Pertanika J. Sci. & Technol. 27 (1): 1 - 31 (2019)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Review Article

A Review: Customers Online Security on Usage of Banking Technologies in Smartphones and Computers

Natarajan Sundaram[1]*, Cherian Thomas[1] and Loganathan Agilandeeswari[2]

[1]*Department of Commerce, School of Social Sciences and Languages, Vellore Institute of Technology, Vellore 632 014, Tamil Nadu, India*
[2]*Department of Digital Communication, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632 014, Tamil Nadu, India*

ABSTRACT

The internet brought a diffusion of technology in the banking arena. Two of the personal devices which aid this phenomenon are the computer (website) and smartphone (web application). Nowadays, banking is done vividly through the internet that causes both computer and smartphone prone to security risks. This review paper aims to highlight the earlier research deliberations, suggested solutions and the factors related to security issues in electronic banking devices in the past six years. Narrative literature review method was used by reviewing 130 papers from selected database journals. The paper discusses the articles between the years 2012 and 2018. It points and poses unanswered questions, which serve as the scope for further research. Neither a computer nor a smartphone has an upper hand when it comes to security. Security of banking technology does not depend on these devices. Rather the onus rests on the users, service providers and banks. The emerging electronic commerce and mobile commerce industry are not considered in this paper. This paper endeavours to provide a better scope for researchers in future to answer unrequited questions on the role of devices in banking technology security. All the past literature has focused on the peoples' attitude towards security threats in online banking. This study challenges to think further, about the influence of security threats to online banking devices.

Keywords: Internet banking, mobile banking, privacy, review, risk, security, trust

ARTICLE INFO

Article history:
Received: 14 April 2018
Accepted:12 September 2018
Published: 24 January 2019

E-mail addresses:
nsundaram@vit.ac.in (Natarajan Sundaram)
cherian28@gmail.com (Cherian Thomas)
agila.l@vit.ac.in (Loganathan Agilandeeswari)
* Corresponding author

ISSN: 0128-7680
e-ISSN: 2231-8526

INTRODUCTION

The birth of banking technology took place with the arrival of plastic cards and Automated Teller Machines (ATM) in the 1960s'. Later, in 1983, when the internet came into existence, there was a sudden disruption of technology in the banking industry. Banks that were housed in brick and mortar structures started reaching the doorsteps of customers through the internet. Two major devices that made the banking technology disruption to reach the hands of the people were smartphones (web application) and computers (website). Similarly, disruptions also evolved these devices, which eventually led to cost effective and efficient technology to progress faster. In spite of technology disruptions that were being heralded as a positive sign for all such benefits that it had brought, it also had its own set of challenges and issues in the form of security. Figures 1 and 2 are given below to show how the internet (computer) and mobile banking (smartphone) architecture differs from each other and also about the probable online banking cyber attacks.

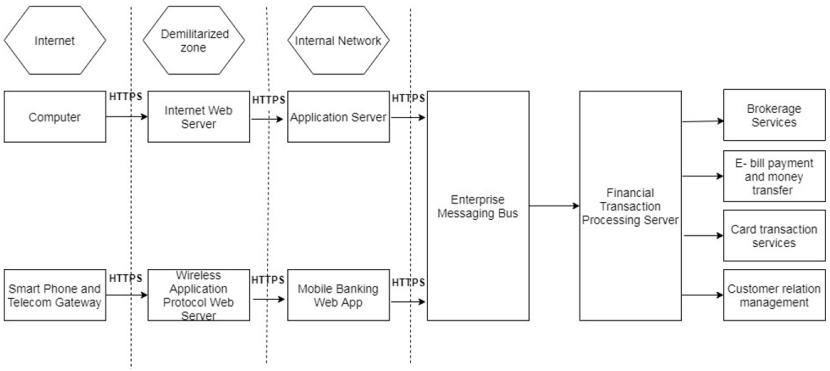

Figure 1. Architectural outlay of internet and mobile banking (Zhang & Morana, 2012)

According to the Cybersecurity Ventures Annual Cybercrime Report, 2017, the depths of security attacks were explicitly stated. The report predicted a loss of about $6 trillion of the online banking customers by 2021 exclusively due to cyber crimes. One in six customers was said to be prone to cyber attacks, according to a research by MarkMonitor in 2014. DDoS (distributed denial-of-service) attacks, ransomware, and an increase in zero-day exploits are counted as the major factors that lay behind cyber crimes, while phishing still ruled as the major weapon of new entrant cyber attackers. The banking technology has been exposed to a large security risk due to increase in internet users world-wide, emergence of the Internet of Things (IoT) and big data, increase in wearable and wireless devices, newly written software codes, flourishing digital contents and booming sensor technology. Although biometrics have replaced the password, transition to this new technology have set to touch $1 trillion. The occurrences in the frequency of ransomware attacks are set to reduce from 40 seconds per business firm in 2016 to 14 seconds per business firm in 2019.

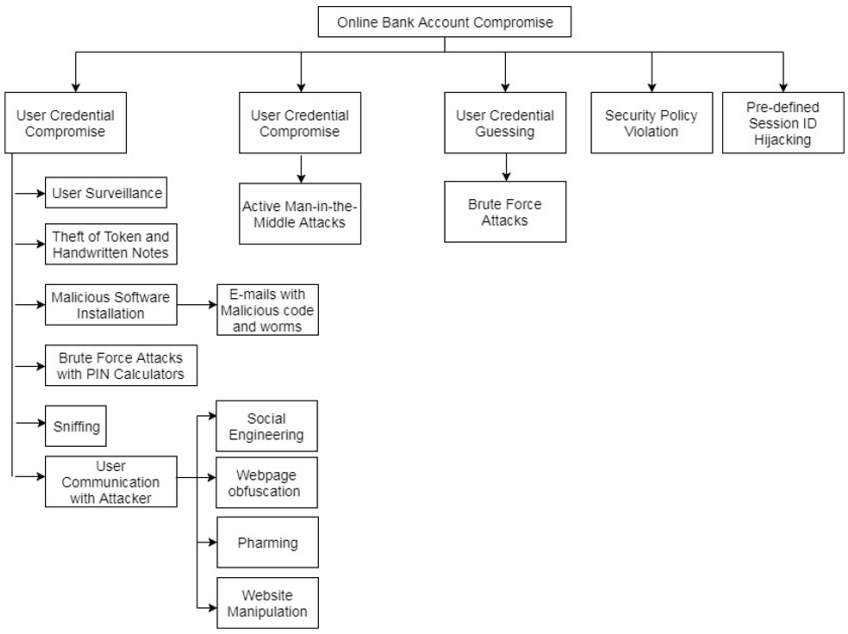

Figure 2. A bird's eye view of probable cyber attacks in the internet and mobile banking (Zhang & Morana, 2012)

By 2021, a dearth of about 3.5 million employees in cybersecurity profession is estimated. Firms are expected to spend around $10 billion to train their employees on cybersecurity awareness. In particular, banks which are the store-house of money are extensively prone to cyber threats. Bloomberg Businessweek posits that banks globally were set to lose $700 billion annually due to cyber threats. These factors have made the studies towards banking technology security to be highly relevant at present and in days to come. At present, the security vulnerability scales are slightly tilted towards mobile based applications than a website. According to Verizon's Data Breach Investigation Report, 2016, it was found that web applications were easy to break into using SQL (Structured Query Language) injection or malware which can go undetected. This is due to the existence of millions of legitimate users and proxy servers. However, this review paper has taken both the website (computer) and the web application (smartphones) aspects into account.

As presumed, not all the cyber crimes are motivated by monetary gains. Cyber crimes have evolved to include those crimes that are done in order to quench revenge either by an individual or a group that upholds an ideology. On the contrary, Verizon's Data Breach Investigation Report, 2016 pointed that 89% of cyber threats in 2015 were due to monetary gains and data leakage than other causes. Another dangerous trend observed is that attackers

have evolved from humans to computer bots which are trained to break security. The Financial Industry Cybersecurity Report of Security Scorecard, 2016 stated that financial industry faces the highest vulnerability compared to other industries in terms of network security and other subsequent factors.

The aim of this review paper is to transcribe the security issues of banking technology in the literary works of past six years, into one single literary piece to make a note as to where the current research stands. The discussions carried in this paper regarding banking technology security are viewed both from the customers and industry point of view. In the following sections, the paper is organized as a research methodology that discusses the approach on which the paper is built upon, followed by the review of past relevant literature. The paper finally concludes and outlines the scope and offers few areas that promote further research.

RESEARCH METHODOLOGY

The review paper was conceptualized to provide a comprehensive view of the present security landscape of banking technology. An extensive search was conducted in eight databases of publishers viz. Elsevier, Emerald, IEEE (Institute of Electrical and Electronics Engineers), Inderscience, Sage, Springer, Taylor and Francis, and Wiley. The keyword used for the search was 'security issues on the internet or mobile banking'. A total of 130 articles were reviewed between the time period of 2012 and 2018. The year 2012 was crucial for this study since internet banking fraud cases shot from mere 94 in 2011 to 1,003 in 2012, which is an increase of 967%. The losses due to this were pegged at 3 million Euros (Febelfin, 2013).

