INFLUENCE OF FINTECH ON MOBILE PAYMENTS

DUSSA HEMANATH

RESEARCH SCHOLAR, S.K.INSTITUTE OF MANAGEMENT,
SRI KRISHNADEVARAYA UNIVERSITY, ANANTHAPURAMU, A.P

Dr. D. PRABHAKAR

PROFESSOR, S.K.INSTITUTE OF MANAGEMENT,
SRI KRISHNADEVARAYA UNIVERSITY, ANANTHAPURAMU, A.P

KALAVALA RAMPRASAD

RESEARCH SCHOLAR, S.K.INSTITUTE OF MANAGEMENT,
SRI KRISHNADEVARAYA UNIVERSITY, ANANTHAPURAMU, A.P

Abstract

Due to recent developments in IT technology, various Fintech technologies composing of finance and technology are being developed. Especially, as a result of rapidly growing on-line market and supply of mobile devices, the requirement for mobile Fintech payment service that enables easy on-line and o -line payment has increased. in keeping with the study of Digital Payment Systems Market in India conducted by Orbis research portrayed that the Indian digital payments industry is forecasted to reach $700 billion by the year 2022, in terms of transactions. in addition, it was expected that quite 80% of urban India can adopt digital payments as an integral part of their daily lives by 2022, and retail shops can follow suit, at an increased adoption rate of 70%. The study will survey the recent trends of mobile Fintech payment services and categorised them supported the service forms to recommend requirements and security challenges so better and securer service can be provided within the future. First, the study defined existing payment services and Fintech payment services by comparing them, and analysed recent mobile Fintech payment services and their worth. Finally, it defined requirements that mobile Fintech payment services should meet and security challenges that future and present mobile Fintech payment services can encounter in the perspective of mutual authentication, authorization, integrity, privacy, and convenience. Through the suggested study, it's expected that mobile Fintech payment services can develop into more secure services in the future.

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

Introduction:

Mobile payment refers to the payment for goods or services or transfer of money through mobiles/smartphones. The mobile payment market is anticipated to grow at a CAGR of 33.8% from 2017 to 2023 to achieve a market size of $4,574 billion by 2023. within the current scenario, services and goods providers extensively supply their services through mobile apps to help customers by providing a simple and convenient looking expertise.

The rise in demand for simple and hassle-free purchase of products and services results in increased preference of customers toward digital and cashless payments. many global players, like Apple and Samsung, have designed new ways to expand their reach and gain a bigger share in the world mobile payment market.

Based on mobile payment type, the mobile payment market is divided into mobile wallets/bank cards and mobile cash. With the expansion in awareness about mobile wallets, together with launch of mobile case apps like Google wallets and Paytm, the mobile case phase is predicted to witness strong growth within the returning years. However, mobile cash is predicted to stay the most important revenue contributor throughout the analysis amount. supported application, retail occupied the most important share within the mobile payment market in 2016. With the advent of hotels and car rental apps, the hospitality & transportation phase is projected to witness the best rate of growth to succeed in $1,087,662 million by 2023.

To provide simplified mobile payment services to those users and to pro-vide financial services specialised for users and service providers, financial Technology (Fintech) composing of finance and technology are being developed worldwide. according to the 2014 report by Accenture, the amount of investment on world Fintech venture corporations has inflated over 3 times in five years from $920 million in 2008 to $2.97 billion in 2013. Also, it was predicted that market share of us money companies can drop from 85.7% in 2013 to 60 minutes in 2020, and it's predicted that it'll get replaced by software (SW) companies. However, because the mobile payment service market growing, mobile payment services are exposed to many threats. therefore, the requirement and security challenges for mobile Fintech payment service should be defined to develop a secure and convenience service. so as to securely offer such a mobile payment services, a spread of mobile payment and security studies are being conducted. Kadhiwal et al. defined security ways that can be applied to mobile payments in step with kind and summarized security properties, and Linck et al. proposed a security guideline that satisfies the customer by measuring and questioning mobile payment security issues from the customer’s viewpoint. Dahlberg et al. categorised mobile payment analysis progress over eight years from 2002 to 2015 based on the mobile payment framework. Also, Zhou et al. known and analysed the factors poignant continuance intention of mobile payments so mobile payment service suppliers may still attract customers to use payment services. However, though several researches on mobile payment are being conducted, to the best of our information, there's no analysis as of however that summarizes the security requirements by comparing and analyzing the prevailing payment service and mobile Fintech payment service. so as to provide mobile Fintech payment service firmly and conveniently within the rapidly growing mobile payment market, it's necessary to outline requirements for Fintech payment service and classify security challenges.

