Kang *Hum. Cent. Comput. Inf. Sci.* (2018) 8:32
https://doi.org/10.1186/s13673-018-0155-4

Human-centric Computing and Information Sciences

RESEARCH Open Access

Mobile payment in Fintech environment: trends, security challenges, and services

Jungho Kang*

*Correspondence:
kjh7548@naver.com
Department of Information Security, Baewha Women's University, Seoul, Republic of Korea

Abstract

Due to recent developments in IT technology, various Fintech technologies composing of finance and technology are being developed. Especially, because of rapidly growing online market and supply of mobile devices, the need for mobile Fintech payment service that enables easy online and off-line payment has increased. According to the 2013 report by market research company Gartner, purchase related global mobile payment market size was predicted to grow from $45.1 billion in 2012 to $224.3 billion in 2017 with average annual growth of 38%. The study will surveyed the recent trends of mobile Fintech payment services and categorized them based on the service forms to suggest requirements and security challenges so that better and securer service can be provided in the future. First, the study defined existing payment services and Fintech payment services by comparing them, and analyzed recent mobile Fintech payment services to classify mobile Fintech payment service providers into Hardware makers, Operating System makers, payment platform providers, and financial institutions to show their common features. Finally it defined requirements that mobile Fintech payment services must meet and security challenges that future and present mobile Fintech payment services will encounter in the perspective of mutual authentication, authorization, integrity, privacy, and availability. Through the suggested study, it is expected that mobile Fintech payment services will develop into more secure services in the future.

Keywords: Fintech, Mobile payment, Security challenges, Finance technology

Introduction

Although the financial system is already largely digitalized, mobile payment services are used in limited areas, due to various regulations and marketability [1, 2]. However, as numerous mobile devices are supplied worldwide and online shopping is being activated, digital mobile payment market has grown largely [3–7]. According to the 2013 report by market research company Gartner, purchase related global mobile payment market size was predicted to grow from $45.1 billion in 2012 to $224.3 billion in 2017 with average annual growth of 38%, and According to Capgemini's 2016 report, the world's non-cash transaction volumes grew by 8.9% in 2014 to 387.3 billion and it was predicted that in 2015, it will increase by 10.1% to reach 426.3 billion [8]. As the mobile payment market is activated and mobile payment frequency used by users increased, the need for simplified payment has increased. In all digital environments including environments where financial infrastructure is

well-established and developing nations with lacking financial environment where currencies such as cash is not well distributed, the need for simple and convenient mobile payment services is increasing [9, 10]. Especially according to the 2014 report by Gartner, as mobile payment transaction started in Africa and developing nations in Asia, it is expected that mobile payment population will show strong growth until 2016 [11]. To provide simplified mobile payment services to these users and to provide financial services specialized for users and service providers, Financial Technology (Fintech) composing of finance and technology are being developed worldwide [12–14]. According to the 2014 report by Accenture, the volume of investment on global Fintech venture companies has increased more than three times in 5 years from $920 million in 2008 to $2.97 billion in 2013. Also, it was predicted that market share of US financial companies will drop from 85.7% in 2013 to 60% in 2020, and it is predicted that it will be replaced by Software (SW) companies [15]. However, As the mobile payment service market growing, mobile payment services have been exposed to many threats [16–19]. So the requirement and security challenges for mobile Fintech payment service must be defined to develop a secure and convenience service. In order to securely provide such a mobile payment services, a variety of mobile payment and security studies are being conducted. Kadhiwal et al. defined security methods that can be applied to mobile payments according to type and summarized security properties, and Linck et al. proposed a security guideline that satisfies the customer by surveying and questioning mobile payment security issues from the customer's viewpoint [20, 21]. Dahlberg et al. categorized mobile payment research progress over 8 years from 2002 to 2015 based on the mobile payment framework [4]. Also, Zhou et al. identified and analyzed the factors affecting continuance intention of mobile payments so that mobile payment service providers could continue to attract customers to use payment services [22]. However, although many researches on mobile payment are being conducted, to the best of our knowledge, there is no research as of yet that summarizes the security requirements by comparing and analyzing the existing payment service and mobile Fintech payment service. In order to provide mobile Fintech payment service securely and conveniently in the rapidly growing mobile payment market, it is necessary to define requirements for Fintech payment service and classify security challenges. The study explained the mobile Fintech payment infrastructure comparing existing payment services to show the relationship between them and then analyzed the recent trends in mobile Fintech payment service to classify into form of providing payment service and organized the requirements that mobile Fintech payment services should have. Also, the study analyzed and categorized security challenges that mobile Fintech payment services face by suggesting the requirements for it.

The study is organized as follows. "Mobile Fintech payment services" discusses it comparing traditional payment services, and "Trends of recent mobile Fintech payment services" analyzes and categorizes it with service providers. "Requirements and security challenges for mobile Fintech payment services" explains 6 principles for each of them. "Future work" show the next study about large IT companies in Fintech industry, and I finally finish the work by "Conclusion".