REVIEW OF LITERATURE

The core part of the paper is presented in this section. For the reviewing convenience, the process was started by analyzing the online banking[1]. It was split into two: internet banking[2] and mobile banking[3]. These were done in order to study the macro and micro security concerns. Under each form of banking, the review was branched out to deliberations, solutions and impacts that occurred in the past six years.

Online Banking Security- Deliberations, Solutions and Impact

Deliberations. Trust, security and privacy were not only technical issues but they were attitudinal problems as well. This is because banking technologies were termed as

[1] Online Banking is a generic term. It is used to denote any bank transaction done with the help of internet. It is regardless of any device or platform that is used.
[2] Internet Banking is a term used to denote any banking transaction that is done through a website
[3]Mobile Banking is a term that is used to carry out banking transactions trough a web application. The facilities offered will differ with internet banking.

'customer-centric' thus, it must include human element as well (Akram et al., 2018; Ayo et al., 2016). Attitudes like optimism, pioneering, low level of discomfort and risk perception were needed to use any technology (Boon-itt, 2015). A difference of opinion existed amongst people of different age group on trust. Millennials trusted a virtual environment like online banking whereas the older adults trust a physical bank than a virtual one (Alhabash et al., 2015). Structural assurances were the antidote to make older adults trust online banking. It was needed at the pre-adoption stage of online banking (Montazemi & Qahri-Saremi, 2015). On the gender front, a study in Portugal established that women used e-banking more than men since their risk perception was less. The female population consisted of students, unemployed and retirees. Majority of the respondents were not post graduates and had a meagre income of around 1,250 Euros (Fonseca, 2014). Further, it was found that customers did not opt for internet banking due to the lack of trust on banks' operations, whereas mobile banking was avoided due to the inherent security risk perception (Mishra & Singh, 2015). This shows that the nature of banking technology security is not only technological and attitudinal, but it is organizational as well. With regard to privacy, people felt secure while using their own device for bank transaction than a public kiosk. The absence of customer support while using a public kiosk resulted in increasing privacy anxiety (Blut et al., 2016).

Bank customers in Poland who used online banking had the trust that their banks were able to protect them from cyber intrusions (Szopiński, 2016). Finnish bank customers were less concerned about risk in the internet or mobile banking due to trust (Laukkanen, 2016). Non-users had low levels of trust in online banking. Such non-users needed actions and evidence from banks regarding privacy protection, security level and implemented fraud mechanisms, in order to become users (Riffai et al., 2012). Non-users were also found to be lesser users of the internet for any general purpose. There was a positive relationship between hours spent on the banking device and the familiarity with security issues. Hence, awareness programs had to be crafted based on the level of device usage (Jeske & Schaik, 2017). Whether it was users or non- users, it was crucial to have successful online banking transactions each time a customer had logged in. As the number of successful transactions increased, there was a decrease in security concerns. Further, in case of unsuccessful online banking transactions, a transparent and sincere dealing was expected from the part of banks, in order to build customer confidence (Ong et al., 2017).

Bank's negligence towards security issues would negatively affect customers' trust (Mason and Bohm, 2018). Both the banking sector and the police department were treating cyber frauds as mere cases though the scale of such events were alarmingly rising (Koong et al., 2017). Banks were responsible for the cyber threats that were happening and thus the study placed the thrust on an internal reconstruction and clear service standards (Andaleeb et al., 2016). Customer's trust was based on the positive relationship between

their prior experiences and awareness about fraud prevention measures of banks. It was important to notice especially when a cyber fraud occurred due to a third party breach. Age was a moderating variable in that relationship, whereas income had no role (Hoffmann & Birnbrich, 2012). Banks needed cautious customers who could reduce cyber frauds and increase security (Jansen & Schaik, 2017). Students in an educational institution had general and not contextual awareness on identity theft. A general notion that hackers targeted only the rich was a myth that surrounded them. Lack of time or negligence were the causes of students being unprepared to face identity theft threats (Seda, 2014). Banks were giving general awareness to its customers regarding cybersecurity measures, but there was a need to provide context-specific awareness (Ivaturi & Janczewskib, 2013). A reality check on bank customers' awareness about phishing was conducted. The post-test result revealed that there was an improvement in identification of phishing threats. The awful part was that respondents were not willing to incur software cost to avoid phishing threats (Arachchilage et al., 2016). In addition, age, income, education, hours spent on the internet and the technical background were found in not aiding users' ability to identify phishing websites. It was solely the user awareness programmes that alleviated security issues (Purkait et al., 2014). On the part of bank employees, they had uniform awareness on potential risk involved in online banking transactions. This demonstrated that the bank employees were well equipped to support customers in case of any cyber fraud (Murari and Tater, 2014). In another study in Australia, a comparison between bank employees and selected field employees showed that bank employees were 20 percent more aware of information security than other category of employees (Pattinson et al., 2017).

On the legal end, cyber fraud victims were denied justice by courts due to the complexity involved in collecting online banking transaction evidences from banks. The courts must act diligent while dealing with bank fraud victims and should not rely on banking evidence alone (Mason, 2013). Internet of Things was visionary and helpful aspects for humankind, but it had neglected privacy, individual choice, equality and trust. Such negligence was set to cause drastic impediments if not nipped in the bud. Though regulatory measures were in place to build online banking customers trust, there was a total silence where the Internet of Things (IoT) and online banking merged (Dutton, 2014).

In a world ridden with social media craze, it is necessary to make sure that users do not leak their personal identity on the net. The present system followed by all the banks is to create awareness, but the article of Büchi et al. (2017) pointed at the fallacy such awareness programs had, in the light of ever-changing technology. Even legal rights bestowed upon citizens were deemed useless in such a scenario. Therefore, the paper called for constant skill upgrade of users, data breach notifications, erasure, portability and sealing of private information appended with a certification. Such a holistic approach was viewed to bring more security and relevance for customer rights.

Solutions. The banking industry does accept the fact that single-factor authentication was a failure. In order to overcome this limitation, it was opined to have username and password validation, biometric authentication and embedding device with cryptography code. This opinion put a question on the ubiquity of online banking services (Blauw & Solms, 2014). An effective authentication would mean that the word 'liveness' is redefined. It requires systems to secure authentication details encrypted in a server. The systems must be able to use Artificial Intelligence to check whether the user is real, alive and are under control of the transaction (Wojewidka, 2017). The usage of decision support system was recommended, named Banksealer, to alert banks cybersecurity analysts regarding sporadic spending that were found in a customers bank account, thereby proactively preventing security flaws at the entry level itself. The software prepared real-time spending profile of each customer's bank account in order to keep a tab on any cyber flaws (Carminati et al., 2015).

An enhanced online security performance depended on the maximum disclosures of firms and the existing government regulations (Li, 2015). The top management needed to proactively treat security breaches. Rather, they were merely funding security resources only based on imposed government regulatory norms (Chaturvedi et al., 2014). A compulsory, stringent and transparent policy was needed in order to check cyber crimes. For example, the United States Securities and Exchange Commission (SEC) demands firms to file cyber crime-related issues that occurred each year in the annual report of the company (Clark & Harrell, 2013). Various vulnerability points are spotted in e-banking transaction, hence the data must be made secure. Or else, it will lead to legal, financial and reputational risks for banks. Basias et al. (2013) opined about the introduction of SOA (Service Oriented Architecture) in online banking to counter security threats. Such a framework, maintained by a third party was set to increase security manifold and leave the security threats to the hands of the experts.

Green banking activists were challenged since ATM (Automated Teller Machine) bank transaction bills did have an impact on customer relationship and it was a natural structural assurance agent. Discontinuation of paper bills was seen to bring back customers distrust on banks online banking environment (McNeish, 2015). Such an assurance is impossible in the internet or mobile banking arena. Banks are entering into cloud computing nowadays. Although it is a public storage arena, certain security measures like multi-factor biometric technology and protection gateway are needed. Once the security is in place, banks could speed up transactions, add new features and will be able to get more cloud storage space. This would bring in ease of use and security to customers (Nagaraju & Parthiban, 2015). A survey was conducted among potential online banking users to study their preference over retina scanning, fingerprint scanning and facial recognition technologies. They preferred and trusted fingerprint scanning due to the familiarity they had (Tassabehji & Kamala,

2012). It shows that bringing revolutionary security methods was not enough and instead they have to create familiarity in order to be widely used.

Impacts. Online banking trust has an influence on customers satisfaction and utility perception (Lie´bana-Cabanillas et al., 2013). But, there is an increase in ease of use diminished security (Maditinos et al., 2013). Therefore, ease of use has a negative influence on customer satisfaction. (Sikdar et al., 2015). Ease of use is a part of the solution to enhance Information and Communication Technologies. But there is a price to pay for this solution in the form of loss of security.

Banks need to start seeing banking technology from a customers' attitude perspective. (Akram et al., 2018; Ayo et al., 2016). Customers must have positive attitude towards online banking (Boon-itt, 2015). Following is the brief summary of themes on the above literature, given in Table 1.