The study explained the mobile payment ecosystem and its forms of payments. Also, the study analysed and categorized security challenges that mobile Fintech payment services face by suggesting the requirements for it. The study is organized as follows. “Mobile payment ecosystem” discusses its differing types, and analyses “Trends of recent mobile Fintech payment services”. And conjointly explained the “mobile payment technology” and its 2 broad categories. “Requirements and security challenges for mobile Fintech payment services” explains 6 principles for each of them. “Future work” show the next study concerning large IT companies in Fintech industry, and that i finally finish the work by “Conclusion”.

Mobile payment ecosystem

The modern payment processing ecosystem involves a complex network of consumers, merchants, banks, and payment/network processors. it's heterogeneous, not solely from the perspective of various sorts of operators, but also due to the existence of varied technologies and operating models. Banks are the traditional operators in this house. However, the expansion in mobile payments has seen new entrants, such as financial technology firms and mobile phone manufacturers, increasing their share. to lead the way for the future of mobile payments, technology companies try to change the landscape of mobile payments with innovative, software-based payment solutions with distinctive options driving a lot of of the process onto their platforms. The industry is increasingly investing in enhanced security and convenience options. local factors play a significant role when it involves the adoption of the technology.

for instance, in emerging economies, the low level of banking penetration has played a crucial role within the development of mobile payment solutions as a provider of financial services.

Types of mobile payments

Mobile payment technology is evolving rapidly, with numerous innovations being explored to shape the future of how consumers make digital payments through mobile payment gateways.

Mobile Wallets

A mobile wallet is simply a digital wallet. in a mobile wallet app, the user will add a card (debit or credit) and store the details associated with the card. this enables users to make payment for his or her purchases with mobile phones rather than using a physical card. One will use mobile wallets to make in-store payments and on-line purchases, pay for digital content, and transfer money. Users can also receive offers, cashback, and rewards on transactions made. Some mobile wallets enable withdrawal, however largely the app is restricted to payments and transfers. They facilitate secure, speedy and hassle-free payments for purchase of goods and services. These wallets are economical and facilitate lower the payment processing time and reduce fraud.

SMS Payments.

Short messaging service (SMS) payment entails paying for products and services using a text message, that is sent via a mobile phone. during this type of payment, the client sends a text message with all the necessary data concerning the transaction to mobile payment providers. The provider clears and settles the dealings between the seller and also the client. the value of the purchase is either side to the monthly charge statement or subtracted from the pre-paid balance. SMS was one of the earliest modes of mobile payments before the advent of smartphones because the ability to text was all that was needed. SMS payment is perceived as additional convenient and safe, because the client isn't required to produce his credit card or bank details and no personal detail is shared throughout transactions. SMS payments are popular in Europe, particularly for making payments for parking and buying bus/train tickets.

Direct Operator Billing

Operator billing is a way to pay through your mobile service provider, permitting subscribers to make purchases and place the cost onto their monthly phone bills. This service is expedited by mobile service providers, who connect millions of consumers through the utilization of simple and fast mobile payments. This mode of payment doesn't use any banking infrastructure. the main benefits of using direct operator billing are financial inclusion and smooth customer experience. the major drawbacks are weaker security, high probabilities of fraud, and huge carrier charges.

Internet Payments

Apart from using mobile wallets, SMS payments, and direct operator billing, one might also make on-line payments through a phone browser, like safari and chrome. this may be done either by manually entering card details on an e-commerce site, like Amazon or by using mobile applications, like PayPal. This technique is thought as wireless application protocol (WAP) payment, that was normally used before the advent of smartphones. WAP is actually a technology utilized by a mobile phone to access the web. This payment technique re-quires a limited-capacity WAP browser and an online connection.

