Bachelor's thesis

Information and Communications Technology

2024

Xingyu Chen

Network Security Risks Caused by Third-Party Payment

– A Case Study of Apple Pay

Bachelor's Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2024 | 36

Xingyu Chen

Network Security Risks Caused by Third-Party Payment A Case Study of Apple Pay

The rapid growth in the adoption of third-party payment systems such as Apple Pay necessitates a thorough investigation of the security risks they present to users and how they impact user acceptance of the technology. This study used the qualitative case study methodology, employing document and thematic analysis of secondary sources, to explore the security landscape of Apple Pay through the lens of the Technology Adoption Model (TAM). The study addressed key questions regarding network security risks, vulnerabilities in the security architecture, causes of recent security breaches, and strategies to enhance transaction security. Key findings revealed that phishing, man-in-the-middle attacks, and data breaches are significant risks impacting user trust and acceptance. Vulnerabilities were identified in the tokenization process, biometric authentication methods, and third-party integrations. Recent security incidents were largely attributed to human error, software vulnerabilities, and insider threats. Effective strategies for enhancing security include the implementation of Multi-Factor Authentication (MFA), continuous monitoring with AI and machine learning, and comprehensive user education and awareness campaigns. Insights drawn from this study may be helpful in the development of secure and user-friendly third-party payment systems.

Keywords: *third-party payment systems, Apple Pay, security risks, TAM, vulnerabilities*

Contents

Figures

List of Abbreviations

BCBA	Block-wise Chosen Boundary Attacks
BEAST	Browser Exploit Against SSL/TLS
BREACH	Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext
CBC	Cipher Block Chaining
CRIME	Compression Ratio Info-lead Made Easy
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPS	Intrusion Prevention Systems
MFA	Multi-Factor Authentication
NVD	National Vulnerability Database
OTP	One-Time Passcode
POODLE	Padding Oracle on Downgraded Legacy Encryption
SSL	Secure Socket Layer
TAM	Technology Acceptance Model
TLS	Transport Layer Security

1 Introduction

In recent years, rapid technological advancements and changing consumer behaviours have brought about a profound transformation in the finance sector. The proliferation of digital payment systems has revolutionized ways of carrying out financial transactions, marking a departure from traditional financial methods that rely heavily on physical currencies and conventional banking systems (Shi et al., 2021). Mobile phone technologies and the widespread availability of the internet have led to the seamless integration of digital solutions into people's everyday lives. Currently, consumers rely heavily on their smartphones and other mobile devices to make financial transactions and also manage their finances on the go.

A growing trend in this paradigm shift is the emergence of third-party payment platforms such as Apple Pay, Ali Pay, Google Pay, Samsung Pay, and PayPal among others, which have emerged as critical players in the digital payment ecosystem. Figure 1 below presents a summary of third-party payment apps based on their number of worldwide user. Apple Pay is a prominent example of a third-party payment platform, offering its users a convenient and secure way of carrying out contactless transactions using Apple devices (Guo & Bouwman, 2016). The growing adoption of Apple Pay and other related third-party platforms has been prompted by a combination of factors including the growing preference for convenience among users, the growth of e-commerce, and rising concern about the security of traditional approaches for conducting financial transactions (Solat, 2017).

