International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 5
ISSN: 2088-5334

Investigating the Security Threats on Using M-Payment Applications in Saudi Arabia: Exploratory Study

Raed Alotaibi [a], Abdulrahman Alghamdi [b,*]

[a] *Shaqra Community College, Shaqra University, Kingdom of Saudi Arabia*
[b] *College of Computing and Information Technology, Shaqra University, Kingdom of Saudi Arabia*
Corresponding author: [*]alghamdia@su.edu.sa

***Abstract*— Online banking, debit cards, credit cards and mobile payments are the most common payment types in Saudi Arabia. This study explored security threats that affect m-payment applications in Saudi Arabia by interviewing 16 IT professionals to explore their insights and opinions about those security threats. Cybersecurity threats present the biggest challenge for most mobile systems, as mobile payments can be affected by cyber-attacks and require sophisticated approaches to achieve the desired security. In our study we report on the impact of security threats on the utilization of mobile payment applications and provide evidence related to those threats and their impact on the use of mobile payment applications. Evidence was provided regarding the security threats and their impact on using mobile payment applications. Information was also provided related to security threats such as Distributed Denial-of-Service, phishing attacks and malware. Although the participants in this study demonstrated a positive attitude regarding the safety and security of mobile payments, they also highlighted the security threats that impact m-payments. The results showed that the three main threats in Saudi Arabia were Distributed Denial-of-Service (DDoS), phishing attacks and Malware (Malicious software). This study makes two contributions. The first is to theory, by filling the gap in the literature because it is the first study to explore the threats to using m-payment in Saudi Arabia. Secondly, this study contributes to practice by providing a clear picture for service providers and users about threats they may face when using m-payment.**

***Keywords*— Cybersecurity; cyber threats; mobile payments security; information systems; computer science.**

Manuscript received 8 Sep. 2021; revised 16 Dec. 2021; accepted 17 Jan. 2022. Date of publication 31 Oct. 2022.

I. INTRODUCTION

Payment mechanisms have improved dramatically in recent years. Everyone used to pay by cash. Bank cards were then implemented as a new payment method. Among the benefits of mobile banking is that cards are now being introduced with the latest technologies, finding their way into smartphones via NFC. The financial services sector has recognized the promise of mobile banking and is embracing mobile banking apps. In Saudi Arabia, online banking, debit cards, credit cards, and mobile payments are the most common payment types. Many m-payment systems have been implemented and are widely used because they have advantages such as being broadly accessible, having lower transaction costs, and being easily used [1]. Contactless payment technologies are gaining acceptance in Saudi Arabia due to government policy resulting from the COVID -19 pandemic, with mobile payments being the latest payment system. Although mobile payments have been steadily gaining acceptance in Saudi Arabia, little research has been conducted to investigate the barriers to mobile payment adoption among its citizens [2]. Mobile payments refer to online payment activities using mobile devices (for example, a smartphone) to transfer money, make online purchases, pay bills, etc. While they provide users with a high level of convenience, they are vulnerable to multiple mobile payment system attacks. Due to advances in mobile technology and the use of smartphones, smartphones have been widely recognized as a potential payment option and a great successor to card payments, as people prefer to carry their mobile devices everywhere rather than their wallets [3]. This study explored the security threats that impact m-payment applications in Saudi Arabia by interviewing IT professionals. According to Liao and Yang [4], "Mobile payments are services that use mobile devices to make payments". In developing countries, the adoption of m-payments is weak [5]. Liao and Yang [4] claimed that m-payments will be the main method in commercial transactions in physical stores and websites because they rely on new smart technologies. There are some advantages to using m-payments such as bulk

payments, security, eliminating the need for cash, convenience, and speed of transactions [6]. According to Sundaram et al [7], there are some serious cyber threats that can negatively affect users and companies such as DDoS attacks (Distributed Denial-of-Service), malicious software (malware) and phishing attacks. Interest in mobile payment services has increased as many businesses and customers have realized the benefits. The use of mobile payment services has proven beneficial to consumers and businesses alike [8].

Furthermore, mobile payments have offered great benefits and many challenges. Cybersecurity threats are the biggest challenge for most mobile systems as mobile payments are likely to be affected by cyberattacks and require sophisticated approaches to achieve the desired security [9]. In addition to the usefulness and importance of cybersecurity for mobile payments systems [10], [11], it is also necessary to discuss previous research in mobile payment systems security and highlight and describe some potential threats in those systems.