Mobile Banking

Mobile banking is a commonly used application currently as most of the banks have their own mobile applications. Mobile banking refers to the utilization of phones or different cellular devices to perform on-line banking tasks. The user must sign up with the banking app and verify the details of the account. every bank will have a unique sign-up and verification procedure.

Trends of recent mobile Fintech payment services

In this chapter, I show the recent mobile Fintech payment service trends and there are many mobile Fintech payment service providers which can be classified.

Trend 01: Banks becoming platform players to aid collaboration, retain payments' role

Trend 02: Infrastructure rationalization is likely as payments intermediaries come together or evolve

Trend 03: Payment vendors and banks are expected to consolidate their operations to form larger groups

Trend 04: Open APIs enable stakeholder collaboration

Trend 05: Alternate payment channels such as contactless and wearables gain acceptance

Trend 06: Banks and FinTechs explore distributed ledger technology to transform cross-border payments

Trend 07: Instant payments processing likely to become the 'new normal' for corporate treasurers, industry at large

Trend 08: As global cyber attacks rise, regulators focus on data-privacy law compliance

Trend 09: Robotic process automation, machine learning help payment service providers in fraud detection

Trend 10: Payments firms continue to invest in advanced authentication technologies to fight fraud and data breaches

Recent mobile Fintech payment services

A report by PwC observes that up to 28 percent of the payments sector may be taken over by fintech by 2020. This demonstrates the emerging importance of fintech in the financial sector. The following are the top 10 fintech payment companies and their worth:

Square

Based in San Francisco, square is a fintech firm with an estimated price of US$ 5.5B. the company offers mobile payment services. it's launched its app in over a hundred countries and in multiple languages. Currently, the company accepts Apple Pay and is additionally working closely with Snapchat.

Stripe

Based in San Francisco, Stripe is a Fintech Company that allows payment via mobile app or through the internet. According to Stripe insider Lewis Clark, Stripe's valuation is $9.2bn and has raised $440m upto date. Stripe has partnered with Apple, Facebook and twitter to provide e-commerce solutions.

PayPal

PayPal was founded in 1998 with headquarters in Palo Alto, United States. In 2002, the company became a fully owned subsidiary of eBay. PayPal offers online money transfer across the world and is worth $2.8 billion. To open a PayPal account, you need an email address. This email is then linked to your PayPal account. Money can then be securely paid into or transferred directly through your PayPal account. You can also send money to other people using your PayPal account.

Adyen

With a value of around US$2 billion, Adyen is a financial technology company based in Amsterdam. It provides a platform that allows you to make payments despite your physical location. The company has been expanding aggressively to other parts of the world, notably Asia Pacific. Moreover, Adyen has client base close to 4000 merchants including Groupon, Facebook, and AirBnB.

Transferwise

Transferwise is a London based fintech company providing international money transfer. The company was launched in 2011 and currently has over 1 million customers who send more than £800m via the Transferwise platform every month. Transferwise is valued at US$1.5 billion.

Klarna

Klarna is based in Stockholm and is worth over US$1.2 billion. It provides a wide range of financial technology solutions but focuses mainly on online payments. Other services offered include payment for public transport and peer-to-peer cash transfer.

Boku

Boku operates in over 70 countries and is worth $1.2 billion. The company allows consumers to make payments for their online purchases using mobile phones. Boku has a huge potential to serve more consumers especially in jurisdictions where many people do not operate the traditional bank accounts.

Apple Pay

Apple Pay is a product of the US tech giant; Apple, based in Cupertino, California. Apple Pay is a feature built in Apple mobile phones and Apple watch. Although Apple is an established tech company worth $1.4 Trillion, Apple Pay is new creation and is worth about $500 million.

M-PESA

M-PESA is a mobile phone-based money transfer and funding service, launched in 2007 by Vodafone for Vodacom and Safaricom, the biggest mobile network operators in Tanzania and Kenya. The mobile money transfer company was initial launched in Nairobi, Kenya and spread to many other African countries. Currently, M-PESA is getting used even outside Africa in countries like Pakistan. it's calculable to be worth close to $400 million.

Paytm

Paytm is a mobile money transfer service provider based in New Delhi. The company targets the large Indian population that does not have even bank accounts. This gives the company a great potential for growth. Paytm is estimated to be worth about $400 million.