Mobile Fintech payment services

In this chapter, I discuss the mobile payment services for Fintech comparing traditional payment services.

In principle, using payment services requires from the user opening an account at his or her bank and receiving a payment instrument (card, etc.) linked to the account from the issuing bank to pay merchants online or offline. Merchants who have requested payment must exchange payment information with the financial institution in order to receive funds while providing consistent payment service from the various financial institutions. So they send the payment information received from the user to the acquirer securely through the payment processor without being sent directly to the financial institution. The acquirer forwards the payment information to the relevant financial institutions so that the payment can be made to merchants in the future. This series of processes for payment through mobile devices is called mobile payment service. As shown in Fig. 1, mobile payment service can be divided into existing payment service that directly links to financial institutions and Fintech payment service that links with financial institutions through IT companies. Payments in the both services are made directly to the service provider or through an integrated payment agency, a subcontractor that supports both existing payment services and Fintech payment services. However, although traditional payment services use IT technology like Fintech payment services do, it has some limitations and problems over the Fintech payment services. If a mobile payment in the existing payment service is made through different financial institutions, a different payment method must be used for each financial institution even when using the same service, since the financial institution system and platform which provide traditional payment services were not created for payment services and were not largely specialized for user convenience [23–25]. In other words, the existing payment service directly utilizes financial institution systems so that it must be dependent on the financial institution system and policy where the payment instrument is issued [26]. For

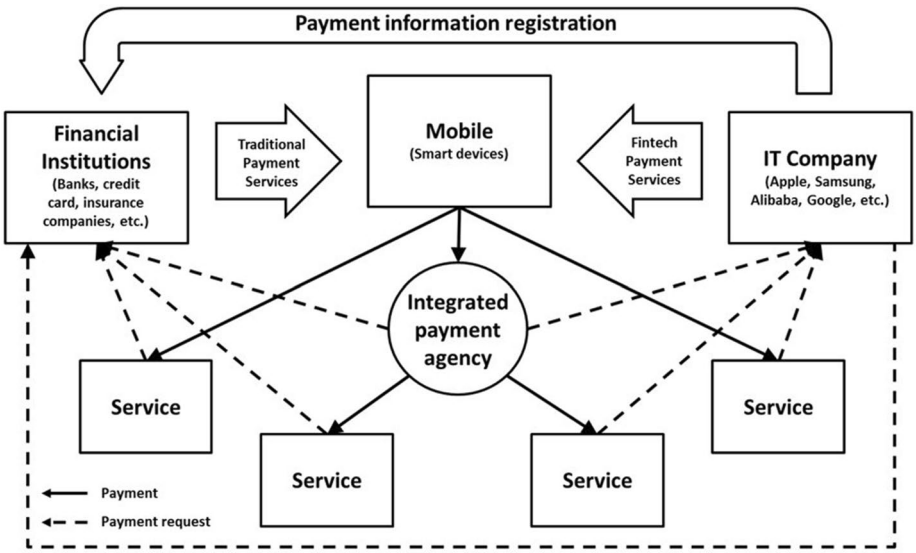

Fig. 1 Mobile payment infrastructure in Fintech environment

example, when a payment is made using an existing payment service, in order to use the card offline for each situation, one must always have multiple cards to use them when making a payment, and online, one must individually enter the card information to make a payment. In addition, it is difficult to use customized services because the benefits are provided to the users in accordance with the policy of the financial institution used as a payment means, such as a card or a bank separate from the service paid by the user. On the other hand, unlike existing payment services, Fintech payment service enables users who are using a specific financial institution to use an independent customized payment service that is not dependent on the payment service of the financial institution but that is tailored to the convenience of the user. As shown in Fig. 1, Fintech payment service is linked with existing financial institutions and digital payment infrastructure based on IT technology, where the user's payment information is registered with the financial institution so that the user can use the payment service independently from the financial institution system, and therefore it offers a much more versatile and convenient payment method than traditional payment services. Also, without the need to be specialized for a single financial institution, by linking with various banks and card companies, the user can utilize various payment services of financial institutions with a single payment method. For example, if a user has inputted multiple bank accounts and card information on the Fintech payment service, the user can easily pay for the transaction by simply selecting the desired payment institution in the Fintech payment service. In addition, because Fintech payment service providers can customize payment services not only for the user needs but also the merchants, compared to traditional payment services, it has more diverse purposes and methods of use.

Trends of recent mobile Fintech payment services

In this chapter, I show the recent mobile Fintech payment service trends. As shown in Fig. 1, there are many mobile Fintech payment service providers which can be classified.

Recent mobile Fintech payment services

Apple pay

Apple pay is a mobile Fintech payment service that is dependent on both HW maker and OS maker [27]. It only works on Apple devices and iOS manufactured by Apple and like Samsung pay, payment service can be used without unlocking the lock screen and biometric authentication is executed through print recognition. Also by making payments through encrypted one-time token information, information is not exposed externally and by supporting a separate Secure Element (SE) that can independently and securely store sensitive information, security was improved. Also it was made so that Apple pay app does not need to be executed to make payments and by making it accessible on Apple watches as well as iPhones, it has greater convenience. However, unlike Samsung pay, it only supports Near Field Communication (NFC) which means there are few stores that can be used and it lacks compatibility for using in existing payment infrastructure.