A secure Mutual Authentication Protocol (SMAP) based on a Universal 2nd Factor (U2F) protocol has been proposed to protect user account security and improve the mobile payment experience. Mobile payment protection has been considered by focusing on phishing attacks on the Android platform. This has involved developing a defense strategy that monitors running apps and alerts users when malicious apps leak payment information. The strategy's feasibility has been demonstrated by using an Alipay dataset [12]. A thorough assessment of the many aspects of the m-payment system, including vulnerability analysis, infrastructure, architecture, and threats from potential and probable worms and viruses, was presented by Hassan et al. [13]. Wazid et al. [8] evaluated the exploitation and vulnerabilities of current and potential malware for mobile phones. Bosamia [14] investigated and assessed potential threats and vulnerabilities to mobile wallets and concluded that the trust boundaries for mobile wallets in the current payment approach are highly elevated. However, threat identification approaches have not matured to the extent predicted. Due to the exponential growth of mobile wallets, the entire field is still under intense research, including new solutions to specific threats or vulnerabilities.

Jin et al. [15] examined mobile payment security threats and ways to develop security approaches to reduce security risks to the bare minimum. They made the following recommendations: (1) Users must have a dialectical mindset and be aware of mobile payments; (2) Users should not be so concerned about security threats that they are afraid to use them or are overconfident in their ability to use them without protection; (3) As technology advances, new security threats can emerge, so users should be vigilant and continue to learn and master security knowledge and skills and flexibly employ appropriate preventive measures to monitor their security risks and mitigate potential losses effectively. Mobile payments have introduced both great benefits and many problems since their introduction. The biggest challenge for most mobile systems is related to cybersecurity threats, as mobile payments can be affected by cyber-attacks and require sophisticated approaches to achieve the desired security [9]. It is necessary to mitigate cyber dangers and threats [16]. Ease of use and trust influence the attitude toward using e-payment systems [17]. We next present and describe the potential threats to and vulnerabilities of mobile payment systems.

A. Distributed Denial of Service (DDOS) Attacks

DDoS attacks on payments are a growing threat. They involve resetting or overwhelming target resources to the point where their system, application, or network becomes unavailable to their user base. There are three types of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: (1) Flooding attacks; (2) Protocol attacks, and (3) Application Layer attacks. DDoS attacks are initiated by threat actors seeking to interrupt mobile payment services. These might affect transactions related to services hosted in the cloud [18]. Distributed Denial-of-Service (DDoS) is considered to be a crucial and longstanding threat on the Internet [19] . Similarly, [20] claimed that Distributed Denial of Service (DDoS) attacks aim to deny services on the Internet and have become one of the most dangerous threats to the Internet and to users. [21]noted that it is easy to conduct a DDoS attack even if there are not many resources.

B. Phishing Attacks

Phishing attacks are one of the most serious attacks in which an attacker attempts to obtain and impersonate victims' credentials [22]. Mobile phones have customers' personal and corporate data that can be used to conduct sophisticated attacks. Users are attacked by e-mails in an attempt to trick them into disclosing information. According to Goel and Jain [23], "Phishing is an online identity theft in which an attacker tries to steal user's personal information, resulting in financial loss of individuals as well as organizations." In the past, phishing attacks focused on desktop users, but they now focus on mobile device users [19] [23]. Datta et al. [24] believed that users could be hacked by social engineering and cyberstalking to steal their money, and it is difficult to follow the hackers on the Internet who successfully exploit this. Rivers et al. [25] and Bosamia [14] asserted that phishing attacks that aim to obtain users' information are considered to be the main threats to users of mobile wallet applications.

C. Malware (Malicious Software):

Mobile malware is one of the main threats to a mobile payment system. Many mobile payment systems depend on SSL/TLS to protect data on the Internet. However, SSL/TLS and its implementation may also have vulnerabilities that malicious users could leverage to breach security. Malicious software or malware attacks often take advantage of weaknesses in mobile payment services, third-party software, and operating systems to control the target's device. Malware attacks can also use social engineering methods to trick targets into installing the malware and stealing valuable information. Many types of malware exist Trojan Horse, Spyware, Adware, Banking Trojans, Ransomware, Advanced Persistent Threats, and Remote Access Trojans (RATs) [26]. Users should be aware and very cautious because malware attacks can be used to steal important data such as PIN numbers and bank card details [13]. Bosamia [14] claimed that a Malware attack threatens mobile wallet application users. Sharmeen et al. [27] noted that malware is the biggest threat to sensitive data such as corporate/financial information and personal data.