Table 1

Brief summary about online banking reviews

Deliberations
Trust
i. Millennials trust a virtual bank more than a physical bank (Alhabash et al., 2015). In order to bring more customers, structural assurance must be given at the pre- adoption stage (Montazemi & Qahri-Saremi, 2015). Non-users need actions and evidence from banks regarding privacy protection, security level and implemented fraud mechanisms, in order to become users (Riffai et al., 2012).
ii. Customers trust banks to protect them from cyber attacks (Szopiński, 2016). Finnish bank customers are an example for this (Laukkanen, 2016). But, Bank's negligence towards security issues would negatively affect customers trust (Mason & Bohm, 2018). Therefore, customers do not opt for internet banking due to the lack of trust on banks operations (Mishra & Singh, 2015).
iii. The more the number of successful transactions, the lesser will be the security concerns of bank customers (Ong et al., 2017).
Risk perception
i. Women used e-banking more than men since their risk perception was less. (Fonseca, 2014).
ii. People felt secure while using their own device for bank transaction than a public kiosk (Blut et al., 2016)

Table 1 *(Continue)*

Security
i. There is a positive relationship between hours spent on the banking device and the familiarity with security issues (Jeske & Schaik, 2017). Customers trust are based on the positive relationship between customers prior experiences and awareness about banks fraud prevention measures (Hoffmann & Birnbrich, 2012)
ii. Both the banking sector and the police department are treating cyber frauds as mere cases (Koong et al., 2017). Banks were responsible for the cyber threats (Andaleeb et al., 2016).
iii. Lack of time or negligence are the causes of students being unprepared to face identity theft threats (Seda, 2014). But, banks need cautious customers who could reduce cyber frauds and increase security (Jansen & Schaik, 2017)
Awareness
i. Banks must stop giving general awareness and start giving context-specific awareness to its customers (Ivaturi & Janczewskib, 2013).
ii. Bank employees are uniformly aware about cyber security among themselves (Murari & Tater, 2014). Bank employees are 20% more aware about online banking safety than the other employees (Pattinson et al., 2017).
Regulations
i. Courts must act with diligence and should not only rely on banks evidence (Mason, 2013).
ii. Internet of Things lacks regulations and therefore it is risky (Dutton, 2014).
iii. Legal rights are useless unless proper measures are in place (Büchi et al., 2016).
Solutions
Security
i. Single-factor authentication is a failure (Blauw & Solms, 2014). Artificial Intelligence must be used for authenticating the transaction (Wojewidka, 2017).
ii. Spending pattern of each customer helps banks keep track of its' customers' money (Carminati et al., 2015).
iii. SOA (Service Oriented Architecture) maintained by a third party will increase security and bring expertise (Basias et al., 2013).
iv. People opt for security technology based on previous experience (Tassabehji & Kamala, 2012).
Regulations
i. Companies that follow maximum disclosures of government regulations are found to be more concerned about security issues (Li, 2015). Such a disclosure must be made not out of regulatory compulsion (Chaturvedi et al., 2014). Regulatory bodies need to promote maximum disclosure norms (Clark & Harrell, 2013).

Table 1 *(Continue)*

Innovation
i. Paper bills are needed as evidence for banking transactions (McNeish, 2015). Secured cloud computing is an answer to ensure that bank transaction evidences are not tampered (Nagaraju & Parthiban, 2015).
Impacts
Trust
i. Online banking trust has an influence on customers satisfaction and utility perception (Lie´bana-Cabanillas et al., 2013). But, ease of use has a negative influence on customer satisfaction (Sikdar et al., 2015).

Following are the potentially open problems that were discussed in the previous studies:

i. Americans had issues on trust than Malaysians, due to the absence of collective culture (Yuen et al., 2015).
ii. It is a challenge for banks to create security in developing countries (Susanto et al., 2013).

Internet Banking Security- Deliberations, Solutions and Impact

Deliberations. A look at the traditional banking would show that face-to-face bank transactions used to occur and customers could reach out to a bank employee. In the present online banking context, there was a vacuum in terms of such an interaction. Customers were seeking guarantee in this aspect, if anything goes wrong in the online world (Harrison et al., 2014). Humans were wired to act this way (Upadhyay & Jahanyan, 2016). Bank customers were divided into innovation lovers and laggards. Hence, banks had to offer different benefits to each group. Innovation lovers wanted technology usefulness, whereas laggards wanted technology simplicity (Yousafzai & Yani-de-Soriano, 2012). With changing technology, even bank regulations had changed. This kept bank customers in the dark in the internet banking space. Bashir and Madhavaiah (2014) called for transparency from banks to update customers with recent regulations. Additionally, bank customers that engaged in internet banking were bound for losses in terms of security, money and time (in case of becoming a victim of cyber fraud). These losses were bound to affect intention to use internet banking. In order to prevent it, banks could introduce money back guarantee policies or insure each bank transaction (Martins et al., 2014).

Solutions. Proactive measures from banks were needed in order to build trust. These measures were giving free security software and agreement to indemnify customers from any cyber threats (at banks' convenience and discretion). Awareness programs must be conducted by banks Information Technology officers (Chandio et al., 2013). These awareness programs must be interactive and extensive in nature (Bauer et al., 2017).

Non-users of internet banking were supposed to undergo a trial session of using internet banking. Bank employees would aid such sessions for inviting possible risk concerns and to give a firsthand experience to bank customers on how things work. It was advisable for bank employees to be available over the telephone in order to provide assurance and take proactive security measures during the time of emergency (Patsiotis et al., 2012)

Banks needed to engage in conversation with customers about security factors in internet banking. Such measures would build trust. They could provide firewalls, sophisticated encryption tools and intrusion detection systems, in order to prove that the bank is trustworthy with the money of their customers (Juwaheer et al., 2012; Tarhini et al., 2016). Preparation of risk profiling to authenticate user's web browser during each login would help banks to keep each customers bank accounts in check. Such an exercise would also improve the risk perception of customers (Butler & Butler, 2015).

Impacts. Risk existed in internet banking (Shanmugam et al., 2015). It was due to ample exposure of networks to the outside virtual world (Kesharwani & Tripathy, 2012). There was laxness on the part of banks on validating each transaction. It was suggested to add codes to each transaction in order to resolve any issues pertaining to any failed transaction (Mohammadi, 2015). There were two types of risks at play viz., internal and external risks. Internal risks were lower technical knowledge and lesser ease of use. External risks were failed transactions and internet frauds. When internal risks led to a deficiency in the usage of internet banking, external risks heightened perceived risk attitude of bank customers. Each of these risks needed to be treated separately by banks (Roy et al., 2017). Trust influenced perceived risk more than perceived ease of use. Banks were advised to keep bank customers informed about the movement of their money in the bank account, irrespective of whether it was a charge levied or payments/ receivables made (Bashir & Madhavaiah, 2015). Similarly, unless perceived risk was not taken care of, it was going to hinder convenience (Clemente-Ricolfe, 2017). Perceived risk must be replaced with perceived security in order to raise trust in internet banking (Damghanian et al., 2016). Risk and security were two things that banks were grappling with the terms of internet banking adoption. Young bank customers trusted internet banking more than the older ones due to sound technical background and risk awareness (Giovanis et al., 2012). For certain categories of people like the postponers, opponents and rejectors, for whom the risk perception was negative, had ended up causing rebellion in the form of negative word of mouth. This led to adverse social influence in the society (Mzoughi & M'Sallem, 2013).

Customers wanted web privacy. Web privacy had influence over adopting internet banking, which was moderated by the attitude to use. Only when a bank customer was able to do a transaction with ease and had an assurance on web privacy, he or she will venture to use internet banking (Rawashdeh, 2015). Not only web privacy, but the security and error-free records were also detrimental in producing customer satisfaction (Raza et al.,

2015). There was a need for increased perceived security in bank customers so that initial trust could be built. This further led to the adoption of internet banking. The challenge for banks was in creating sufficient security in developing countries. Such a challenge could be met only by government support in the form of law and funding. It was also found that government support can directly produce initial trust, but cannot compel internet banking usage (Susanto et al., 2013).

Electronic service quality has enhanced both electronic satisfaction and electronic loyalty. Electronic trust was found to be playing a moderating role in this process (Butt & Aftab, 2013, p.6). The effect of service quality on trust was much higher than the effect that trust could have on customer satisfaction (Kundu & Datta, 2015). The electronic trust had the potential to influence perceived usefulness and behavioural intention of bank customers (Mansour, 2016). Cognitive evaluation theory was borrowed to explain the role of motivation in the adoption of internet banking in developing countries. The citizens of such countries were found to undertake internet banking transactions only if they had intrinsic motivation. However, the working of intrinsic motivation was found to be moderated by trust (Akhlaq & Ahmed, 2013).

Issues of trust existed for both users and potential users. There was a cultural nuance with regard to trust issues that divided people. In a study which was conducted on trust issues taking into account the power distance and individualism, Americans had trust issues than Malaysians (Yuen et al., 2015). Trust could enhance performance expectancy and effort expectancy. This was because bank customers felt that using internet banking was something worthwhile investing in. The paper discussed as to how trust was born. Trust in a physical bank was the first step towards using the technology that this same bank provided (Chaouali et al., 2016). It was hard to create initial trust, especially for internet-only banks. Such banks needed to have service level agreements with their customers and needed to prove that each policy was simplified and matched with the banking industry standards (Kaabachi et al., 2017). Trust had a significant influence on the adoption of internet banking (Sharma et al., 2015). The elements of trust were benevolence, competence and integrity from the bankers side, which motivated bank customers to use internet banking (Yiga & Cha, 2014). Once bank customers switched to continued usage, benevolence could be replaced with shared values, since benevolence became subjective for the continued user (Yu et al., 2015).