Samsung pay

Samsung pay is a HW maker based payment service which can be used in the latest Samsung phones running android OS after S6 series [28]. Samsung pay enable

payment through Samsung pay by linking with numerous financial institutions globally and once a payment method is registered, payment can be made without inputting payment information again. Also, unlike other mobile Fintech payment services, without the need for unlocking the lock screen, pay service can be used by executing the Samsung pay app. Through biometric authentication through fingerprint recognition, security was improved and recently they are preparing services through iris recognition. Also, In addition to SE for sensitive payment information, Host Card Emulation (HCE) is utilized which enables accessing payment information with only the software by storing in the cloud, and by using tokenized credit card information tokens, exposure of the payment information to the outside was prevented. Like Apple pay, Samsung pay can conduct off-line payment through NFC and considering most stores currently are Magnetic Secure Transmission (MST) affiliates rather than NFC, it supports payment method through MST to improve convenience and compatibility.

LG pay

LG pay is a HW maker based payment service which can be used in the LG G6 phones running android. LG Pay is able to make payment by connecting to various financial institutions like Samsung pay. Although only available in Korea, few financial institutions are available, they operate in a magnetic way and are available in most stores. Another advantage of LG pay is that it can be used without releasing the lock screen like Apple Pay and Samsung Pay because it is made by the hardware manufacturer. If you swipe your finger up from bottom, you can get a list of available cards right away. Samsung pay has to close all existing browsers and apps to make a payment, but LG pay can use it without having to. Payment authentication can be selected from simple passwords and fingerprints. Whenever a payment was made for secure payment, LG pay generated a new virtual card number to prevent the card number from being leaked. Therefore, we have applied double security system with password and virtual card number for the payment. Since LG pay supports only the payment of magnetic type, the payment range is smaller than that of Samsung Pay, which also supports NFC.

Android pay

Android pay is an OS maker based Fintech payment service [29]. Although a service called Google wallet was first introduced before Android pay, by omitting prepaid rechargeable card function from Google wallet and enabling registering and using cards in the Android pay app, it was newly introduced. Like Apple pay, payments can be made only through NFC and user authentication is done through fingerprint recognition or passwords during payment. Also, like Samsung pay and Apple pay, security was improved through token technology using virtual card numbers through HCC. Also, unlike Samsung pay and Apple pay which works only on Galaxy series, iPhone, and Apple watch, Android pay has high versatility, supporting Android phones that have Android 4.4 KitKat or above. However, the app must be executed when using Android pay which lacks convenience compared to Apple pay.

Alipay

Alipay is a payment platform provider based mobile Fintech payment service that can be used regardless of HW maker or OS maker [30]. It is a payment service introduced by China's largest E-commerce company Alibaba which can be used regardless of mobile device or OS. Alipay uses a method where a unique barcode or Quick Response (QR) code is created on the smart phone screen when user authenticates, so that when the cashier scans the code, the payment information delivered to the smart phone is approved, and it does not require high-priced smart phones that have fingerprint recognition function for user authentication or NFC for near field communication. Also it has the advantage that the service provider making the payment does not have to install separate hardware other than barcode scanners, such as POS devices. However, because it has the disadvantage that dedicated Alipay app must be installed for the service provider, apart from areas where Alipay is widespread, it has limited use. Alipay uses a method where the user separately opens an Alipay account linked to a bank to recharge cash.

Wechatpay

Wechatpay is the payment function of Wechat messenger which is widely used in China. Because users can transfer or pay currency with Wechat pay QR code, Wechatpay is mainly used as payment method in many offline stores in China as well as online. Wechatpay also has secured service customers through a large number of social media clients called Wechat Messenger, which prevents customers from leaking to the other messengers and attracts new customers. If you register your financial payment card in Wechat, you can easily make payment and remittance without a card.

Starbucks siren order

Starbucks app, like Alipay, is a payment platform provider based mobile Fintech payment service. Starbucks which has branches all over the world enabled payment through points on gift cards rather than actual cash before Fintech started being introduced and currently through siren order in the Starbucks app, provides mobile Fintech payment service to order and pay for Starbucks products. Without the need to order and pay at a Starbucks branch, advance order can be made through the app and online payment is done through Starbucks gift cards or affiliate cards. Although it has limited versatility due to it being limited to payment of Starbucks products, but providing customized ordering service such as personalized menus and history, it can provide Starbucks specialized service.

PayPal here

PayPal here is a mobile POS for merchants making payments rather than users purchasing services [31]. While traditional payment services required payment software and hardware such as POS or barcode readers making a burden for small-scale stores to install and maintain, PayPal here enables users to pay with credit cards or PayPal accounts through linking with financial institutions by attaching a PayPal here reader on normal smart phones. By providing an easy payment service for small stores and areas where traditional payment services such as POS or barcode readers have not been activated, it increased the versatility of payment service.