Mobile spyware can be installed on a mobile phone that allows another person to monitor activity on the phone remotely. Users may install such programs without realizing they are installing spyware capable of recording their incoming and outgoing SMS messages and call logs for dialed and received calls. The spyware then sends this data to an account on a server owned by the spyware author. An example of such spyware is Flexispy (spyware), which has existed for some time. In an SMS-based m-payment system, such malware could seriously compromise the user's privacy, as a malicious attacker could make minor changes to such spyware and track all transactions made by a user [28].

II. Materials and Method

This study adopted a qualitative research method to explore the security threats that may impact the use of m-payment applications in Saudi Arabia. This method was adopted because it allows the researcher to explore in-depth participants' opinions about the problem [29]. A qualitative study focuses on how people experience a problem and how they understand it [30]. According to Tomaszewski et al. [29], many qualitative studies are interested in exploring the factors that impact human behavior. To collect the data, semi-structured interviews with 16 Saudi IT professionals were adopted in this study to explore their insights and opinions about security threats that may impact the use of m-payment applications in Saudi Arabia. The sample size of 16 participants is common according to Mason's analysis of 560 Ph.D. studies that adopted qualitative interviews as their main method [31]. Every interview was expected to take approximately 30 minutes. The interview questions were translated into Arabic by expert translators as the target participants were native Arabic speakers. The collected data were translated into English by expert translators to ensure accurate translation. Before conducting the interviews, the researcher sent an e-mail to obtain participants' consent and inform them about the topic and the study's aims. The data were analyzed by NVivo software which has five key functions: to manage data, manage ideas, query data, model visually, and report [30].

III. Results and Discussion

The results revealed that using mobile payment applications was considered by participants to be secure and safe. Participant 1 stated, "Thanks to encryption technology, mobile payments are secure and safe. With 950 million users making mobile transactions according to Statista in 2019 and online banking virtually commonplace, it has to be". Similarly, Participant 2 asserted that "Mobile payment is safe and secure for several reasons. Firstly, mobile payment is more secure than swiping a credit card at a terminal. The financial information or transaction data does not leave the mobile device as opposed to methods like credit card payment, making it more difficult for hackers to compromise it". Participant 4 also commented, "In my opinion, mobile payment is much safer than swiping or online payment methods." He further expressed his opinion when he stated, "This is the case as in most cases when a hacker manages to reach a system, mobile payment data is not recovered, hence, protecting the user's credit or visa card data from hackers.

Moreover, the user's card details are not transferred during a mobile payment transaction. Rather, a more encrypted version of the card details is embedded with the transaction to authorize the payment. However, it is still advisable to be careful even with the latest and advanced payment methods as there are still weaknesses within the system that potential hackers can exploit". Participant 6 claimed that, "Security of mobile payment directly depends on users, how they use it and what they use for their payments." Participant 5 confirmed that "Basically, mobile payment is secure and safe until the leakage of usernames and passwords. Also, it depends on mistakes made by users".

On the other hand, Participant 10 stated, "Mobile payment is still secure and safe if users follow the security instructions as no payment method is completely safe from theft." Participant 15 responded, "It is quite safe and getting better regarding security and privacy measures." To conclude, Participant13 strongly asserted, "It is secure, especially if you are dealing with a known provider. Some security we can influence directly, like having 2FA or a one-time code before accessing the application, and the provider should be under PCI DSS compliance so a user can decide whether to go with them or not. However, in general, these applications will be highly secure."

In this study, we considered the impact of security threats on the utilization of mobile payment applications. Evidence was provided regarding the security threats and their impact on using mobile payment applications. Information was also provided about security threats such as Distributed Denial-of-Service, phishing attacks, and malware. Although the participants in this study demonstrated a positive attitude regarding the safety and security of mobile payments, they also highlighted the security threats that impact m-payments. This outcome is similar to issues addressed by Wycech [32], who found that participants had a positive attitude and that mobile-payment applications are secure and safe because of the encryption technology.