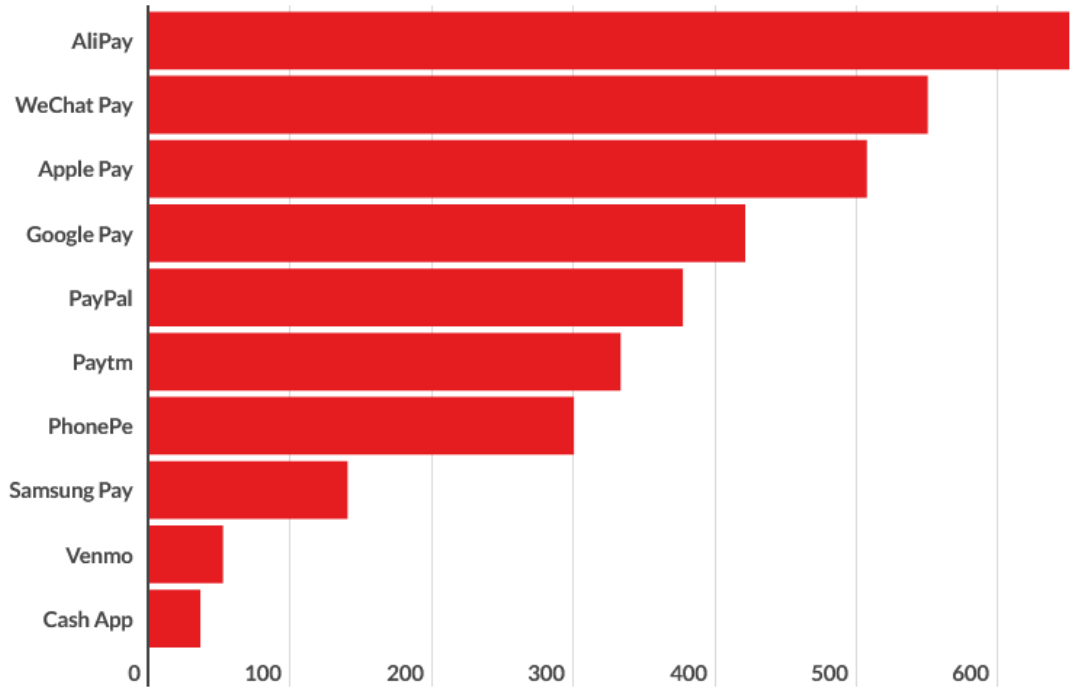

Figure 1: Third-Party Payment Systems Users (2024) (Source: Curry, 2024)

1.1 Overview of Apple Pay

Apple launched its payment service, Apple Pay in September 2014. As of 2024, the platform has over 60.2 million users living in the United States and the figures are projected to grow to over 75 million by 2030. Globally, Apple Pay users stand at 638 million as of 2024 but are expected to grow to 705 million by 2027. Figures 1 and 2 below summarise these statistics.

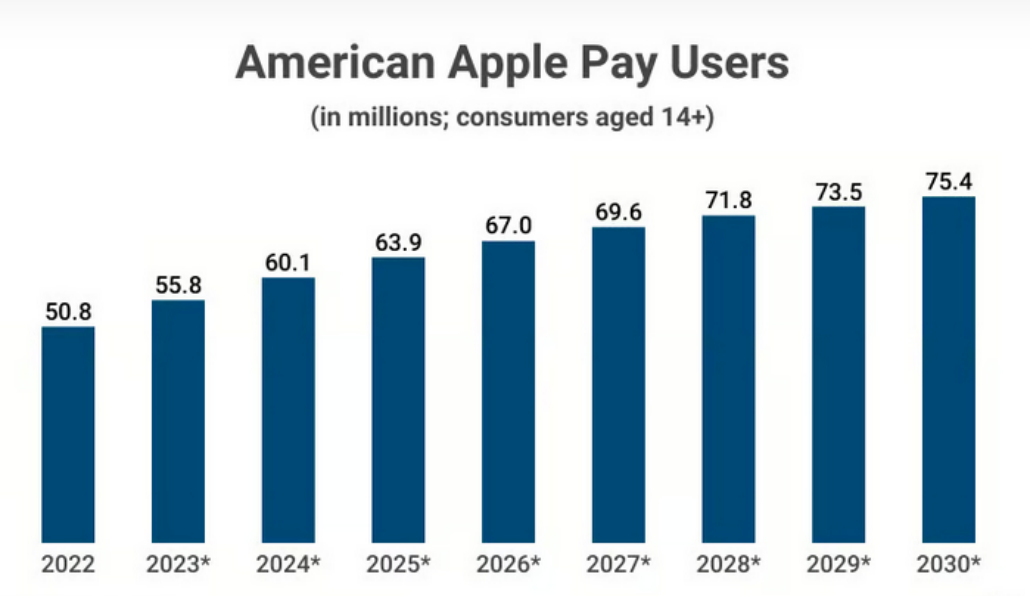

Figure 2: Apple Pay users in the US (2022-2023) (Source: Capital One Shopping, 2024).