Mobile Payment Technology

There are two broad forms of mobile payments technologies: proximity and re-mote payments. when each party are physically within the same location, it's referred to as proximity payments. in this case, communication between parties is done directly using contactless radio technologies. Remote payments, on the opposite hand, can be done regardless of the payer's location, and are performed using a communication link, SMS, or a mobile application. Proximity-based mobile payments use totally different technologies to establish communication needed for a sure-fire dealing. These are also referred to as point-of-sale (POS) solutions.

Near Field Communication

Near Field Communication (NFC) is the most popular means that of contactless communication between two devices. It permits users to wave an NFC phone over an NFC-compatible payment reader or card machine and transfer data with-out touching the devices. NFC-enabled devices produce a radio frequency current captured by NFC-compatible payment machines using a radio frequency identifier in proximity that reads the information and processes the payment. NFC is really a set of radio-frequency identification (RFID) – a technology that enables identification using radio waves. Transactions don't need multiple levels of authentication to be successful and the benefits include convenience, security, and speed. one of the major disadvantages is that it needs an additional piece of hardware, typically not integrated into smartphones or POS devices. However, an increasing variety of companies are now investment in this technology. Google has launched Google Pay, which supports Master card, Pay Pass, and PayPal offers money transfers between smartphones.

Sound Wave-based Payments

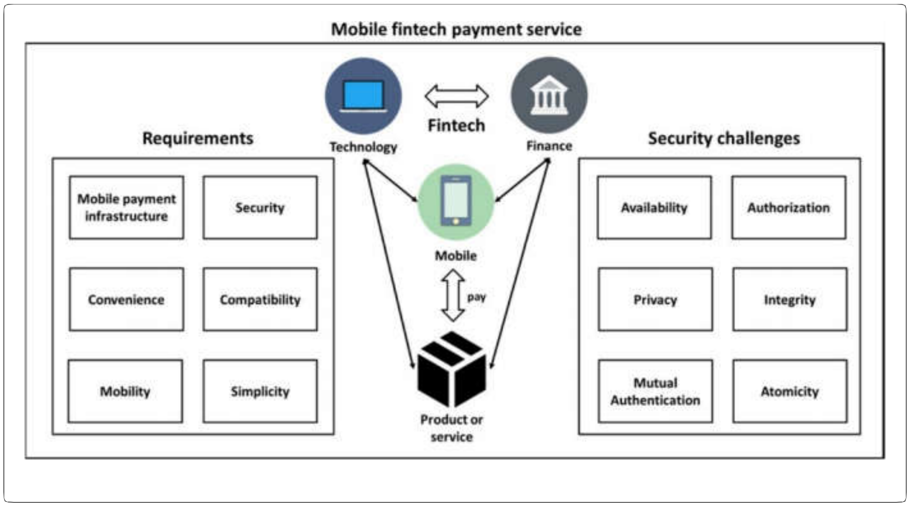
In this technology, an algorithm is used to encode information into sound waves, which can be transmitted without the net. A transaction begins once the payment device of a merchant generates a sound wave containing secured encrypted information for payment, which the mobile phone of a client receives and interprets into analog signals using the rule. The client then has to answer this signal and authenticate to complete the transaction. Sound waves produced are unique to every dealing and not affected by different background sounds. this option doesn't need additional hardware (unlike in NFC), however needs code. This makes it an accessible answer in countries where smartphones aren't affordable and people and organizations need to trust basic technologies to process payments.

Magnetic Secure Transmission

This technology uses a magnetic signal to transmit data. Magnetic signals, which ar the same as the magnetic strip on a conventional payment card, are picked up by card terminals and payments are processed. This technology works at nearly all payment terminals that have a card reader and doesn't sometimes need any additional software. it's a more secure way to transfer payment information than the other contactless communication, because it uses a system known as tokenization, wherever a card’s number is converted into a unique alphanumeric identifier using proprietary algorithms. The unique identifier is then sent to the card’s payment network, wherever it's decrypted and therefore the transaction authorized. the actual card number is stored in a secure vault with the payment processor and doesn't remain on the merchant or the mobile wallet provider systems. Samsung Pay uses magnetic secure transmission technology to enable digital payments.