A previous study conducted by Yin et al. [12] supports the argument of this study that the method of m-payment is secure when using the public key encryption cryptosystem. This qualitative study finds that using m-payment applications is more secure than swiping credit or debit cards in public. Similar to the previous study, it also revealed that mobile payment applications save customers the effort of physically getting cash and cards out of their wallets [33]. This study's findings show that m-payment is safe because users follow security instructions as the payment method is not safe from theft. However, a study by Alhallaq et al. [33] asserted that, in the case of mobile phone loss, m-payment is a potential risk.

The results revealed that the first threat that may impact the use of m-payment applications is Distributed Denial-of-Service (DDoS). Participant 14 defined DDOs as "a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of the Internet." Participant 3 explained how the DDos worked: "DDoS attacks are one of the most potent weapons of hacking on the Internet with regard to mobile payments. When a website is brought down entirely by cyber criminals, it generally means it has become a DDoS attack victim. Hackers do this by flooding or

crashing the website with too much traffic. DDoS has a different type of protocol attack, and it involves sending big data packets through communication protocols". Participant 8 stated, "I think it might affect mobile payments to some extent because as far as I know, these attacks might target the servers that communicate with the mobile payment apps. However, the effect of this type of attack might be more evident in online payments". Participant 2 asserted that "DDoS attacks are considered to be a threat to mobile payment." Similarly, Participant 9 responded that "it is considered as the most famous threat, which is to deny the availability of services. Users cannot use an application or wallet, and service providers cannot provide their services". Participant 6 believed that DDos is a threat that may affect the use of m-payments, explaining, " A DDoS attack on a target server has different goals such as to destroy or damage useful data in the targeted server/network or to plan to collect data from slowed down systems such as login details of such accounts." Participant 15 believed that DDos might have effects on m-payment, such as customers no longer using the application, "It could restrict the availability of the service and might lead to customers leaving the application; hence, reputation damage occurs."

In this study, participants suggested that Distributed Denial-of-service was one of the security threats that impact usage of m-payment applications. The participants stated that due to DDoS attacks on servers, service providers are unable to provide their services and customers are unable to utilize the m-payment applications. Useful data is damaged, login systems slow down, and customers leave. A previous study conducted by Rivers et al. [25] supports the argument that the services of online wallets used by m-payment providers can be attacked by threat actors using DDoS to interrupt m-payment services. Attacks by DDoS affect the transactions that need real-time access (login) through m-payment applications to payment services that are hosted in the cloud. This study also found that DDoS causes disruption to the server with o flood of Internet. A previous study conducted by Rivers et al. [25] supports these findings, asserting that DDoS attackers devastate mobile money servers with fake traffic that blocks requests of customers in real time and makes services unavailable to customers by flooding the servers.

Another threat that may impact the use of m-payment applications is phishing. Participant1 claimed that "Phishing attacks are a threat to mobile payments. Phishing attacks prey on less tech-savvy individuals by tricking them into handing out sensitive information, which can include data such as passwords required to make mobile payments". Participant11 asserted that "It is a critical security threat. It aims to steal users' credentials and, thus, result in applying for unwanted payments". Participant 6 explained this threat: "Phishing attacks can be from many sources such as e-mails, messages and especially from many social networks. Unknown attacks may come at any time from any device or network, and the primary target is to steal important data". In this regard, Participant 4 considered phishing attacks to be a threat to using m-payments, "Phishing attacks on mobile devices are widely known as Smishing. These attacks are initiated using a message that is disguised as a message of concern from a bank representative that prompts the user to click a compromised link intended to get the consumer's data from the respective mobile payment applications. For that reason, phishing is still a threat to mobile payment users and can potentially cause great damage to their account balance." Participant 14 confirmed that phishing attacks are a threat to using m-payment, "The phishing attacks are the most common security threat for mobile payment solutions. In phishing, attackers send an e-mail or SMS that lures people to hand over personal information".