Following is the brief summary on the above points, given in Table 2.

Table 2

Brief summary about internet banking reviews

Deliberations
Trust
i. Internet banking has altered a personal interaction. This creates trust vaccum (Harrison et al., 2014).
ii. Money back guarantee policies or insuring each bank transaction helps to preserve the trust of customers on banks (Martins et al., 2014).
Security
i. Bank customers are of two types, innovation lovers want technology usefulness and laggards want technology simplicity. Hence, security technology must promote both want technology usefulness and technology simplicity (Yousafzai & Yani-de-Soriano, 2012).
Regulations
i. Banks must update customers with latest regulatory changes (Bashir & Madhavaiah, 2014).
Solutions
Trust
i. In order to build trust, banks can provide security software for less cost and indemnity agreement (Chandio et al., 2013; Juwaheer et al., 2012; Tarhini et al., 2016). In addition, interactive and extensive awareness programs must be conducted (Bauer et al., 2017).
ii. Bank employees need to aid non-users at each juncture during the initial stages of internet banking usage (Patsiotis et al., 2012).
Risk perception
i. Preparation of risk profiling to authenticate user's web browser during each login would help improve the risk perception of customers (Butler and Butler, 2015).
Impacts
Security
i. Security was compromised since networks were exposed to the outside virtual world (Kesharwani & Tripathy, 2012). Hence, each transaction must be coded and validated in order to aid faster problem resolution (Mohammadi, 2015).
ii. Internal security risks create aversion for internet banking and external risks create negative risk perception for bank customers. Each of these risks needed to be treated separately by banks (Roy et al., 2017).
iii. Error free transactions led to customer satisfaction (Raza et al., 2015). Electronic service quality enhanced both electronic satisfaction and electronic loyalty (Butt & Aftab, 2013). The effect of service quality on trust was much higher than the effect that trust could have on customer satisfaction (Kundu & Datta, 2015).

Table 2 *(Continue)*

Trust
i. Bank customers will use internet banking if trust and ease of use exists (Rawashdeh, 2015).
ii. Trust influenced perceived risk more than perceived ease of use (Bashir & Madhavaiah, 2015).
iii. Trust can increase performance expectancy and effort expectancy (Chaouali et al., 2016).
iv. Trust can influence perceived usefulness and behavioural intention of bank customers (Mansour, 2016).
v. Intrinsic motivation to use internet banking is triggered by trust (Akhlaq & Ahmed, 2013).
vi. Young bank customers trusted internet banking more than the older (Giovanis et al., 2012).
vii. Initial trust must be formed through service level agreements between the bank and the customers ((Kaabachi et al., 2017). It can be also formed through benevolence, competence and integrity from the bank (Yiga & Cha, 2014). Once bank customers switched to continued usage, benevolence could be replaced with shared values (Yu et al., 2015).
Risk
i. Lack of attention to perceived risk would aggravate inconvenience (Clemente-Ricolfe, 2017). Perceived risk must be replaced with perceived security in order to raise trust in internet banking (Damghanian et al., 2016).
Risk perception
i. For certain categories of people like the postponers, opponents and rejectors, for whom the risk perception was negative, had ended up causing rebellion in the form of negative word of mouth. This led to adverse social influence in the society (Mzoughi & M'Sallem, 2013).

Following are the potentially open problems that were discussed in the previous studies:

Americans had issues on trust than Malaysians, due to the absence of collective culture (Yuen et al., 2015).

It is a challenge for banks to create security in developing countries (Susanto et al., 2013).

Mobile Banking Security -Deliberations, Solutions and Impact

Deliberations. There was no communication from the bank towards its customers on legal procedures in case of cyber frauds. In such cases, it was better if the banks could help the customers on legally carrying out the claim procedure (Purwanegara et al., 2014). The law was also not clear in punishing the guilty. In most of the cases, it was the bank which got accused. Ashta (2017) suggested for a case-by-case analysis. In cases where customers were negligent, they could be held guilty, whereas in cases where it was found that the network was insecure, the bank, service provider and the mobile operator could be held liable. Failure in the creation of awareness about safety measures was legally pointed as the guilt of banks. Mobile money economy needed laws that are both risk sensitive as well as transaction sensitive (Wonglimpiyarat, 2014).

Mobile banking users were of the opinion that it was not the banking institution that they feared, but rather it was the technology (Makanyeza, 2017). It was a norm that banks used marketing media to allay the fears caused by various risks involved in mobile banking. The banks were urged to boost up the value addition that a user would get instead of stressing on the risks that were inherent in a mobile banking environment (Glavee-Geo et al., 2017). Employing different marketing strategy as per the risk profile of users was an option that could be looked into. For frequent users, marketing of mobile banking could cancel psychological risk whereas, for infrequent users, marketing of mobile banking could cancel both financial and psychological risk (Chen, 2013). A brand name which offered trust was considered to be vital while offering mobile banking services (Tobbin, 2012). Mobile banking could not follow penetration pricing strategy which the mobile operators followed rather it had to follow skimming strategy, in order to meet security cost. To sum up, offering low-cost service and putting customers at risk with low-security level was not advisable for banks (Tran & Corner, 2016). Mobile phones were three times susceptible to phishing attacks than a desktop computer. The difference in the functioning of the system is the reason for such vulnerability (Goel & Jain, 2017). Scan and pay model lessened mobile payment process time, but such a benefit had been overshadowed by concerns about its security. It was observed that innovation had clearly let down users in this regard, without the backing of a robust security system (Taylor, 2016).

Solutions. A slew of solutions to increase mobile banking security were suggested based on the utility as follows. The smartphones ever-growing storage space was an indirect potential threat for stealing critical data that was stored in these phones (Das & Khan, 2016). Fingerprint biometric technology could be used in smartphones, using which online transactions could be undertaken. The fingerprint so collected by the banks would be encrypted for authentication. This could prevent security breach and misuse (Belkhede et al., 2012). Selfie was a new trend among millennials. In this context, asking facial recognition for bank transaction authentication is a near future possibility (Cook, 2017). Payments must be tokenized through identification numbers. This was in order to increase users privacy. None of the users information were revealed as it was eclipsed by the token which was issued. Organizations needed to register with the Token Service Providers (TSPs) to authenticate each token received (Yu et al., 2017). A model was developed by Bojjagani and Sastry (2017) for both smart and feature phones. It avoided storage of any critical bank transaction data. A 160 bytes sized encrypted message encoder known as P-224 could send the authentication details securely.

Non-repudiation of transactions must be focused rather than focusing on authentication and integrity of data that was transferred. Encryption of data was still alien in mobile payments and therefore a model known as Mobile Payment Consortia System (MPCS) using Public Key Interface (PKI) was suggested (Britto et al., 2012).

Impacts. Trust was a significant factor which reflected the mobile banking application's security character, the integrity of the information technology team and the awareness programs that banks organize (Chandio et al., 2013). Trust influenced customer loyalty towards mobile phone operators as well. It is because users conducted sensitive transactions like mobile banking over the mobile phone operator's network (de Reuver et al., 2015). Trust decided the pathway of each individual's attitude towards mobile banking (Kumar et al., 2017). Non-users lacked initial trust because third parties existed apart from banks (Xin et al., 2015). They needed structural assurances as well as familiarity (Zhou, 2012). Web applications were a means for banks to know customers more closely and also to negate trust deficiency (Berraies et al., 2017). The mere usage of web application technology was not going to help; rather there was a cycle that bank customers needed to go through when it comes in gaining initial trust. The cycle started with the influence of task-technology fit on performance expectancy, and then influence initial trust, which was an antecedent in adopting mobile banking (Oliveira et al., 2014). New users needed privacy controls and regulatory aspects in place before adopting mobile banking (Duane et al., 2014). The mediating effect of trust grew stronger when self-learning happened in customers, which influenced customers intention to use mobile banking (Shaw, 2014). Trust was a product of good service quality and was moderated by security. It had a positive significance over customer satisfaction. However, mobile banking interface had no role to play in building trust (Arcand et al., 2017). But, system quality did influence trust (Chemingui & Lallouna, 2013). With regard to the unbanked, responsible agents must be employed who can transfer money through mobile banking and thereby increase trust (Tobbin, 2012). It was trust and self-efficacy of the user that led to adopting mobile banking (Shankar & Datta, 2018).

Perceived risk and trust were used by Alalwan et al. (2016) as independent variables. A negative risk perception was a deterrent towards the adoption of mobile banking. This was attributed to the nature of mobile banking which was heterogeneous, uncertain and intangible. There was growing negative risk perception about information content and the nature of mobile banking (Sreejesh et al., 2016). All the customers would not have the same level of risk perception and it might get changed depending on the skills that each customer had (Ozturk et al., 2017). Perceived risk and perceived control had a significant influence on the adoption of mobile banking for users in urban cities. But, it was only perceived control which was predominant for users in metropolitan cities (Gupta et al., 2017). Perceived risk was divided into performance risk and privacy risk. Both such risks have negatively affected the usage of mobile payments (Khalilzadeh et al., 2017). Even in such rising risk environment, any user with a positive attitude was bound to adopt mobile banking (Garrett et al., 2014). Such a positive attitude was because of low perceived risk (Mohammadi, 2015). With regard to how non-users perceived risk, they even feared a

simple security feature like a PIN (Personal Identification Number), due to fear of theft (Sohail & Al-Jabrib, 2014).

