stored in the financial institution. There is also a risk of leaking information stored in other financial institutions that share the accredited certificates. Mobile FinTech applications lack complex procedures such as installing a separate security program, such as ActiveX and have the advantages of using the mobile devices service wherever they are connected, but the mobile FinTech application also means that security is equally vulnerable.

II. RELATED RESEARCH

A. FinTech security threat

Security accident potential is becoming increasingly higher as FinTech focus on convenience and simplify the authentication procedure for existing security. Types of security threats are becoming increasingly intelligent and daring. These threats can threaten not only monetary damages but also physical, mental harm, and even life. Types of security threats that can arise include.

First, There is a security threat to biometric authentication. Streamline the authentication procedure that you enter by hand. And, by recognizing human body, behavioral patterns, voice recognition, fingerprint, and iris, A probabilistic authentication approach has emerged to match the error range between the measurement results and pre-registered templates. However, it is highly likely to be certified by others with bio information leakage, error range matching error. Compared to one's own handwriting. In fact, that in 2014, Operate an iris, using a picture of Putin president. And, a case has been reported to unlock the smart phone by used tools similar to fingerprints[4]. Information that is used as a personal identification value, such as fingerprint and iris, is particularly susceptible to information leakage if it can not be reissued and can not be changed.

Second, There is a threat to the easy payment security incident. Naver Pay, Kakao Pay, and Bentmo used authentication procedures to simplify authentication procedures using certified certificates and enter a simple password or was easy to make financial transactions using the information stored in the address book stored on the smart phone. Instead of a difficult combination of English, number, and emoticons, the convenience of a 6-digit number of passwords increased. But, that means it has become vulnerable in security. In 2014, the denial use ratio of overseas PayPal Co, which provided a simple payment service through an environment based authentication using Beacon, is 0.3%. And, PayPal showed 1,500 times higher security accident rates

compared to Korea, which introduced authentication methods through public certification or SMS[5].

Third, There are ID Federation vulnerabilities. These days, there is a growing number of websites introducing OAuth protocols that allow other websites to used without membership. That connected account at the implementation process of these protocols is easily exposed to hacking.

Finally, There is a threat to financial security. Because the FinTech service operates through partnerships with various companies, the area of responsibility between companies is blurred, and there is a danger of a blind spot in the security system. Also, if a security accident occurs in one place, there is a high possibility that security accidents will spread to other linked financial institutions.

B. Industry status FinTech in Korea

Unlike the rapidly growing international FinTech industry, Although the domestic FinTech is well equipped with an IT infrastructure, it stays at a standstill. In the latest pay zone, big ICT companies such as Naver and Daum have entered the remittance and Payment Payments Market but failed to produce any particular achievement[6]. The Settlement service of the IT platform, mobile payments service using NFC method emerged. And, as shown in Table 1, banks and card issuers are pushing for new services that combine smart technology.

Table. 1. FINTECH CASE OF DOMESTIC FINANCIAL COMPANY

Company	Introduction Time	Service
Kookmin Bank	August 2012	Smart branch
Shinhan Bank	July 2012	Smart branch
Samsung Fire&Marine	January 2009	Online car insurance
Shinhan Card	March 2013	Use Big Data
Hyundai Card	January 2012	Use Big Data

In fact, there are currently large ICT companies in Korea that are rushing to FinTech markets, but the commercialization performance of the FinTech service is nonexistent compared to abroad. The reason why the domestic FinTech industry was stagnant was that businesses were in a difficult situation to push ahead with the FinTech project due to the excessive entry barriers and regulations by the rule of law. But, as the government is actively expressing its willingness to raise ties with FinTech, renewed interest in FinTech is increasing interest and participation in financial firms. For example, Samsung Electronics adopted a credit card payment service by acquiring a credit card payment service that was bought by a U.S.-based credit card company in the United States at the end of 14 years. As shown in Table 2, the FinTech industry is expected to be activated with various support strategies of government's FinTech industry promotion strategy.

Table. 2. PROGRESS STATUS OF DOMESTIC FINTECH

Field	Domestic Status
Payment	Cash, Credit Card, Wire Transfer, Foreign Remittance, Foreign Exchange
Remittance	Online payment service utilizing platform of non-financial company
Deposits and loans	Establishment of introduction plan of internet bank
Investment fund recruitment	Investment-type plastic funding bill will be passed by the National Assembly.
Asset management	Introduction of online fund supermarket
Insurance	Introduction of online insurance supermarket
Etc	Establishment of Big Data Guideline and establishment of integrated credit information concentration agency

C. Industry status of overseas FinTech

As shown in Table 3, investment in overseas FinTech industries has continued to grow steadily from $ 9 million in 2008, In particular, financial data analysis and software sector investments have increased.