Quick Response code

The Quick Response (QR) code is a new form of barcode read by digital devices, like smartphones, that are equipped with a camera. The QR code is an advanced form of the older version of the two-dimensional barcode. It contains a lot of data and is usually used to track information on products. it's also used in making payments. QR codes consist of black squares within the sort of a matrix or a grid with a white background. The QR code reader extracts information from the pattern in the QR matrix. With the aid of QR codes, banks can give multiple services as well as utility fund transfers, bill payments, mobile top-ups, and peer-to-peer or peer-to-merchants fund transfers. for each transaction, a seller presents the QR code to its client to form a payment. The QR code contains data, like bill number, bill amount, bank details of the seller, and all the other relevant information needed to complete the transaction. The customer scans the code using an installed mobile application, and the quantity is then deducted from the customer's digital case. customers will, thus, complete payments in seconds. The technology is secure, as personal data doesn't get compromised. Merchants, too can save on pay-outs made to banks and ensure that information theft doesn't originate from their outlets.



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 Figure.

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. 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. 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 utilized. For example, if certain communication protocols such as NFC must be used or if it can only be used on certain kind of services, the versatility of mobile Fintech payment service becomes very limited. Especially, current mobile Fintech payment services have incomplete infrastructure when compared to traditional payment infrastructure and sometimes it lacks availability as compared to traditional human systems.

Compatibility

Mobile Fintech payment services should be compatible with traditional payment services and financial environment like banks and card companies. Introduction of mobile Fintech payment service isn't a simple replacement however convergence with existing payment service and it should have compatibility to utilize existing payment services and infrastructure. Through this compatibility, while not the need for ever-changing existing payment service-based systems and infrastructure, each are often used and it are often wide used while not resistance from users. also, by minimizing changes in existing payment services, it should minimize the costs to implement the new environment.

Mobility

Mobile Fintech payment services should be supported by the mobility of mobile devices. because of the nature of mobile devices, they have to be continuously on the move with the user and communicate externally based on wireless networks. Existing payment service was created through a designated reader or external device at a designated place for payment. Mobile Fintech payment services mustn't need additional devices, apart from external devices that was already used for existing payment services, regard- less of wherever the mobile device is and wherever the payment is made. Thus, by increasing utilization of the infrastructure provided by the existing payment system to make sure the mobility of the payment service, the convenience of the user can be maximized.

Security

Because payment services ar directly associated with the assets of users, security could be a requirement in mobile Fintech payment service. in order that sensitive security info of the user isn't exposed to malicious attackers, mobile payment services should be created securely in terms of both HW and SW, and even if multiple payments are created with a similar payment service, info concerning the payment method should not be exposed to unauthorized third parties. also from info used throughout the utilization of mobile Fintech payment service, the user or user info should not be exposed. If secure payment service isn't provided, it cannot only cause monetary damages to users but also invade user privacy based on payment info the user used.

Simplicity

Mobile devices are becoming lighter and smaller with the development of IoT technology. This trend can result in the development of various wearable devices, and many users can wear 3–4 wearable devices within the future. this mobile payment service is optimized for smartphones, but it should even be ready to make payments on wearable devices that don't have a small screen or screen. additionally, since wearable devices are small in size, most of them are poor in computing performance, thus it's 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'll be able to still launch mobile payment services, though you do not meet all of those requirements.

but they'll not be available to users at the end of the day, as a result of the other competitors can have. especially, security factors are background areas that users cannot see or experience directly, however once a security incident happens, users will lose trust and will not be used though 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 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 should be conducted before conducting payment. The absence of mutual authentication will cause critical financial damage not solely to the user and service subject but also the payment financial organisation. If a malicious attacker assumes the identity of a mobile user, it will deliver false payment info to the service subject to avoid payment and if it assumes the identity of service subject, payment is received from the user and not provide the service. because in mobile Fintech payment service, not only face-to-face but also remote net payments is created, mobile devices should be authenticated as well as the user throughout authentication. However, if the procedures of mutual authentication become complex due to security, it can rather make mobile Fintech payment services more complicated compared to traditional payment services which may greatly reduce convenience. due to recent developments in IT technology, biometric authentication like finger- print 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 should be accessible only to the authorized subjects. also payment subjects must not be able to see info other than approved info even if it participates in the payment process. for example, users must provide passwords for payment method info to the service provider to proceed with mobile Fintech payment service but sensitive payment information should be accessed and seen only at the financial organization that actually deals with cash. If authorization on info isn't appropriately given to payment subjects, hackers will easily intercept the payment info of users without mutual authentication and moreover, they will control the information. additionally, even service subjects will claim excessive fees without the data of users and financial institutions will figure out conception patterns of users without the agreement of users.