A breach in privacy and confidentiality were found to discourage mobile banking adoption (Vaithilingam et al., 2013). If customers had a prior online shopping experience, privacy concerns about mobile payments were set to come down (Su et al., 2018). During a survey conducted among the young respondents, it was found that they were not affected monetarily or security wise. It was the fear of social rejection and the system performance failure that caused inhibition in adopting mobile banking (Yadav et al., 2015). In another study, among generation Y, it was found that security had a negative relationship with hedonic motivation to use mobile banking (Boonsiritomachai & Pitchayadejanant, 2017). Full-time employees were more worried about the risk factors when compared to students, who were only bothered about performance efficiency (Bhatiasevi, 2016). Although trust was focused on being the sole ingredient for adopting mobile banking, another study pointed at the need to add both trust and perceived risk (Slade et al., 2015). On the continuation of usage of mobile payment, aversion to risk still existed in the minds of the consumers (Cao et al., 2018). But such a risk apprehension was not about the mobile payment provider but rather it was about technology security (Thakur, 2014). Though smartphones were able to provide hedonic benefits and utility, when it came to payments, privacy and psychological risks would fail mobile payments adoption (Cocosila & Trabelsi, 2016). Smartphone users did not follow efficient smartphone security practices as per a survey conducted among students (Jones & Chin, 2015). The challenge of facing hackers lied in the fact that it was difficult to identify legitimate users. In developing world, where mobile phone Subscriber Identification Module (SIM) were shared or having ownership to more than one individual, there were all possible chances of losing money and privacy, within the customers known circle (Kizzaa, 2013). This made customer redressal for banks harder. However, on the brighter side, technology advancement was a positive sign that risks could come down and adoption rate of mobile banking would considerably pickup thereafter (Mullan et al., 2017). Social influence did reduce perceived risk in potential users of mobile banking. Such a finding was found in collective cultures that existed in China and India (Yang et al., 2012).

A survey in the United Kingdom (UK) revealed that customers were pitted against risk and trust in mobile payments (Slade et al., 2015). Mobile payments offered by banks were considered to be trustworthy than retail mobile payment providers or mobile operators (Tran & Corner, 2016). Banks were trusted since their work code stressed on the obligation to maintain secrecy about the bank customers account details. Such a trust was going to compensate the risks that customers faced. On another front, customers did acknowledge the benefits of small payments made in tolls or for using public transport. Such benefits were going to counterbalance the risks that customers face (Hampshire, 2017). Customers could savour such benefits only when they became a user and experienced such benefits

firsthand. Therefore, risks were prevalent and were hard to stop, but banks could focus on giving risk assurance, benefits and trust (Shaikh and Karjaluoto, 2015). With regard to experiencing benefits, customers must be able to feel that promised benefits were delivered. If there was a bad experience, it needed to be rectified by undertaking feedback from the customer (Nel & Boshoff, 2017). Risk had more prominence in the continued usage stage whereas trust carried prominence in the pre-adoption stage (Zhou, 2013). Although the study found that trust completely did not go out of a continued usage stage, it had an indirect effect on intention to continue to use mobile payments. In the continued usage space, the importance of confirmation was stressed. Confirmation from the bank about each transaction boosted trust, customer satisfaction and perceived usefulness. It allayed privacy concerns (Susanto et al., 2016). Moreover, confirmation received from government agencies would be comparatively more convincing and satisfying for mobile banking users (Upadhyay & Chattopadhyay, 2015). Publicizing the mobile banking security measures undertaken by the bank in their website could lead to wider transparency and increased trust (Malaquias & Hwang, 2016).

Following is the brief summary on the above points, given in Table 3.

Table 3

Brief summary about mobile banking reviews

Deliberations
Regulations
i. Banks need to help customers in claiming losses in case of cyber frauds (Purwanegara et al., 2014).
ii. Courts must not deal with bank transactions based on the precedents; rather it must be on a case-by-case basis (Ashta, 2017). Hence, Mobile banking needed laws that are both risk sensitive as well as transaction sensitive (Wonglimpiyarat, 2014).
Risk perception
i. Mobile banking users feared technology (Makanyeza, 2017).
ii. Mobile banking advertisement must focus on benefits rather than risks (Glavee-Geo et al., 2017). Marketing strategy must be different between frequent and infrequent users (Chen, 2013). A brand name which offers trust was considered to be vital while offering mobile banking services (Tobbin, 2012).
Security
i. In the name of offering services at a lower cost, security must not be compromised (Tran & Corner, 2016). In that aspect, scan and pay model was a failure (Taylor, 2016).
ii. Mobile phones were three times susceptible to phishing attacks than a desktop computer due to the varying system architectures (Goel & Jain, 2017).

Table 3 (Continue)

Solutions
Security
i. Fingerprint biometric technology should be encrypted and authenticated for safer use (Belkhede et al., 2012).
ii. Selfie usage in smartphones would aid facial recognition for bank transaction authentication (Cook, 2017).
iii. Tokenization of Payments using identification numbers will help keep bank transactions hidden from intruders (Yu et al., 2017).
iv. Banking security technology must shift from authentication to non-repudiation of bank transactions (Britto et al., 2012).
Impacts
Trust
i. Trust depends on mobile banking application's security character, the information technology teams integrity and the awareness programs that banks organize (Chandio et al., 2013). Trust is also based upon mobile phone operators (de Reuver et al., 2015).
ii. Initial trust starts with task-technology fit on performance expectancy (Oliveira et al., 2014). It must be supplemented with self-learning (Shaw, 2014). Trust and self-efficacy leads to mobile banking adoption (Shankar & Datta, 2018).
iii. Trust is created out of good service quality (Arcand et al., 2017).
iv. Trust and perceived risk must go hand in hand (Slade et al., 2015).
v. Mobile payments offered by banks were considered to be trustworthy than retail mobile payment providers or mobile operators (Tran & Corner, 2016).
vi. Confirmation from the bank about each transaction boosted trust, customer satisfaction and perceived usefulness (Susanto et al., 2016). Moreover, confirmation received from government agencies would be comparatively more convincing and satisfying for mobile banking users (Upadhyay & Chattopadhyay, 2015).
Risk perception
i. Non-users dread using mobile banking due to the existence of third parties (Xin et al., 2015). They even feared a simple security feature like a PIN (Personal Identification Number) (Sohail & Al-Jabrib, 2013). They need structural assurances and familiarity to overcome this aversion (Zhou, 2012). They need the help of agents, in some cases (Tobbin, 2012).
ii. A negative risk perception was a deterrent towards the adoption of mobile banking (Alalwan et al., 2016). It was due to the information content and the nature of mobile banking (Sreejesh et al., 2016). But, a customer with positive attitude would overcome negative perception (Garrett et al., 2014).

Table 3 *(Continue)*

Risk perception
iii. Risk perception changes depending on the skills that each customer had (Ozturk et al., 2017). Perceived risk and perceived control influenced the adoption of mobile banking for urban city users. It was only perceived control for metropolitan city users (Gupta et al., 2017).
iv. Frequent users were still averse to risk (Cao et al., 2018).
v. Risk removed the hedonic motivation out of mobile banking (Cocosila & Trabelsi, 2016).
vi. Social influence reduced perceived risk in potential users of mobile banking (Yang et al., 2012).
Security
i. Privacy and confidentiality breach discouraged mobile banking adoption (Vaithilingam et al., 2013). If customers had a prior online shopping experience, privacy concerns about mobile payments were set to come down (Su et al., 2018).
ii. Security had a negative relationship with hedonic motivation to use mobile banking (Boonsiritomachai & Pitchayadejanant, 2017).
iii. Apart from security, the fear of social rejection and the system performance failure causes aversion to mobile banking (Yadav et al., 2015).
iv. Full-time employees were more worried about security than students (Bhatiasevi, 2015).
v. Publicizing the mobile banking security measures undertaken by the bank in the website could lead to wider transparency and increased trust (Malaquias & Hwang, 2016).

Following are the potentially open problems that were discussed in the previous studies:

A smartphones' ever-growing storage space was an indirect potential threat for stealing critical data that was stored in these phones (Das & Khan, 2016) Smartphone users were poor at security practices (Jones & Chin, 2015).

Frequent changes in Subscriber Identification Module (SIM) makes it hard for banks to authenticate its customers (Kizzaa, 2013).

CONCLUSION, SCOPE AND LIMITATIONS OF THE STUDY

The intensity of trust wavered between the computer (website) and smartphone (web application). There were studies still undertaken to prove the credibility of each device. Previous studies also revolved around the familiarity and the age of respondents who handled online banking for quite a long time. It was not able to set a benchmark stating the optimum level of years needed to call someone an established online banking user.

However, each of these devices was found to possess security characteristics of their own. Both the computer and the smartphone had external cyber threats, the cost involved in overcoming security issues, adequate awareness, owning up the security of the devices. Bank customers were never ready to take up the blame. Mobile phone users were more vulnerable than desktop users since the level of security that a desktop user would take to secure the device was seen to be much higher. Moreover, ignorance of a mobile phone's operational function was another reason (Kiljan et al., 2018; Zhang et al., 2017).