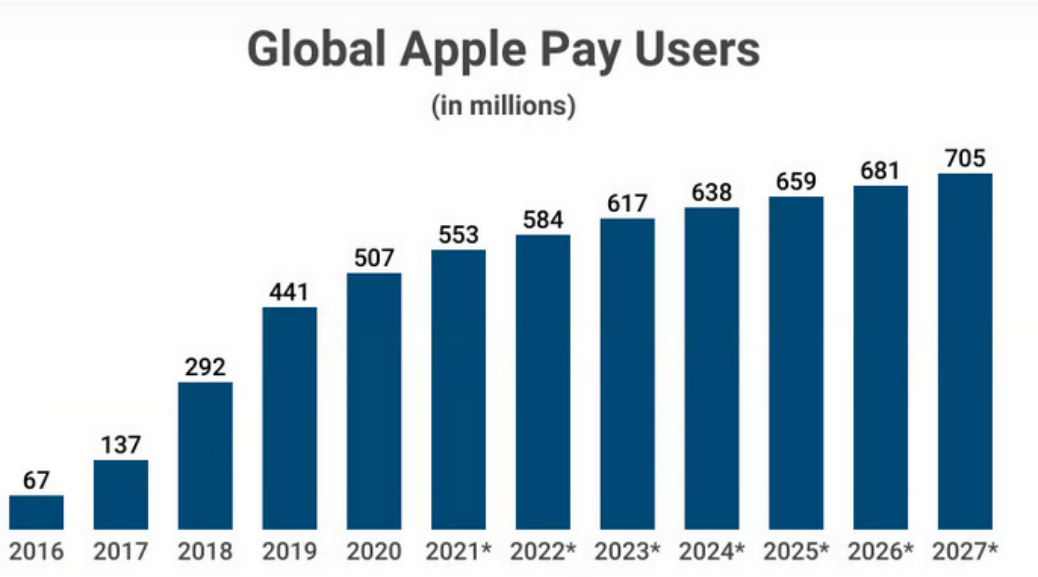

Figure 3: Apple Pay global users (2016-2027) (Source: Capital One Shopping, 2024).

Based on these statistics, Apple Pay users, both in the US and globally have grown significantly despite the platform facing growing competition from other

third-party payment platforms such as Google Pay, Alipay, Paypal, and Stripe among others (Capital One Shopping, 2024).

Apple Pay uses interoperable Near-Field-Communication (NFC), allowing iPhone and iPad (iOS) and Apple Watch (Watch OS) users to conduct biometric (pulse and fingerprint) as well as contactless payments within mobile apps and at brick-and-mortar stores (Agarwal et al., 2020). As such, merchants operating in physical stores should have complementary NFC payment terminals for them to accept Apple Pay. In mediating these transactions, Apple has formed partnerships with credit card networks, including MasterCard, Visa and American Express as well as multiple other banking institutions to process and settle payments between client cardholders and merchants (Boison & Tsao, 2019). Apple Pay acts as a third-party proxy or mediator between the bank accounts of the card holders and those of the merchants where it supports and enforces the existing roles as well as business models of the financial institutions within the existing payment ecosystem. During its initial launch, Apple Pay preserved the exclusive right to gain access to the NFC chip using its secure element, which stores sensitive payment information such as payment tokens (controlled by the credit card issuers) and cryptogram (operated by banking institutions) (Solat, 2017).