The study found that phishing attacks were another security threat regarding the usage of mobile payment applications. The participants stated that phishing attackers trick the customers into giving sensitive information such as passwords that can be required when making mobile payments and that this results in unwanted payments. Phishing can be conducted through various means, for instance, e-mail, text messages, and social media networks. Rivers et al. [25] asserted that mobile devices are being used for both personal and business purposes, particularly in mobile payment services. Mobile devices are collecting an increasing amount of customer data, which could aid in executing sophisticated attacks. These assaults use phishing e-mails and social engineering to target users, utilizing various communication methods such as e-mail, phone, SMS, and publicly available data about users such as social media. This study further reveals that a phishing attack on a cell phone is termed SMiShing, that is, by sending an SMS that causes damage to the account balances of customers. SMS Phishing or SMiShing is a social engineering threat that induces users to take actions based on the target, such as clicking a link or acting in a specific way. SMiShing attacks take advantage of people's trust in their phones because they appear genuine. Users are generally unprepared for a danger delivered by SMS, making SMiShing assaults simple to exploit [34].

Another threat that may impact on using m-payment applications is Malware (Malicious Software). Participant 13 claimed, "Many threats can hit mobiles like Worms, Trojans, Spyware, Ransomware, Backdoor, etc. Malware can affect the use of an m-payment system, for example, faking an application." Similarly, Participant 2 asserted, "Malware is considered a security threat to using mobile payment services since it is harmful software after all. Attackers use malware attacks to compromise the security of a mobile device and control it remotely. Different malware has different functions which threaten the availability and security of mobile payment services." Participant 5 explained this threat and provided more detail: "Malware uses a designed file or code to damage data of a personal computer, network or another device. It can destroy data, resources, slow down the process of a computer or mobile phone which supports them." Participant 1 confirmed, "Malicious software, or malware, is a security threat to mobile payments. It is a threat because of what it can do once on a computer or other portable devices". Participant 16 commented, "There are many malware apps or websites that try to target people and steal their money. Using mobile payment with such apps or websites is an example of these threats". Participant 7 believed that "Malwares, all of them, whether they are viruses, Trojans, worms etc., can affect mobile payment. They can attack the privacy of the transactions, or hackers can use them to run and use mobiles

remotely. They harm the trust in the mobile payment systems." Spyware, among other types of malware, was emphasized by several participants to be a frequent threat that may impact the use of m-payment applications. Participant 13 defined spyware as follows, "Mobile spyware is software that can be installed on a mobile phone that will allow someone else to monitor activities on the phone remotely so it can control any application like payment applications." Participant 7 claimed that spyware could threaten payment systems from individual hackers or companies.

Some spyware was not only used to steal credentials, but they also are harmful and collect information for advertisements and commercial use, which is also considered an attack on privacy." Participant 4 asserted that spyware is yet another threat that has been increasing on mobile devices as it was on computer devices. This attack involves the installation of spyware in the mobile device of the user without the user's consent and allows the hacker to spy on the user's activities. In most cases, the spyware can even be installed by the most trusted people, normally close relatives, friends, and colleagues. However, a comprehensive anti-virus program can screen any spyware within a mobile system." Participant 11 explained its harm: "It can breach user privacy and access his/her credential data and also may cause harm to the mobile device."

This study found that Malware is also a security threat to mobile payment. Participants stated that Malware such as Trojans, Backdoor, and Worms seriously affect the m-payment system. This study further revealed that the threat of spyware installation is one of the most common types of malware. Installing the spyware in a user's cell phone without the user's consent allows the hacker to spy on the user's activities. Contrary to the findings of this study, a previous study by Wazid et al. [8] found that the Malware world is subjected to Trojans rather than by Worms/Viruses because Trojans do not need any vector of propagation, and they rely on user interest in downloading and installing them. This study found that spyware is used to steal credentials such as passwords and pin codes. Supporting this argument, Wazid et al. [8] asserted that malware such as PbStealer steals data from a user's phone. Such malware is then used to steal sensitive data from the mobile phone, such as users' PIN codes.

This study found that a compressive anti-virus program can screen out any spyware within a mobile system to avoid threats like Malware. Supporting this argument, a previous study by Wazid et al. [8] asserted that various companies such as Kaspersky and F-secure have recognized the significance of combating malware in mobile phones. These companies have released various anti-virus programs that provide complete protection from various types of mobile malware. Moreover, these companies also provide disinfecting tools for viruses, such as Skulls, Cabir, etc. Installing such anti-virus software on mobile devices is prudent to protect users from any malware-related threats. Contrary to this argument, a previous study by Singh and Kalra [35] asserted that losing a mobile device is a common security threat for the application of the mobile device and security experts agreed that most of the mobile threats come from customers losing their mobile devices rather than malware or any security breach.