Protection agencies and banks were called to avoid victimization of online banking users. It also challenged the training and awareness methodology effectiveness which needed upgrading and loopholes to be plugged up. There was a missing link that awareness programs had. Such programs were deemed to be information dispensing platforms rather than hands-on training venues. "Did security upgrades kill ubiquity?" was a relevant question that was pointed out.

The core anxiety that existed both for non-users and users was assurance. This was echoed in several papers. A focus on how structural assurances could be provided and its effect on increasing electronic trust could be looked into. The role of how structural assurances and physical banks support played a major part in reducing security apprehensions could not be denied. If online banking and mobile banking were tools that banks used to reach the doorsteps of customers, the same enthusiasm from banks never existed when it came to the security of these devices while undertaking banking transactions. With regard to the web application, bank customers apprehension existed on the accounts that were vulnerable in the hands of third party service providers.

With regard to smartphones or computers, it was better to employ facial recognition security system while banking. Such a technology was emerging and ubiquitous. It promised far superior security when compared to other biometric systems, since it took the control from humans and placed it on machines in order to maintain integrity in authentication (Xiao & Yang, 2010). Studies could focus on the acceptability of such a technology among users for long-term usage.

As time passes by, the debate as to whether the bank or the customer was responsible for the cybersecurity issues have not yet reached a consensus. Ease of usage was considered hindrance for the adoption of online banking. Such a notion had been questioned now, on the premise of lack of security in online banking. Taking TAM (Technology Acceptance Model) as the base, many researchers argued regarding the relevance of trust. There was still a confusion on what trust influenced and did not.

As this paper analyzed past trends, it was observed that adoption of mobile banking was the prime arena in which security was discussed. It did not matter what device was used, but rather it was the open network that was common to both computer and smartphones that led to security issues. Neither of the devices scored higher with regard to the degree

of risk, rather, the risk was found to be prevalent. Each solution discussed was unique, however, challenges existed when it came to implementation due to time and cost that was involved. As technology became redundant, so did the solutions. Hence, a sustainable solution that would keep bank customers safe continued as a quest for researchers in the years to come. However, customers believed that regardless of the smartphone or the desktop, they trusted that bank offered devices to be safer than user-owned devices (McGill & Thompson, 2017). Figure 3 is given below as a snapshot to the differences between internet and mobile banking.

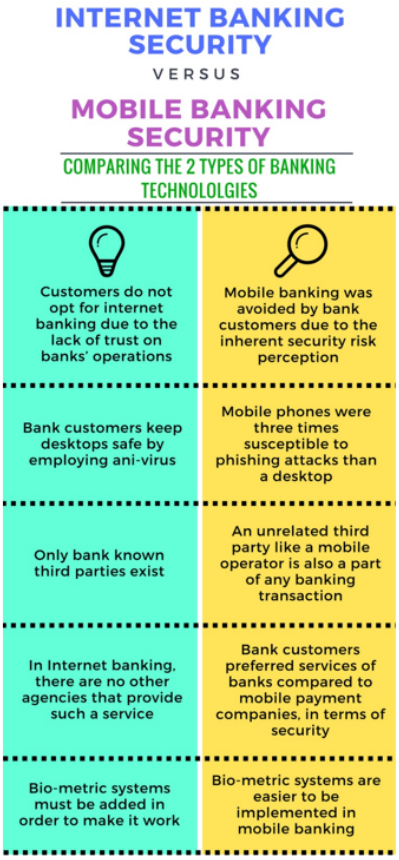

Figure 3. Differences in technology security of internet and mobile banking

This paper had focused on the banking cyber security aspects of computer and mobile phone devices since both the devices were the centre of attention when it came to Information and Communication Technology (ICT) studies. The computer was the basic device out of which other devices have evolved over time and smartphones are devices that have reached the masses extensively. The study had followed the traditional method of evaluating, analyzing and synthesizing the past six years literature works of various

authors. This paper dealt with factors that were both conceptual as well as technical aspect of security issues. An effort had been made to balance both, but it was done by keeping the conceptual aspect as the base for all the technical solutions discussed. At various junctures, the paper had also taken into account the security issues and challenges that the device produces, wherein the banking element would seem missing. Solutions discussed were not an end for security issues. Deliberations that were mentioned focused on the prevalent thoughts about bank technology security doing rounds in various circles. Impacts inferred noted on the pattern of behaviour that both humans and technology showed under various circumstances.

An aligning area was the emerging electronic commerce and mobile commerce industry which had a connection with mobile payment aspect. This paper had not ventured into those aspects.

REFERENCES

Akhlaq, A., & Ahmed, E. (2013). The effect of motivation on trust in the acceptance of internet banking in a low income country. *International Journal of Bank Marketing, 31*(2), 115-125.

Akram, R. N., Chen, H. H., Lopez, J., Sauveron, D., & Yang, L. T. (2018). Security, privacy and trust of user-centric solutions. *Future Generation Computer Systems, 80*, 417-420.

Alalwan, A. A., Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management, 37*(3), 99-110.

Alhabash, S., Jiang, M., Brooks, B., Rifon, N. J., LaRose, R., & Cotten, S. R., (2015). *Online banking for the ages: Generational differences in institutional and system trust.* Bradford, UK: Emerald Group Publishing Limited.

Andaleeb, S. S., Rashid, M., & Rahman, Q. A. (2016). A model of customer-centric banking practices for corporate clients in Bangladesh. *International Journal of Bank Marketing, 34*(4), 458-475.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185-197.

Arcand, M., PromTep, S., Brun, I., & Rajaobelina, L. (2017). Mobile banking service quality and customer relationships. *International Journal of Bank Marketing, 35*(7), 1068-1089.

Ashta, A. (2017). Evolution of mobile banking regulations: a case study on legislator's behavior. *Strategic Change, 26*(1), 3-20.

Ayo, C. K., Oni, A. A., Adewoye, O. J., & Eweoya, I. O. (2016). E-banking users' behaviour: E-service quality, attitude, and customer satisfaction. *International Journal of Bank Marketing, 34*(3), 347-367.

Bashir, I., & Madhavaiah, C. (2014). Determinants of young consumers' intention to use Internet banking services in India. *Vision, 18*(3), 153-163.

Bashir, I., & Madhavaiah, C. (2015). Consumer attitude and behavioural intention towards Internet banking adoption in India. *Journal of Indian Business Research, 7*(1), 67-102.

Basias, N., Themistocleous, M., & Morabito, V. (2013). SOA adoption in e-banking. *Journal of Enterprise Information Management, 26*(6), 719-739.

Bauer, S., Bernroider, E.W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers and Security, 68*, 145-159.

Belkhede, M., Gulhane, V., & Bajaj, P. (2012). Biometric mechanism for enhanced security of online transaction on Android system: A design approach. In *Proceedings of 14th International Conference on Advanced Communication Technology (ICACT)* (pp. 1193-1197). Pyeong Chang, Korea (South).

Berraies, S., Ben Yahia, K., & Hannachi, M. (2017). Identifying the effects of perceived values of mobile banking applications on customers: Comparative study between baby boomers, generation X and generation Y. *International Journal of Bank Marketing, 35*(6), 1018-1038.

Bhatiasevi, V. (2016). An extended UTAUT model to explain the adoption of mobile banking. *Information Development, 32*(4), 799-814.

Blauw, F., & Solms, S. V., (2014). Streamlined approach to online banking authentication in South Africa and Europe. In *Proceedings of IST-Africa 2014 Conference* (pp. 1-10). Dublin, Ireland.

Blut, M., Wang, C., & Schaefer, K. (2016). Factors influencing the acceptance of self-service technologies: A meta-analysis. *Journal of Service Research, 19*(4), 396-416.

Bojjagani, S., & Sastry, V. N. (2017). A secure end-to-end SMS-based mobile banking protocol. *International Journal of Communication Systems, 30*(15), 1-19.

Boon-itt, S. (2015). Managing self-service technology service quality to enhance e-satisfaction. *International Journal of Quality and Service Sciences, 7*(4), 373-391.

Boonsiritomachai, W., & Pitchayadejanant, K. (2017). Determinants affecting mobile banking adoption by generation Y based on the Unified Theory of Acceptance and Use of Technology Model modified by the Technology Acceptance Model concept. *Kasetsart Journal of Social Sciences, 30*, 1-10.

Britto, S., Kumar, R., & Rabara, S. A. (2012). An end-to-end secure mobile payment system using public key infrastructure system. *Journal of Algorithms and Computational Technology, 6*(3), 395-409.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication and Society, 20*(8), 1261-1278.

Butler, M., & Butler, R. (2015). Investigating the possibility to use differentiated authentication based on risk profiling to secure online banking. *Information and Computer Security, 23*(4), 421-434.

Butt, M. M., & Aftab, M. (2013). Incorporating attitude towards Halal banking in an integrated service quality, satisfaction, trust and loyalty model in online Islamic banking context. *International Journal of Bank Marketing, 31*(1), 6-23.

Cao, X., Yu, L., Liu, Z., Gong, M., & Adeel, L. (2018). Understanding mobile payment users' continuance intention: A trust transfer perspective. *Internet Research, 28*(2), 456-476.

Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *Computers and Security, 53*, 175-186.