Stripe

Stripe is a service providing mobile payment module. Rather than using their own financial infrastructure, they provide a platform for pay-as-you-go payments. In addition to its own platform, it is also compatible with third-party platforms such as Facebook, Twitter, and Applepay. Especially, on Facebook and Twitter, you can pay by button only. In addition, it provides a simple interface to developers as well as users, and it is dedicated to security essential to payment.

Mobile payment with VISA

Visa is a credit card that accounts for 60% of international credit accounts worldwide. Although it does not have its own mobile payment platform, it provides payment services in connection with various mobile payment platforms such as Apple Pay, Samsung Pay, and Google Pay. Visa is a financial institution that works with the user's financial account to process the actual payment process. The mobile payment services mentioned above are used in conjunction with financial systems such as Visa MasterCard, Amex, and others.

CitiPay

Citi bank is a financial institution that can open an account and can manage the customer's account, and also provides a credit card by itself. Already CitiBank offers a Citi Pay mobile payment service, attracting a large number of customers using mobile apps and credit cards. When you choose the card you want from the Citi Pay app, you will receive a barcode that you can pay and is available at the merchant that Citi Pay is affiliated with. It combines the functions of financial institutions with the mobile IT technology, but it has the disadvantage that only the Citi credit card can be used and payment can be made only at the franchisee.

Classification of mobile Fintech payments

Analyzing the mobile Fintech payment services currently being used, mobile Fintech payment service providers can be divided into HW makers, OS makers, payment platform providers, and financial institutions as shown in Fig. 2.

Fig. 2 Classification of mobile Fintech payment services

HW makers

HW makers based payment services are dependent on HW makers and only operate on mobile devices developed by the corresponding HW makers. Generally, it implements a method of securely storing sensitive user financial information within mobile devices in HW module form, and it enables payment by linking traditional financial institution systems with SW such as OS or Apps. Because it is dependent on HW, independently it can improve security through adding biometric authentication technology such as fingerprint recognition or iris recognition that require HW modules and it can also select physical payment methods such as NFC and magnetic secure transmission. Also, unlike other SW based payment services, it enables payment without the need for executing mobile apps or unlocking lock screens.

OS makers

OS makers based payment services are dependent on OS makers and operate only on mobile devices installed with the OS of the corresponding OS makers. Generally, OS based payment services are linked to traditional financial institution systems like HW based payment services and makes payments through mobile Apps independently or dependent on HW. Sensitive user financial information is stored on security HW module of the mobile or is managed through implementing SW based trust zones. Also by linking with biometric authentication modules installed on the mobile device, it can provide additional authentication service. Payment can be made through the Internet or according to mobile device, can be made through NFC, and if it is not linked to HW, the corresponding payment service can be used only if lock screen is unlocked and the dedicated payment App is executed.

Payment platform providers

Payment platform providers based payment services are developed and provided based on their products or services. Unlike HW makers and OS makers based payment services, payment platform providers based payment services cannot directly compose payment service environment on mobile because the mobile devices and OS were not developed by them, but based on established mobile devices and OS environment, under the pretense of satisfying the requirements of each mobile device and OS maker, it can provide payment service. Because it is a payment service independent from OS and mobile devices can provide customized payment services for corresponding payment platform providers and it can provide payment services regardless of mobile device or OS. Also because service payments can be made through cards and points without linking with financial institutions, it independently gives benefit to the users which can make them dependent on the corresponding payment platform provider. However, when providing services linking to financial institutions, it has the limitation that it needs to satisfy security requirements that the financial institution indicates.