Integrity

Mobile Fintech payment services should have integrity. If the payment information or information changed by mobile devices to make payments are changed by malicious attackers or external factors, it will have direct damage to financial assets of the users. Also, in contrast to actual cash or checks, mobile Fintech payment services exchange digital currency which suggests users cannot instantly be alerted of damages and if integrity isn't kept, users will continuously be exposed to repeated damage. Also, to point 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 info or patterns of users, on top of financial damage on users and payment subjects, it will greatly invade the privacy of users. also as a result of mobile Fintech payment goes through payment service of an IT company instead of directly through a financial institution, it's the problem that regardless of the will of the user, payment info can be delivered to any or all subjects participating within the payment which might harm the privacy of the users. info used in payment should be delivered encrypted, divided into purpose and sensitivity, and payment subjects should not be ready to figure out info excluding the mini- mum info necessary to proceed with the payment. for example, once a user pays for a service using card info through mobile Fintech payment service, the merchants must not know the card info and the card company must not know the user purchased service history. One-time card info or tokens are being wide used to protect user privacy.

Atomicity

Mobile Fintech payment service should completely conduct a payment or not at all. due to the development of IT technology, payment methods are simplified but due to the rise of subjects participating within the process of payment, it's become more complex. throughout the method of payment, if payment is halted during the pro- cess 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 won't be able to receive service even when processing payment or the service provider won't be able to receive payment even when providing service. Mobile Fin- tech payment service providers should make it so payment is {made|is formed|is created} only when the payment process is completely conducted from start to finish to prevent these sorts of damages and should notify 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 should not provide lower security compared to traditional payment services. Also, whereas maintaining a similar level of security as traditional payment services, it should have the provision wherever payment can be created simply whenever and where the user needs. However, because it doesn't directly undergo financial institutions to conduct payment, it's tough to maintain a similar level of security as traditional payment services. Also, if various security procedures are demanded on the user to have high security, it will rather have reduced convenience compared to traditional payment services. Mobile Fintech payment service should have the availability that satisfies both the security needs of subjects collaborating in payment and user convenience.

In order for a mobile payment service to be securely provided, it should have mutual authentication, authorization, integrity, privacy, atomicity, and availability as mentioned above. financial services should be a lot of rigorous than alternative services because it directly affects property if one vulnerability is found within the service. If you are doing not meet those needs, it'll cause not only a simple service error but also a catastrophic property damage to the user. while the present payment services and the mobile payment service security needs are similar in several respects, mobile payment services run on a range of devices and operative systems and lack the resources to run security pro- grams. in addition, since it is mobile, it's not fixed in one location, thus it's difficult to build a security system than existing payment system. many firms are constantly releasing mobile payment services, so as to survive the competition, it's necessary to develop services in consideration of all these aspects.

Future work

In this paper, we examine the mobile payment market within the Fintech environment. in the next study, we will investigate the settlement market of the Fintech environment during which large IT companies enter the finance industry. as the boundaries of every industry area are gradually being destroyed, the financialization of enormous IT corporations can become quicker and quicker. Future analysis can explore the money services of enormous IT companies with important potential in the mobile payment market and study security requirements.

Conclusion

Mobile payment services that were provided exclusively by financial institutions till recently developed into various mobile Fintech payment services due to rapid development of IT technology and increase in needs for convenient payment ways. unlike traditional payment services, payment services is 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's 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 mobile payment technology methods also by organizing mobile Fintech services that are currently actually used such as square, Stripe, PayPal, Adyen, Transferwise, Klarna, Boku, Apple Pay, M-PESA, Paytm, the study analyzed the recent mobile Fintech payment service trends. Lastly, the study analyzed security challenges which will arise when developing mobile Fintech payment services to be secure and convenient, to outline 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 don't have the ability to open an account, the mobile payment system depends on the prevailing financial institution or is necessarily connected, however within the future, IT companies can add or bypass their own account functions. In future research, we'll investigate and study the mobile payment process that develops in the main within the IT-oriented financial companies known as FinTech.