Chandio, F. H., Irani, Z., Abbasi, M. S., & Nizamani, H. A. (2013). Acceptance of online banking information systems: an empirical case in a developing economy. *Behaviour and Information Technology, 32*(7), 668-680.

Chaouali, W., Yahia, I. B., & Souiden, N. (2016). The interplay of counter-conformity motivation, social influence, and trust in customers' intention to adopt Internet banking services: The case of an emerging country. *Journal of Retailing and Consumer Services, 28*, 209-218.

Chaturvedi, M., Narain Singh, A., Prasad Gupta, M., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transforming Government: People, Process and Policy, 8*(3), 374-397.

Chemingui, H., & Lallouna, H. B. (2013). Resistance, motivations, trust and intention to use mobile financial services. *International Journal of Bank Marketing, 31*(7), 574-592.

Chen, C. (2013). Perceived risk, usage frequency of mobile banking services. *Managing Service Quality: An International Journal, 23*(5), 410-436.

Clark, M., & Harrell, C. E. (2013). Unlike chess, everyone must continue playing after a cyber-attack. *Journal of Investment Compliance, 14*(4), 5-12.

Clemente-Ricolfe, J. S. (2017). Consumer perceptions of online banking in Spain using netnography: A positioning story. *International Journal of Bank Marketing, 35*(6), 966-982.

Cocosila, M., & Trabelsi, H. (2016). An integrated value-risk investigation of contactless mobile payments adoption. *Electronic Commerce Research and Applications, 20*, 159-170.

Cook, S. (2017). Selfie banking: is it a reality? *Biometric Technology Today, 3*, 9-11.

Damghanian, H., Zarei, A., & Kojuri, M. A. S. (2016). Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran. *Journal of Internet Commerce, 15*(3), 214-238.

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security, 24*(1), 116-134.

de Reuver, M., Nikou, S., & Bouwman, H. (2015). The interplay of costs, trust and loyalty in a service industry in transition: The moderating effect of smartphone adoption. *Telematics and Informatics, 32*(4), 694-700.

Duane, A., O'Reilly, P., & Andreev, P. (2014). Realising M-Payments: modelling consumers' willingness to M-pay using smart phones. *Behaviour and Information Technology, 33*(4), 318-334.

Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the internet of things. *Info, 16*(3), 1-21.

Fonseca, J. R. (2014). E-banking Culture: A comparison of EU 27 countries and Portuguese case in the EU 27 retail banking context. *Journal of Retailing and Consumer Services, 21*(5), 708-716.

Febelfin. (2013). *Safe internet banking? Here is some useful advice!* Retrieved March 25, 2018, from https://www.safeinternetbanking.be/en/safe-internet-banking-here-some-useful-advice.

Garrett, J. L., Rodermund, R., Anderson, N., Berkowitz, S., & Robb, C. A. (2014). Adoption of mobile payment technology by consumers. *Family and Consumer Sciences Research Journal, 42*(4), 358-368.

Giovanis, A. N., Binioris, S., & Polychronopoulos, G. (2012). An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece. *EuroMed Journal of Business, 7*(1), 24-53.

Glavee-Geo, R., Shaikh, A. A., & Karjaluoto, H. (2017). Mobile banking services adoption in Pakistan: Are there gender differences?. *International Journal of Bank Marketing, 35*(7), 1090-1114.

Goel, D., & Jain, A. K. (2017). Mobile phishing attacks and defence mechanisms: state of art and open research challenges. *Computers and Security, 73*, 519-544.

Gupta, S., Yun, H., Xu, H., & Kim, H. W. (2017). An exploratory study on mobile banking adoption in Indian metropolitan and urban areas: a scenario-based experiment. *Information Technology for Development, 23*(1), 127-152.

Hampshire, C. (2017). A mixed methods empirical exploration of UK consumer perceptions of trust, risk and usefulness of mobile payments. *International Journal of Bank Marketing, 35*(3), 354-369.

Harrison, T. S., Onyia, O. P., & Tagg, S. K. (2014). Towards a universal model of internet banking adoption: Initial conceptualization. *International Journal of Bank Marketing, 32*(7), 647-687.

Hoffmann, A. O., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. *International Journal of Bank Marketing, 30*(5), 390-407.

Ivaturi, K., & Janczewski, L. (2013). Social engineering preparedness of online banks: An Asia-Pacific perspective. *Journal of Global Information Technology Management, 16*(4), 21-46.

Jansen, J., & Schaik, P. V. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security, 25*(2), 165-180.

Jeske, D., & Schaik P. V. (2017). Familiarity with Internet threats: Beyond awareness. *Computers and Security, 66*, 129-141.

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management, 35*(5), 561-571.

Juwaheer, T. D., Pudaruth, S., & Ramdin, P. (2012). Factors influencing the adoption of internet banking: A case study of commercial banks in Mauritius. *World Journal of Science*, *Technology and Sustainable Development, 9*(3), 204-234.

Kaabachi, S., Mrad, S. B., & Petrescu, M. (2017). Consumer initial trust toward internet-only banks in France. *International Journal of Bank Marketing, 35*(6), 903-924.

Kesharwani, A., & Tripathy, T. (2012). Dimensionality of perceived risk and its impact on Internet banking adoption: An empirical investigation. *Services Marketing Quarterly, 33*(2), 177-193.

Khalilzadeh, J., Ozturk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior, 70*, 460-474.

Kiljan, S., Vranken, H., & Eekelen, M. V. (2018). Evaluation of transaction authentication methods for online banking. *Future Generation Computer Systems, 80*, 430-447.

Kizza, J. M. (2013). Mobile money technology and the fast disappearing African digital divide. *African Journal of Science, Technology, Innovation and Development, 5*(5), 373-378.

Koong, K. S., Liu, L. C., Qin, H., & Ying, T. (2017). Occurrences of online fraud complaints: 2002 through 2015. *International Journal of Accounting and Information Management, 25*(4), 484-504.

Kumar, V., Kumar, U., & Shareef, M. A. (2017). Mobile banking: A tradeoff between mobile technology and service for consumer behavioural intentions. *Transnational Corporations Review, 9*(4), 319-330.

Kundu, S., & Datta, S. K. (2015). Impact of trust on the relationship of e-service quality and customer satisfaction. *EuroMed Journal of Business, 10*(1), 21-46.

Laukkanen, T. (2016). Consumer adoption versus rejection decisions in seemingly similar service innovations: The case of the Internet and mobile banking. *Journal of Business Research, 69*(7), 2432-2439.

Li, D. C. (2015). Online Security Performances and Information Security Disclosures. *Journal of Computer Information Systems, 55*(2), 20-28.

Liébana-Cabanillas, F., Munoz-Leiva, F., & Rejón-Guardia, F. (2013). The determinants of satisfaction with e-banking. *Industrial Management and Data Systems, 113*(5), 750-767.

Maditinos, D., Chatzoudes, D., & Sarigiannidis, L. (2013). An examination of the critical factors affecting consumer acceptance of online banking: A focus on the dimensions of risk. *Journal of Systems and information Technology, 15*(1), 97-116.

Makanyeza, C. (2017). Determinants of consumers' intention to adopt mobile banking services in Zimbabwe. *International Journal of Bank Marketing, 35*(6), 997-1017.

Malaquias, F. F., & Hwang, Y. (2016). Trust in mobile banking under conditions of information asymmetry: Empirical evidence from Brazil. *Information Development, 32*(5), 1600-1612.

Mansour, K. B. (2016). An analysis of business' acceptance of internet banking: An integration of e-trust to the TAM. *Journal of Business and Industrial Marketing, 31*(8), 982-994.

MarkMonitor. (2014). *MarkMonitor Press Release*. Retrieved March 18, 2018, from https://www.markmonitor.de/brand-protection-domain-management-resources/press-releases/release/latest-research-finds-one-in-six-online-bargain-hunters-duped-by-sites-selling-counterfeit-goods.

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management, 34*(1), 1-13.

Mason, S. (2013). Electronic banking and how courts approach the evidence. *Computer Law and Security Review, 29*(2), 144-151.

Mason, S., & Bohm, N. (2018). Banking and fraud. *Computer Law and Security Review, 33*, 237–241.

McGill, T., & Thompson, N. (2017). Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour and Information Technology, 36*(11), 1111-1124.

McNeish, J. (2015). Consumer trust and distrust: Retaining paper bills in online banking. *International Journal of Bank Marketing, 33*(1), 5-22.

Mishra, V., & Singh, V. (2015). Selection of appropriate electronic banking channel alternative: Critical analysis using analytical hierarchy process. *International Journal of Bank Marketing, 33*(3), 223-242.

Mohammadi, H. (2015). A study of mobile banking usage in Iran. *International Journal of Bank Marketing, 33*(6), 733-759.

Montazemi, A. R., & Qahri-Saremi, H. (2015). Factors affecting adoption of online banking: A meta-analytic structural equation modeling study. *Information and Management, 52*(2), 210-226.

Mullan, J., Bradley, L., & Loane, S. (2017). Bank adoption of mobile banking: stakeholder perspective. *International Journal of Bank Marketing, 35*(7), 1154-1174.

Murari, K., & Tater, B. (2014). Employee's attitude towards adoption of IT-based banking services: A case of Indian private sector banks. *Competitiveness Review, 24*(2), 107-118.