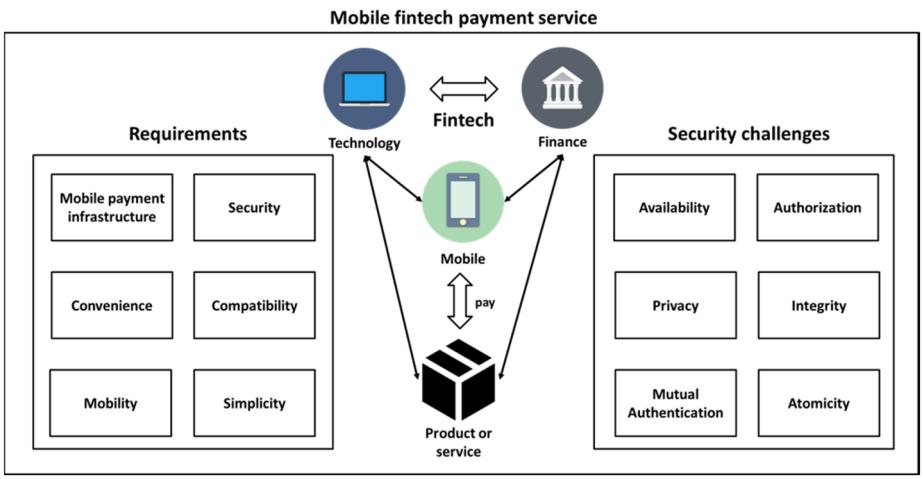

Fig. 3 Requirements and security challenges for mobile Fintech payment services

Financial institutions

Financial institution payments are payment services provided through actual financial institutions using IT technology or by converging with other payment services. Like payment platform provider based payment services, because it does not develop mobile devices or OSs, it cannot directly configure payment service environment and payment services can be provided only if it satisfies the requirements of mobile device and OS maker. Also because it is dependent on financial institutions, unlike other payment services, payments can be made only through accounts and cards of the corresponding financial institution. However, because it can control its own financial system, it can additionally provide financial services from the traditional financial system as well as payment.

Requirements and security challenges for mobile Fintech payment services

Based on mobile Fintech payment service trend analysis, this chapter organized requirements and challenges for mobile Fintech payment services as shown in Fig. 3.

Requirements for mobile payments in Fintech

As Fintech technology develops, various forms of mobile payment services are being provided based on IT technology. These mobile payment services can deliver services in various forms such as HW makers based, OS makers based, payment platform providers based, and financial institutions based, but commonly, they must satisfy the following requirements.

Convenience

Mobile Fintech payment services must be more convenient than traditional payment services [32–34]. For example, an existing payment service tries to provide the convenience to the user, but since the payment platform, User Interface (UI), or additional benefit is dependent on the financial institution, there is a limitation in meeting needs of the users. If the user must go through various procedures through

the payment service, it is not appropriate for Fintech mobile payment service. Fintech mobile payment services, unlike traditional payment services, must provide customized payment services based on user's needs and convenience minimizing conscious billing procedures through convenient payment procedures such as simple password or biometric authentication.

Mobile payment infrastructure

Mobile Fintech payment services must have mobile Fintech payment infrastructure where desired services can be paid through mobile anywhere and anytime [35, 36]. Even if a Fintech mobile payment service has superior convenience or function compared to traditional payment service, if it does not have the infrastructure to use the payment service, the service cannot be used. For example, if certain communication protocols such as NFC must be used or if it can only be used on certain services, the versatility of mobile Fintech payment service becomes very limited. Especially, current mobile Fintech payment services have incomplete infrastructure compared to traditional payment infrastructure and sometimes it lacks availability compared to traditional human systems.

Compatibility

Mobile Fintech payment services must be compatible with traditional payment services and financial environment such as banks and card companies [37–39]. Introduction of mobile Fintech payment service is not a simple replacement but convergence with existing payment service and it must have compatibility to utilize existing payment services and infrastructure. Through this compatibility, without the need for changing existing payment service based systems and infrastructure, both can be used and it can be widely used without resistance from users. Also by minimizing changes in existing payment services, it must minimize the costs to implement the new environment.

Mobility

Mobile Fintech payment services must be supported by the mobility of mobile devices [3, 40, 41]. Due to the nature of mobile devices, they need to be continuously on the move with the user and communicate externally based on wireless networks. Existing payment service was made through a designated reader or external device at a designated place for payment. Mobile Fintech payment services should not require additional devices, apart from external devices that was already used for existing payment services, regardless of where the mobile device is and where the payment is made. Thus, by maximizing utilization of the infrastructure provided by the existing payment system to ensure the mobility of the payment service, the convenience of the user can be maximized.

Security

Because payment services are directly related to the assets of users, security is a requirement in mobile Fintech payment service [42–44]. So that sensitive security information of the user is not exposed to malicious attackers, mobile payment services must be constructed securely in terms of both HW and SW, and even if multiple payments have been

made with the same payment service, information about the payment method must not be exposed to unauthorized third parties. Also from information used during the use of mobile Fintech payment service, the user or user information must not be exposed. If secure payment service is not provided, it cannot only cause monetary damages to users but also invade user privacy based on payment information the user used.

Simplicity

Mobile devices are becoming lighter and smaller with the development of IoT technology [45, 46]. This trend will lead to the development of various wearable devices, and many users will wear 3–4 wearable devices in the future. The current mobile payment service is optimized for smartphones, but it should also be able to make payments on wearable devices that do not have a small screen or screen. In addition, since wearable devices are small in size, most of them are poor in computing performance, so it is necessary to develop a light payment system to provide a simple payment service.

In order for mobile payment service to be successful, mobile payment infrastructure, compatibility, mobility, security, and simplicity should be ready as mentioned above. You can still launch mobile payment services, even if you do not meet all of these requirements. But they will not be available to users at the end of the day, because the other competitors will have. In particular, security factors are background areas that users can not see or experience directly, but once a security incident occurs, users will lose trust and will no longer be used even if they meet other conditions.

Security challenges for mobile Fintech payment services

In this chapter, security challenges that must be solved for mobile Fintech payment services to develop in the future was classified divided into mutual authentication, authorization, integrity, privacy, atomicity, and availability.