Table. 3. GLOBAL FINTECH INVESTMENT(USD BILLIONS)

2008	2009	2010	2011	2012	2013
9.3	9.8	19.8	24.3	27.0	29.7

Global ICT companies offer various types of remittances and payments service based on payment demand and mobile network on their site. And recently, based on innovative technology and idea, start-up FinTech enterprises are actively advancing to the FinTech industries with differentiated business models.

III. RESPONSE PLAN

A. Response plan from FinTech Security Threats

FinTech is essential to maintain trust in financial transactions while supporting convenience and diversity since it uses personal information.

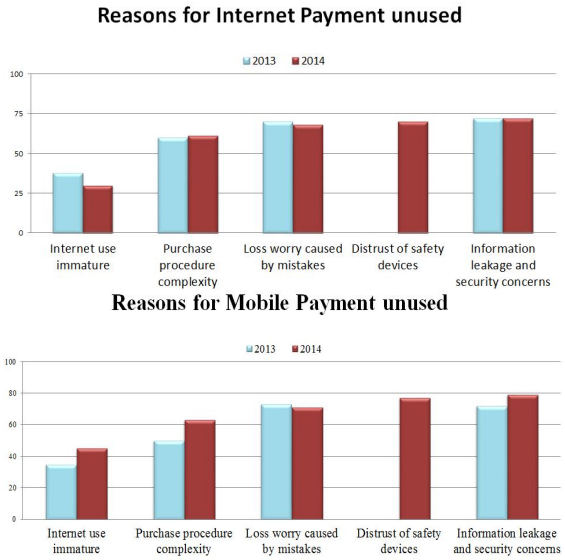

Fig. 3. Results and Implications of the Usage of Payment Methods for 2014

As shown in Figure 3, according to the survey results of the use of the payment method in 2014 by the National Statistical Office, show that the " information leak and security concerns " for various reasons are the highest among the various reasons why the Internet or mobile payments are avoided. These days, After occupying the user's device first and obtaining information, there is a way to attack confidential information or personal information by obtaining access to the internal system. Companies offering FinTech services should come up with measures to secure the safety of the FinTech service based on the government's policy to attract consumers. Measures to secure safety include the following.

First, Ensure that technological neutrality is attained. Examples of representative technical neutrality are the compulsory use of authorized certificates. Technical neutrality means 'not forcing use of specific technologies or services'[7]. However, the official certificate used by the government is actually PKI(Public Key Infrastructure) based security solution. As the government implemented such policies, the technology sector became a Non-competitive state, and technological competitiveness was eliminated, and the security level of the public certificate was not improved. Most of the financial institutions still adhere to the existing methods, although the mandatory use of the authorized certificate and the compulsory installation rules of the security program are abolished. To implement a materially neutral technology, it is necessary to abolish certain technologies such as authorized certificates, Active-X, etc., and allow financial firms to apply IT freely.

Second, it has to switch from 'pre-check' to 'post-intensive'[8]. As the FinTech service changes and develops, the type of supervision of regulatory about security needs to be changed as well. Therefore, as it becomes Spontaneous motivation to FinTech companies, it is unnecessary to insist to pre-regulatory, such as traditional regulatory methods. Rather than eliminating the certification method assessment committee system and the security review system about the new electronic financial transaction, it should strengthen the post-regulatory on the level of security.

Third, You need to share cyber security threats. Millions of malicious codes are occurring each day for About 3.5 billion internet users worldwide. Under these circumstances, cyber threats are becoming more intelligent and expanded to IoT. Under these circumstances, joint security barriers can be stacked by sharing information about cyber threats collected by each firm. The United States has already enacted information sharing laws and operates a shared platform for threat information through the Department of Homeland Security. And, In August 2014, the nation is expanding its scope of information sharing by operating a cyber threat information analysis and sharing systems at the Korea Internet Security Agency.

Fourth, Security is ensured user authentication technology can be applied. Real name authentication methods are provided that allow real name authentication without meeting each other in FinTech service. Of these authentication methods, it is necessary to apply the certification technology suitable for the FinTech service, considering the convenience of security and service[9].

Fifth, We need to protect biometric authentication. NIST presents a security guide when introducing biometric authentication, such as responding to authentication threats by others, responses to biological information leaks, and criteria for forge discriminant minimum performance[10].

- Response to authentication threats by others
  - Performance requirements of biometric authentication products(EER 0.001 less than)
  - Should be certified as Other authentication methods in case of over number of authentication failure
  - Requires verification of using of biometric authentication sensors that meet criteria
- Response to bio information leakage
  - Removed bio-formation samples immediately after extraction of feature information
  - Store and compare in user terminal internal. Provide bio template re-issuance function when sent externally.
- Provides for minimum criteria about forge verification(90%)

Sixth, the financial authorities should change their future direction and should break away from individual regulations on business subjects. The traditional financial regulation regulates the financial institution by dividing the financial business to a licensed system. But, it is very unrealistic that financial authorities regulate the number of Internet platforms business people in the era of FinTech. Deviate from the traditional regulatory framework, And, If you regulation on centralized issues, financial authorities can have a broad mandate to create and interpret the regulations that apply to all Internet service providers, not to mention specific industries.