Mzoughi, N., & M'Sallem, W. (2013). Predictors of internet banking adoption: Profiling Tunisian postponers, opponents and rejectors. *International Journal of Bank Marketing, 31*(5), 388-408.

Nagaraju, S., & Parthiban, L. (2015). Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *Journal of Cloud Computing, 4*(1), 1-23.

Nel, J., & Boshoff, C. (2017). Development of application-based mobile-service trust and online trust transfer: An elaboration likelihood model perspective. *Behaviour and Information Technology, 36*(8), 809-826.

Oliveira, T., Faria, M., Thomas, M. A., & Popovič, A. (2014). Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. *International Journal of Information Management, 34*(5), 689-703.

Ong, K. S., Nguyen, B., Faridah, S., & Alwi, S. (2017). Consumer-based virtual brand personality (CBVBP), customer satisfaction and brand loyalty in the online banking industry. *International Journal of Bank Marketing, 35*(3), 370-390.

Ozturk, A. B., Bilgihan, A., Salehi-Esfahani, S., & Hua, N. (2017). Understanding the mobile payment technology acceptance based on valence theory: A case of restaurant transactions. *International Journal of Contemporary Hospitality Management, 29*(8), 2027-2049.

Patsiotis, A. G., Hughes, T., & Webber, D. J. (2012). Adopters and non-adopters of internet banking: A segmentation study. *International Journal of Bank Marketing, 30*(1), 20-42.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: A comparative study. *Information and Computer Security, 25*(2), 181-189.

Purkait, S., Kumar De, S., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management and Computer Security, 22*(3), 194-234.

Purwanegara, M., Apriningsih, A., & Andika, F. (2014). Snapshot on Indonesia regulation in mobile internet banking users attitudes. *Procedia-Social and Behavioral Sciences, 115*, 147-155.

Rawashdeh, A. (2015). Factors affecting adoption of internet banking in Jordan: Chartered accountant's perspective. *International Journal of Bank Marketing, 33*(4), 510-529.

Raza, S. A., Jawaid, S. T., & Hassan, A. (2015). Internet banking and customer satisfaction in Pakistan. *Qualitative Research in Financial Markets, 7*(1), 24-36.

Riffai, M. M. M. A., Grant, K., & Edgar, D. (2012). Big TAM in Oman: Exploring the promise of on-line banking, its adoption by customers and the challenges of banking in Oman. *International journal of information management, 32*(3), 239-250.

Roy, S. K., Balaji, M. S., Kesharwani, A., & Sekhon, H. (2017). Predicting Internet banking adoption in India: A perceived risk perspective. *Journal of Strategic Marketing, 25*(5-6), 418-438.

Seda, L. (2014). Identity theft and university students: do they know, do they care? *Journal of Financial Crime, 21*(4), 461-483.

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics, 32*(1), 129-142.

Shankar, A., & Datta, B. (2018). Factors affecting mobile payment adoption intention: An Indian perspective. *Global Business Review, 19*(3S), 1–18.

Shanmugam, M., Wang, Y. Y., Bugshan, H., & Hajli, N. (2015). Understanding customer perceptions of internet banking: the case of the UK. *Journal of Enterprise Information Management, 28*(5), 622-636.

Sharma, S. K., Govindaluri, S. M., & Al Balushi, S. M. (2015). Predicting determinants of Internet banking adoption: A two-staged regression-neural network approach. *Management Research Review, 38*(7), 750-766.

Shaw, N. (2014). The mediating influence of trust in the adoption of the mobile wallet. *Journal of Retailing and Consumer Services, 21*(4), 449-459.

Sikdar, P., Kumar, A., & Makkad, M. (2015). Online banking adoption: A factor validation and satisfaction causation study in the context of Indian banking customers. *International Journal of Bank Marketing, 33*(6), 760-785.

Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: extending UTAUT with innovativeness, risk, and trust. *Psychology and Marketing, 32*(8), 860-873.

Sohail, M. S., & Al-Jabri, I. M. (2014). Attitudes towards mobile banking: are there any differences between users and non-users? *Behaviour and information technology, 33*(4), 335-344.

Sreejesh, S., Anusree, M. R., & Mitra, A. (2016). Effect of information content and form on customers' attitude and transaction intention in mobile banking moderating role of perceived privacy concern. *International Journal of Bank Marketing, 34*(7), 1092-1113.

Su, P., Wang, L., & Yan, J. (2018). How users' Internet experience affects the adoption of mobile payment: A mediation model. *Technology Analysis and Strategic Management, 30*(2), 186-197.

Susanto, A., Chang, Y., & Ha, Y. (2016). Determinants of continuance intention to use the smartphone banking services: An extension to the expectation-confirmation model. *Industrial Management and Data Systems, 116*(3), 508-525.

Susanto, A., Lee, H., Zo, H., & Ciganek, A. P. (2013). User acceptance of Internet banking in Indonesia: Initial trust formation. *Information Development, 29*(4), 309-322.

Szopiński, T. S. (2016). Factors affecting the adoption of online banking in Poland. *Journal of Business Research, 69*(11), 4763-4768.

Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modeling approach. *Information Technology and People, 29*(4), 830-849.

Tassabehji, R., & Kamala, M. A. (2012). Evaluating biometrics for online banking: The case for usability. *International Journal of Information Management, 32*(5), 489-494.

Taylor, E. (2016). Mobile payment technologies in retail: a review of potential benefits and risks. *International Journal of Retail and Distribution Management, 44*(2), 159-177.

Thakur, R. (2014). What keeps mobile banking customers loyal? *International Journal of Bank Marketing, 32*(7), 628-646.

Tobbin, P. (2012). Towards a model of adoption in mobile banking by the unbanked: A qualitative study. *Info, 14*(5), 74-88s.

Tran, H. T. T., & Corner, J. (2016). The impact of communication channels on mobile banking adoption. *International Journal of Bank Marketing, 34*(1), 78-109.

Upadhyay, P., & Chattopadhyay, M. (2015). Examining mobile based payment services adoption issues: A new approach using hierarchical clustering and self-organizing maps. *Journal of Enterprise Information Management, 28*(4), 490-507.

Upadhyay, P., & Jahanyan, S. (2016). Analyzing user perspective on the factors affecting use intention of mobile based transfer payment. *Internet Research, 26*(1), 38-56.

Vaithilingam, S., Nair, M., & Guru, B. K. (2013). Do trust and security matter for the development of M-banking? Evidence from a developing country. *Journal of Asia-Pacific Business, 14*(1), 4-24.

Wojewidka J. (2017). Why the mobile biometrics surge demands true liveness. *Biometric Technology Today*, *10*, 8-11.

Wonglimpiyarat, J. (2014). Competition and challenges of mobile banking: A systematic review of major bank models in the Thai banking industry. *The Journal of High Technology Management Research, 25*(2), 123-131.

Xiao, Q., & Yang, X. D. (2010). Facial recognition in uncontrolled conditions for information security. *EURASIP Journal on Advances in Signal Processing, 1*, 1-9.

Xin, H., Techatassanasoontorn, A. A., & Tan, F. B. (2015). Antecedents of consumer trust in mobile payment adoption. *Journal of Computer Information Systems, 55*(4), 1-10.

Yadav, R., Chauhan, V., & Pathak, G. S. (2015). Intention to adopt internet banking in an emerging economy: A perspective of Indian youth. *International Journal of Bank Marketing, 33*(4), 530-544.

Yang, S., Lu, Y., Gupta, S., Cao, Y., & Zhang, R. (2012). Mobile payment services adoption across time: An empirical study of the effects of behavioral beliefs, social influences, and personal traits. *Computers in Human Behavior, 28*(1), 129-142.

Yiga, C., & Cha, K. J. (2016). Toward understanding the importance of trust in influencing Internet banking adoption in Uganda. *Information Development, 32*(3), 622-636.

Yousafzai, S., & Yani-de-Soriano, M. (2012). Understanding customer-specific factors underpinning internet banking adoption. *International Journal of Bank Marketing, 30*(1), 60-81.

Yu, P. L., Balaji, M. S., & Khong, K. W. (2015). Building trust in internet banking: a trustworthiness perspective. *Industrial Management and Data Systems, 115*(2), 235-252.

Yu, X., Kywe, S. M., & Li, Y. (2017). Security Issues of In-Store Mobile Payment. *In Handbook of Blockchain, Digital Finance, and Inclusion, 2*, 115-144.

Yuen, Y. Y., Yeow, P. H., & Lim, N. (2015). Internet banking acceptance in the United States and Malaysia: a cross-cultural examination. *Marketing Intelligence and Planning, 33*(3), 292-308.

Zhang, W., & Morana, M. (2012, April 15). *Architectural Design Patterns for SSO (Single Sign On) Design and Use Cases for Financial Web Applications*. Retrieved April 7, 2018, from https://www.slideshare.net/marco_morana/presentation-sso-designsecurity

Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviors of smartphone users in China: An empirical analysis. *The Electronic Library*, *35*(6), 1177-1190.

Zhou, T. (2012). Understanding users' initial trust in mobile banking: An elaboration likelihood perspective. *Computers in Human Behavior*, *28*(4), 1518-1525.

Zhou, T. (2013). An empirical examination of continuance intention of mobile payment services. *Decision Support Systems*, *54*(2), 1085-1091.