Mutual authentication

In mobile Fintech payment service, mutual authentication between mobile Fintech payment service providers and existing financial infrastructures must be conducted before conducting payment. The absence of mutual authentication can cause critical financial damage not only to the user and service subject but also the payment financial institution. If a malicious attacker assumes the identity of a mobile user, it can deliver false payment information to the service subject to avoid payment and if it assumes the identity of service subject, payment can be received from the user and not provide the service. Because in mobile Fintech payment service, not only face-to-face but also remote Internet payments can be made, mobile devices must be authenticated as well as the user during authentication. However, if the procedures of mutual authentication become complex due to security, it can rather make mobile Fintech payment services more complex compared to traditional payment services which can greatly reduce convenience. Due to recent developments in IT technology, biometric authentication such as fingerprint or iris recognition is being widely used to conveniently authenticate remote users.

Authorization

Mobile Fintech payment must be accessible only for authorized users and also the information exchanged for the payment must be accessible only to the authorized subjects. Also payment subjects must not be able to see information other than approved information even if it participates in the payment process. For example, users must provide passwords for payment method information to the service provider to proceed with mobile Fintech payment service but sensitive payment information should be accessed and seen only at the financial institution that actually deals with money. If authorization on information is not appropriately given to payment subjects, hackers can easily intercept the payment information of users without mutual authentication and furthermore, they can control the information. In addition, even service subjects can claim excessive fees without the knowledge of users and financial institutions can figure out conception patterns of users without the agreement of users.

Integrity

Mobile Fintech payment services must have integrity. If the payment information or information exchanged by mobile devices to make payments are modified by malicious attackers or external factors, it can have direct damage to financial assets of the users. Also, unlike actual cash or checks, mobile Fintech payment services exchange digital currency which means users cannot immediately be alerted of damages and if integrity is not kept, users can continuously be exposed to repeated damage. Also, to indicate to both the user and payment service that normal payment has been made, it needs to be able to prove the integrity of the payment.

Privacy

If malicious attackers can figure out payment information or patterns of users, on top of financial damage on users and payment subjects, it can greatly invade the privacy of users. Also because mobile Fintech payment goes through payment service of an IT company rather than directly through a financial institution, it has the problem that regardless of the will of the user, payment information can be delivered to all subjects participating in the payment which can harm the privacy of the users. Information used in payment must be delivered encrypted, divided into purpose and sensitivity, and payment subjects must not be able to figure out information excluding the minimum information necessary to proceed with the payment. For example, when a user pays for a service using card information through mobile Fintech payment service, the merchants must not know the card information and the card company must not know the user purchased service history. One-time card information or tokens are being widely used to protect user privacy.

Atomicity

Mobile Fintech payment service must completely conduct a payment or not at all. Due to the development of IT technology, payment methods have been simplified but due to the increase of subjects participating in the process of payment, it has become more complex. During the process of payment, if payment is halted during the process due to external factors or internal error, even if the user attempted payment,

determination subject might not properly receive the payment request and the user might not be able to receive service even after processing payment or the service provider might not be able to receive payment even after providing service. Mobile Fintech payment service providers must make it so that payment is made only when the payment process is completely conducted from start to finish to prevent these types of damages and must indicate to the participating subjects that the payment has been successfully made.

Availability

While mobile Fintech payment service simplifies payment and expands the domain of availability compared to traditional payment services, it must not provide lower security compared to traditional payment services. Also, while maintaining the same level of security as traditional payment services, it must have the availability where payment can be made simply whenever and wherever the user wants. However, because it does not directly go through financial institutions to conduct payment, it is not easy to maintain the same level of security as traditional payment services. Also, if various security procedures are demanded on the user to have high security, it can rather have reduced convenience compared to traditional payment services. Mobile Fintech payment service must have the availability that satisfies both the security requirements of subjects participating in payment and user convenience.

In order for a mobile payment service to be securely provided, it must have mutual authentication, authorization, integrity, privacy, atomicity, and availability as mentioned above. Financial services should be more rigorous than other services because it directly affects property if one vulnerability is found in the service. If you do not meet those requirements, it will cause not only a simple service error but also a catastrophic property damage to the user. While the existing payment services and the mobile payment service security requirements are similar in many respects, mobile payment services run on a variety of devices and operating systems and lack the resources to run security programs. In addition, since it is mobile, it is not fixed in one location, so it is difficult to build a security system than existing payment system. Many companies are constantly releasing mobile payment services, so in order to survive the competition, it is necessary to develop services in consideration of all these aspects.

Future work

In this paper, we examine the mobile payment market in the Fintec environment. In the next study, we will investigate the settlement market of the techFin environment in which large IT companies enter the finance industry. As the boundaries of each industry area are gradually being destroyed, the financialization of large IT companies will become faster and faster. Future research will explore the financial services of large IT companies with significant potential in the mobile payment market and study security requirements.