IV. Conclusion

This study explored the threats that may impact the use of mobile payment in Saudi Arabia. The analysis of interviews revealed that using mobile payment is secure and safe. The results also showed three main threats to using mobile payment in Saudi Arabia: Distributed Denial-of-Service (DDoS), phishing attacks, and malware (Malicious software). Participants also offered some recommendations regarding safety and protecting sensitive data from these threats. This study makes two contributions. The first is to theory by filling the gap in the literature because it is the first study to explore the threats to using m-payment in Saudi Arabia. Secondly, this study contributes to practice by providing a clear picture for service providers and users about threats they may face when using m-payment and, thereby, being more likely to use m-payment safely.

References

[1] M. Almasri and H. Alshareef, "Mobile cloud-based e-payment systems in Saudi Arabia: A case study," in *ACM International Conference Proceeding Series*, 2019, pp. 5–10, doi: 10.1145/3361785.3361795.

[2] R. Alabdan and M. M. Sulphey, "Understanding proximity mobile payment acceptance among Saudi individuals: An exploratory study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, pp. 264–270, 2020, doi: 10.14569/ijacsa.2020.0110436.

[3] R. Alotaibi, L. Houghton, and K. Sandhu, "Exploring the Potential Factors Influencing the Adoption of M-Government Services in Saudi Arabia: A Qualitative Analysis," *Int. J. Bus. Manag.*, vol. 11, no. 8, p. 56, 2016, doi: 10.5539/ijbm.v11n8p56.

[4] S. H. Liao and L. L. Yang, "Mobile payment and online to offline retail business models," *J. Retail. Consum. Serv.*, vol. 57, p. 102230, 2020, doi: 10.1016/j.jretconser.2020.102230.

[5] A. Pal, T. Herath, R. De', and H. R. Rao, "Contextual facilitators and barriers influencing the continued use of mobile payment services in a developing country: insights from adopters in India," *Inf. Technol. Dev.*, vol. 26, no. 2, pp. 394–420, 2020, doi: 10.1080/02681102.2019.1701969.

[6] S. F. Verkijika, "An affective response model for understanding the acceptance of mobile payment systems," *Electron. Commer. Res. Appl.*, vol. 39, p. 100905, 2020, doi: 10.1016/j.elerap.2019.100905.

[7] N. Sundaram, C. Thomas, and L. Agilandeeswari, "A review: Customers online security on usage of banking technologies in smartphones and computers," *Pertanika J. Sci. Technol.*, vol. 27, no. 1, pp. 1–31, 2019.

[8] M. Wazid, S. Zeadally, and A. K. Das, "Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 56–60, 2019, doi: 10.1109/MCE.2018.2881291.

[9] I. Ahmad, S. Iqbal, S. Jamil, and M. Kamran, "A Systematic Literature Review of E-Banking Frauds : Current Scenario and Security Techniques," *Linguist. Antverp. 2021 Issue-2*, vol. 2, no. June, pp. 3509 – 3517, 2021.

[10] G. Bogdanova, T. Todorov, and G. Georgieva-Tsaneva, "Software approaches and methods to ensure the security of interactive systems," *Cybern. Inf. Technol.*, vol. 18, no. 5, pp. 12–20, 2018, doi: 10.2478/cait-2018-0017.

[11] G. Bogdanova, T. Todorov, and N. Noev, "Protection of semantic organized data. Encryption of RDF graph," *Digit. Present. Preserv. Cult. Sci. Herit.*, vol. 4, pp. 183–188, 2017.

[12] S. Yin, J. Sheng, T. Wang, and H. Xu, "Analysis on mobile payment security and its defense strategy," in *Advances in Intelligent Systems and Computing*, 2019, vol. 773, pp. 941–946, doi: 10.1007/978-3-319-93554-6_95.

[13] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. Al-Khaleefa, "A review on electronic payments security," *Symmetry (Basel).*, vol. 12, no. 8, pp. 1–24, 2020, doi: 10.3390/sym12081344.

[14] M. Bosamia, "Mobile wallet payments recent potential threats and vulnerabilities with its possible security measures." in *International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017)*, Charusat, Changa, India, 2017.