Like this, If the regulation way change, it will make sense to change the personality of the financial authorities. If the existing financial authorities play the role of a supervisor, it is now seen as a necessary time to the role as a supporter. Supervise about FinTech company. At the same time, we need observer and facilitator role to support the necessary skills. In the case of China, China established the ‘ National FinTech Security Technology Specialist Committee ’ in 2015 August. And, The Chinese FinTech Association, the Internet Association, is overseeing and supporting the companies and is seeking to match the intrinsic nature of the FinTech industry[11].

Finally, as shown in Figure 4, FinTech should be protected by establishing procedural systems for prevention, detection, and recovery. Protect against security threats with secure threats from terminal protection or user authentication, establish FDS, and Financial accidents information should be shared. If an issue arises, the cause must be analyzed and dealt with in case of a loss of accident, and compensation and dispute settlement should be repaired quickly.

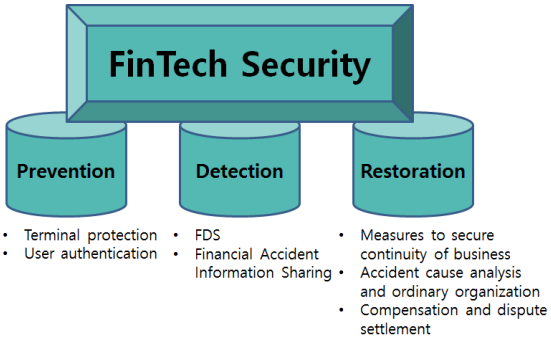

Fig. 4. Ensuring the safety of FinTech service

IV. CONCLUSION

Currently, the FinTech industry is poised to change and reform. At the same time, information security is the goal and obligation to be pursued in the development of the FinTech Industries. Even if new and innovative technologies and services are available, If you don't have reliability in security and safety, Increasing convenience will end up becoming meaningless. To protect against increasingly advanced threats, always predicting accidents, preventing, and corresponding procedures should be managed repeatedly. Financial firms should increase the competitiveness of the financial industry by caution of the personal information of their clients through a safer authentication approach rather than authentication way using the accredited certificate. It can be difficult to predict the direction of developing FinTech. But, If we combine the technologies of the biometric technology and accredited certificate technologies with our global company's terminal platforms, we will be able to expect a safe and creative FinTech that will revolutionize the internet environment in the future.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (NRF-2017R1A2B1003394)

REFERENCES

[1] H. Okada, S. Yamasaki, V. Bracamonte. (2017). Proposed classification of blockchains based on authority and incentive dimensions. *Advanced Communication Technology (ICACT), 2017 19th International Conference on*.

[2] Sung, C. (2016). Excavating research areas of FinTech through the analysis of its relevant technologies and policy trends at home and abroad. *Korea Internet Promotion Agency*. Retrieved from https://www.kisa.or.kr/public/library/report_View.jsp?regno=022087&pageIndex=3&searchType=&searchKeyword=

[3] Giseong, J. (2015). A Study on Activation Measures of Local Mobile Easy-to-use Payment. *Convergence security journal*, 15(4), 79-88.

[4] Sanghwan, P. (2017). Security requirements at FinTech. *The Journal of The Korea Institute of Communication Sciences*, 34(3), 15-22.

[5] Kiseung, B. (2016.5). Certified Certificates, Internet Explorer Economic Key Security Technologies. *etnews*. Retrieved from http://www.etnews.com/20160517000250.

[6] Sunyoung, P. (2015). FinTech : New growth engines in the financial industry. *Industrial Engineering Magazine*, 22(4), 22-27.

[7] Jeongkuk, P. (2015). Fintech and Information Security. *Information Science Magazine*, 33(5), 23-32.

[8] NIS, MSIP, KCC, MOSPA, NSRI, KISA. (2016). National Information Protection White Paper 2016. *NIS, MSIP, KCC, MGAHA*.

[9] Byungho, S. (2015). Financial focus : Notes on the introduction of non-faced real name authentication. *Korea Institute of Finance*, 24(3), 10-11.

[10] P. Grassi, M. Garcia, J. Fenton. (2017). Digital Authentication Guideline. *DRAFT NIST Special Publication 800-63-3*.

[11] Taeeon, K. (2017). The paradigm of FinTech security. *Korea Institute of Communication Sciences*, 34(3), 11-14.