Conclusion

Mobile payment services that were provided exclusively by financial institutions until recently developed into various mobile Fintech payment services due to rapid development of IT technology and increase in needs for convenient payment methods. Unlike traditional payment services, payment services can be used with simple password or biometric authentication, and by independently providing payment services without the need for different payment services for each financial service, it has enabled mobile payment through a single payment service. Especially, it provides simplicity to the online/offline store that sells the goods, rather than providing services only considering the payment users. However, although there is much research conducted on mobile payments, to the best of our knowledge, there are no studies that summarize security requirements by comparatively analyzing mobile Fintech payment service with existing mobile payment services. The study defined each characteristic according to mobile Fintech payment service provider type classified into HW makers, OS maker, payment platform provider, and financial institution, and defined requirements that mobile Fintech payment services must meet differentiated from traditional payment services. Also by organizing mobile Fintech services that are currently actually used such as Samsung pay, Apple pay, Android pay, Starbucks app, Alipay, Wechatpay, PayPal here, Stripe, and mobile payment with Visa, the study analyzed the recent mobile Fintech payment service trends. Lastly, the study analyzed security challenges that can arise when developing mobile Fintech payment services to be secure and convenient, to define from the perspective of mutual authentication, authorization, integrity, privacy, and availability. The study put its purpose on describing the currents trends and aiding the development of a better mobile Fintech payment service in the future through mobile Fintech payment analysis. Now that most IT companies do not have the ability to open an account, the mobile payment system is dependent on the existing financial institution or is necessarily connected, but in the future, IT companies will add or bypass their own account functions. In future research, we will investigate and study the mobile payment process that develops mainly in the IT-oriented financial companies called TechFin.

Authors' contributions

JK surveyed the recent mobile Fintech payment services, and analyzed them by classifying into four categories. Finally he suggested the requirements and security challenges for mobile Fintech payment services. The author read and approved the final manuscript.

Authors' information

Jungho Kang was born in Jeju, Korea. He received the Ph.D. of Computer Science & Engineering from Soongsil University, Seoul, Korea in 2014. He is currently teaching students in the Department of Information Security, Baewha Women's University, Korea and working as a software architecture and consultant. Also He is an associate editor of JIPS (Journal of Information Processing Systems), HCIS (Journal of Human-centric Computing), a guest editor of the JoS (Journal of Supercomputing) and a member of the KIPS (Korea Information Processing Society). He has been on the organizing committee of many international conferences. Prof. Kang had written various papers in his research interests and his research interests are network, security, IoT, multimedia, NFC.

Acknowledgements

This work was financially supported by Baewha Women's University.

Competing interests

The author declare no competing interests.

Availability of data and materials

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Funding

Not applicable.