[15] Y. Jin, S. Wang, Y. Qu, Q. Guo, and J. Li, "Study on Security of Mobile Payment," in *Advances in Intelligent Systems and Computing*, 2018, vol. 690, pp. 123–127, doi: 10.1007/978-3-319-65978-7_19.

[16] A. Almaarif and M. Lubis, "Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 5, pp. 1874–1880, 2020, doi: 10.18517/ijaseit.10.5.8862.

[17] M. Najib and F. Fahma, "Investigating the adoption of digital payment system through an extended technology acceptance model: An insight from the Indonesian small and medium enterprises," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 4, pp. 1702–1708, 2020, doi: 10.18517/ijaseit.10.4.11616.

[18] R. Brunt, P. Pandey, and D. McCoy, "Booted: An Analysis of a Payment Intervention on a DDoS-for-Hire Service," in *Workshop on Economics of Information Security (WEIS)*, University of California San Diego,USA, 2017.

[19] M. Zhang *et al.*, "Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches," 2020, doi: 10.14722/ndss.2020.24007.

[20] J. Kaur Chahal, A. Bhandari, and S. Behal, "Distributed Denial of Service Attacks: A Threat or Challenge," *New Rev. Inf. Netw.*, vol. 24, no. 1, pp. 31–103, 2019, doi: 10.1080/13614576.2019.1611468.

[21] A. P. Fajar and T. W. Purboyo, "A Survey Paper of Distributed Denial-of-Service Attack in Software Defined Networking (SDN)," *Int. J. Appl. Eng. Res. ISSN*, vol. 13, no. 1, pp. 973–4562, 2018.

[22] B. Amro, "Phishing Techniques in Mobile Devices," *J. Comput. Commun.*, vol. 06, no. 02, pp. 27–35, 2018, doi: 10.4236/jcc.2018.62003.

[23] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Comput. Secur.*, vol. 73, pp. 519–544, 2018, doi: 10.1016/j.cose.2017.12.006.

[24] P. Datta, S. Tanwar, S. N. Panda, and A. Rana, "Security and Issues of M-Banking: A Technical Report," in *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, Jun. 2020, pp. 1115–1118, doi: 10.1109/ICRITO48877.2020.9198032.

[25] O. Rivers, Y. H. Hu, and M. Hoppa, "A Study on Cyber Attacks and Vulnerabilities in Mobile Payment Applications," in *Journal of The Colloquium for Information …*, 2020, vol. 7, no. 1, p. 9.

[26] O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[27] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware Threats and Detection for Industrial Mobile-IoT Networks," *IEEE Access*, vol. 6, pp. 15941–15957, 2018, doi: 10.1109/ACCESS.2018.2815660.

[28] P. Brey, S. Gauttier, and P.-E. Milam, *Harmful Internet use Part II: Impact on culture and society Study*, no. January. 2019.

[29] L. E. Tomaszewski, J. Zarestky, and E. Gonzalez, "Planning Qualitative Research: Design and Decision Making for New Researchers," *Int. J. Qual. Methods*, vol. 19, p. 160940692096717, Jan. 2020, doi: 10.1177/1609406920967174.

[30] D. Mortelmans, "Analyzing Qualitative Data Using NVivo," in *The Palgrave Handbook of Methods for Media Policy Research*, Springer, 2019, pp. 435–450.

[31] M. Mason, "Sample size and saturation in PhD studies using qualitative interviews," in *Forum Qualitative Sozialforschung*, 2010, vol. 11, no. 3, doi: 10.17169/fqs-11.3.1428.

[32] S. Wycech, "An Investigation of Attitudes towards Mobile Payments.," in *in Management of Information Systems*, no. September, Dublin , Ireland: University of Dublin, 2015.

[33] H. Alhallaq, M. Younas, S. Kamal, and B. Champion, "Understanding Perceived Value of Mobile Payments: A Qualitative Study," 2019.

[34] E. U. Soykan and M. Bagriyanik, "The effect of SMiShing attack on security of demand response programs," *Energies*, vol. 13, no. 17, p. 4542, 2020, doi: 10.3390/en13174542.

[35] A. Singh and M. A. Kalra, "Impact of Mobile Wallets Security on Consumer Attitude towards Use," *Psychol. Educ. J.*, vol. 58, no. 4, pp. 3140–3146, 2021.