References

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

Dahlberg T, Guo J, Ondrus J (2015) A critical review of mobile payment research. Electron Commer Res Appl 14(5):265–284

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

Lee SH, Lee DW (2016) Review on Fintech industry in oversea

Skan J et al (2014) The boom in global Fintech investment

Park YJ, Jang SM (2014) Understanding privacy knowledge and skill in mobile communication. Comput Hum Behav 38:296–303

Liang X et al (2014) Security and privacy in mobile social networks: challenges and solutions. IEEE Wirel Commun 21(1):33–41

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-andro id-bringing-flexible-mac-android/

Li Q, Clark G (2013) Mobile security: a look ahead. IEEE Secur Priv 11(1):78–81

Kadhiwal S, Zulfiquar AUS (2007) Analysis of mobile payment security measures and different standards. Comput Fraud Secur 2007(6):12–16

Linck K, Pousttchi K, Wiedemann DG (2006) Security issues in mobile payment from the customer viewpoint, pp 1–11

Zhou T (2013) An empirical examination of continuance intention of mobile payment services. Decis Support Syst 54(2):1085–1091

Liébana-Cabanillas F, Sánchez-Fernández J, Muñoz-Leiva F (2018) Antecedents of the adoption of the new mobile payment systems: the moderating e-ect of age.

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

Zhou T (2014) Understanding the determinants of mobile payment continuance usage. Ind Manag Data Syst 114(6):936–948

Dahlberg T, Mallat N, Ondrus J, Zmijewska A (2008) Past, present and future of mobile payments research: a litera-ture review. Electron Commer Res Appl 7(2):165–181

Jeong JE, Ban YH (2014) A study on analytical comparison between payment processes by di-erent mobile pay-ment types—focus on types of mobile payment schemes used in Korea. J Digit Des 14(2):641–650

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

Wu J, Liu L, Huang L (2017) Consumer acceptance of mobile payment across time. Ind Manag Data Syst 117(8):1761–1776

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

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

To W, Lai L (2014) Mobile banking and payment in China. IT Prof 16(3):22–27

Yang Y, Liu Y, Li H, Yu B (2015) Understanding perceived risks in mobile payment acceptance. Ind Manag Data Syst 115(2):253–269

Tellez Isaac J, Sherali Z (2014) Secure mobile payment systems. IT Prof 16(3):36–43

Zhou T (2014) An empirical examination of initial trust in mobile payment. Wireless Pers Commun 77(2):1519–1531

Wong K, Kim M (2016) An enhanced user authentication solution for mobile payment systems using wearables. Secur Commun Netw 9(17):4639–4649

Hill C (2015) Wearables—the future of biometric technology? Biometric Technology Today 2015(8):5–9

https://dazeinfo.com/2018/11/07/mobile-payments-in-india-2018/

https://www.techbullion.com/top-10-fintech-payment-companies-worth/

https://www.alliedmarketresearch.com/mobile-payments-market https://www.researchgate.net/publication/260211158_Overview_of_Mobile_Payment_Technologies_and_Security

https://smallbiztrends.com/2015/05/what-is-a-qr-code.html23

https://docs.telerik.com/devtools/winforms/barcode/barcode-types/2d-barcodes/qrcode/overview

https://whatis.techtarget.com/definition/QR-code-quick-response-code

https://www.tccrocks.com/blog/what-is-a-mobile-payment/

https://www.bearingpoint.com/en/our-success/thought-leadership/who-will-be-the-winners-in-the-mobile-payments-battle/

https://www.researchgate.net/publication/260211158_Overview_of_Mobile_Payment_Technologies_and_Security

https://www.tccrocks.com/blog/what-is-a-mobile-payment/

https://www.bearingpoint.com/en/our-success/thought-leadership/who-will-be-the-winners-in-the-mobile-payments-battle/

http://nearfieldcommunication.org/about-nfc.htm