Publisher's Note

Received: 15 May 2018 Accepted: 9 October 2018
Published online: 30 October 2018

References

1. Lee AR, Ahn HY (2016) Fintech users' information privacy concerns and user resistance: investigating the interaction effect with regulatory focus. J Korea Inst Inf Secur Cryptol 26(1):209–226
2. Park SW, Lee IY (2013) Anonymous authentication scheme based on NTRU for the protection of payment information in NFC mobile environment. J Inf Process Syst 9:461–476
3. Thakur R, Srivastava M (2014) Adoption readiness, personal innovativeness, perceived risk and usage intention across customer groups for mobile payment services in India. Internet Res 24(3):369–392
4. Dahlberg T, Guo J, Ondrus J (2015) A critical review of mobile payment research. Electron Commer Res Appl 14(5):265–284
5. José Liébana-Cabanillas F, Sánchez-Fernández J, Muñoz-Leiva F (2014) Role of gender on acceptance of mobile payment. Ind Manag Data Syst 114(2):220–240
6. Perez AJ, Zeadally S, Jabeur N (2018) Security and privacy in ubiquitous sensor networks. J Inf Process Syst 14:286–308
7. Yang S et al (2012) Mobile payment services adoption across time: an empirical study of the effects of behavioral beliefs, social influences, and personal traits. Comput Hum Behav 28(1):129–142
8. Capgemini R (2016) World payments report 2016. Federal Reserve Bank of Dallas Financial Industry Issues
9. Gulamhuseinwala I, Bull T, Lewis S (2015) FinTech is gaining traction and young, high-income users are the early adopters. J Financ Perspect 3(3):16–23
10. Han YH, Lim HK, Gil JM (2017) Hierarchical location caching scheme for mobile object tracking in the internet of things. J Inf Process Syst 13:1410–1429
11. Steeves D (2016) The social impact of FinTech in Nigeria. The FinTech book: the financial technology handbook for investors, entrepreneurs and visionaries, pp 78–80
12. Zavolokina L, Dolata M, Schwabe G (2016) The FinTech phenomenon: antecedents of financial innovation perceived by the popular press. Hum Centric Comput Inf Sci 2:16
13. Li Y, Spigt R, Swinkels L (2017) The impact of FinTech start-ups on incumbent retail banks' share prices. Hum Centric Comput Inf Sci 3:26
14. Lee SH, Lee DW (2016) Review on Fintech industry in oversea
15. Skan J et al (2014) The boom in global Fintech investment
16. Park YJ, Jang SM (2014) Understanding privacy knowledge and skill in mobile communication. Comput Hum Behav 38:296–303
17. Liang X et al (2014) Security and privacy in mobile social networks: challenges and solutions. IEEE Wirel Commun 21(1):33–41
18. Smalley S, Craig R (2013) Security enhanced (SE) android: bringing flexible MAC to android. In: Proceedings of the NDSS, 2013. https://www.ndss-symposium.org/ndss2013/ndss-2013-programme/security-enhanced-se-android-bringing-flexible-mac-android/
19. Li Q, Clark G (2013) Mobile security: a look ahead. IEEE Secur Priv 11(1):78–81
20. Kadhiwal S, Zulfiquar AUS (2007) Analysis of mobile payment security measures and different standards. Comput Fraud Secur 2007(6):12–16
21. Linck K, Pousttchi K, Wiedemann DG (2006) Security issues in mobile payment from the customer viewpoint, pp 1–11
22. Zhou T (2013) An empirical examination of continuance intention of mobile payment services. Decis Support Syst 54(2):1085–1091
23. Cheong CP, Fong S, Lei P, Chatwin CR, Young RC (2012) Designing an efficient and secure credit cardbased payment system with web services based on the ANSI X9.59-2006. J Inf Process Syst 8:495–520
24. Ondrus J, Pigneur Y (2007) An assessment of NFC for future mobile payment systems. In: International conference on the. management of mobile business, 2007. ICMB 2007. IEEE, New York
25. Niina M, Rossi M, Tuunainen VK (2004) Mobile banking services. Commun ACM 47(5):42–46
26. Chen Z, Li Y, Wu Y, Luo J (2017) The transition from traditional banking to mobile internet finance: an organizational innovation perspective—a comparative study of Citibank and ICBC. Hum Centric Comput Inf Sci 3:12
27. Hein B (2014) Apple confirms iPhone 6 NFC chip is only for Apple Pay at launch. Cult of Mac [on-line].[dostęp 15.09. 2014]. Dostępny w: http://www.cultofmac.com/296093/apple-confirms-iphone-6-nfc-apple-pay
28. Xia H, Hou Z (2016) The effect of samsung pay on Korea equity market: using the samsung's domestic supply chain. Hum Centric Comput Inf Sci 2:18
29. Hsiao KL (2013) Consumer use intention of online financial products: the Yuebao example. Libr Hi Tech 31(2):216–235
30. Tang JO, Yu SM (2010) Online payment system of vending machine based on alipay. J Mech Electr Eng 5:035
31. Dwyer B (2014) Paypal here vs. square
32. Liébana-Cabanillas F, Sánchez-Fernández J, Muñoz-Leiva F (2018) Antecedents of the adoption of the new mobile payment systems: the moderating effect of age
33. Liébana-Cabanillas F, Muñoz-Leiva F, Sánchez-Fernández J (2017) A global approach to the analysis of user behavior in mobile payment systems in the new electronic environment. Serv Bus 12(1):25–64

34. Zhou T (2014) Understanding the determinants of mobile payment continuance usage. Ind Manag Data Syst 114(6):936–948
35. Dahlberg T, Mallat N, Ondrus J, Zmijewska A (2008) Past, present and future of mobile payments research: a literature review. Electron Commer Res Appl 7(2):165–181
36. Jeong JE, Ban YH (2014) A study on analytical comparison between payment processes by different mobile payment types—focus on types of mobile payment schemes used in Korea. J Digit Des 14(2):641–650
37. Tan G, Ooi K, Chong S, Hew T (2014) NFC mobile credit card: the next frontier of mobile payment? Telematics Inform 31(2):292–307
38. Wu J, Liu L, Huang L (2017) Consumer acceptance of mobile payment across time. Ind Manag Data Syst 117(8):1761–1776
39. Yang J, Chang C (2010) A low computational-cost electronic payment scheme for mobile commerce with large-scale mobile users. Wireless Pers Commun 63(1):83–99
40. Cao X, Yu L, Liu Z, Gong M, Adeel L (2018) Understanding mobile payment users' continuance intention: a trust transfer perspective. Internet Res 28(2):456–476
41. To W, Lai L (2014) Mobile banking and payment in China. IT Prof 16(3):22–27
42. Yang Y, Liu Y, Li H, Yu B (2015) Understanding perceived risks in mobile payment acceptance. Ind Manag Data Syst 115(2):253–269
43. Tellez Isaac J, Sherali Z (2014) Secure mobile payment systems. IT Prof 16(3):36–43
44. Zhou T (2014) An empirical examination of initial trust in mobile payment. Wireless Pers Commun 77(2):1519–1531
45. Wong K, Kim M (2016) An enhanced user authentication solution for mobile payment systems using wearables. Secur Commun Netw 9(17):4639–4649
46. Hill C (2015) Wearables—the future of biometric technology? Biometric Technology Today 2015(8):5–9