In further enhancing its service, Apple provides Apple Pay APIs for free to third-party developers, allowing them to give Apple Pay functionalities as part of their mobile applications following a screening and review process (Solat, 2017). For developers who do not have their payment processors, Apple can partner with other online payment solution providers such as Stripe and Braintree among others in facilitating the acceptance of biometric-based Apple Pay payments. Such collaborations allow these payment processors to provide third-party developers with an uncomplicated integration process for the acceptance of biometric-based Apple payments. The processors end up charging regular fees for transactions. Apple Pay also has the technical capabilities to come up with rich contextual and valuable payment data although it is not the goal of Apple to utilize such data (Kazan, 2015). Instead, Apple offers the necessary support for

business activities where financial partners may capture valuable payment data. As a result of security concerns and the need for the enhancement of services, Apple Pay collects device location information, date, and time. Apple Pay's business model follows a two-pronged approach: the use of Apple Pay is free for end-users and third-party developers, which is the subsidy side. Also, merchants are not charged for accepting Apple Pay since they still pay regular fees to the payment processors (Kazan, 2015). Apple also charges 0.15% of transaction amounts to banking institutions (money side) through the help of credit card networks (Arnold & Jeffery, 2016). Given the collaborations and the innovative business model adopted by Apple Pay, it is necessary to explore the different security concerns that the platform presents as a prerequisite for understanding the adoption of third-party payment systems, which is a growing trend in modern days.

1.2 Significance of the Study

Despite the numerous efficiency and convenience benefits associated with third-party digital platforms such as Apple Pay, their widespread adoption has led to the identification of novel and more sophisticated challenges and security risks, especially related to network security (Lin et al., 2020; Shi et al., 2021). The interconnected nature of these platforms, coupled with the growing threat of more sophisticated cyber threats, has made third-party payment platforms such as Apple Pay an attractive target for malicious actors intending to exploit their vulnerabilities to benefit financially. Notable incidents highlighting the vulnerabilities of third-party payment systems have been recorded in the extant literature (William et al., 2020; Yang et al., 2019). The nature and complexities reflected in these instances underscore the urgency and importance of addressing the network security risks presented by third-party payment platforms. However, existing studies have only offered a shallow exploration of the vulnerabilities of Apple Pay. For instance, the study by Yang et al. (2019) provides a generic overview of the security issues impacting third-party in-app payment systems. While such an analysis of the security issues presented by these platforms offers the necessary background information for understanding the

unique security risks presented by third-party payment systems, it does not reflect the unique security concerns related to the architectural innovations and collaborative business models adopted by Apple Pay. Williams et al (2020) also offer a review of the security risks presented by the Apple Pay platform but focus essentially on theories such as those developed by Pindrop researcher, David Dewey, to explore potential avenues that hackers may adopt in breaching the system's security mechanisms. While such an approach is insightful in understanding the nature of the risks that third-party payment faces, it does not reflect real-life risk experiences that the Apple Pay platform has suffered since its inception and how this has impacted the adoption of the payment system. Hence, there is a need for an in-depth investigation of the underlying mechanisms of the platform, analysing recent security instances, and identifying potential vulnerabilities to gain more insight and enhance the capacity to mitigate risks, safeguard user data, and ensure the integrity of the platform.

1.3 Research Aims and Objectives

This thesis aims to investigate and analyse the network security risks inherent in third-party payment systems, focusing essentially on Apple Pay, and understand how these threats impact the acceptance and adoption of the technology.

The study will seek to achieve the following objectives:

i. To investigate the key network security risks associated with third-party payment platforms such as Apple Pay and how they impact the acceptance of the technology;

ii. To explore the security architecture of Apple Pay to identify potential vulnerabilities;

iii. To analyse recent network security incidents to gain a deep insight into the security challenges and their underlying causes;

iv. To propose strategies and recommendations for enhanced security for the Apple Pay platform.

1.4 Research Questions

By employing the qualitative case study approach, the study will answer the following research questions:

RQ1: What are the key network security risks associated with third-party payment systems such as Apple Pay and how do they impact the acceptance of these systems?

RQ2: What are the vulnerabilities in the security architecture of Apple Pay?

RQ3: What are the underlying causes of the recent security incidents or breaches associated with Apple Pay?

RQ4: What strategies can be implemented to enhance the security of Apple Pay transactions?

Thesis Overview

This thesis is organised into five chapters. The introduction chapter offers background information on third-party payment systems specifically Apple Pay. It also presents the research problem and the significance of the study, the research objectives and the research questions. The literature review chapter explores existing, relevant literature related to the security risks presented by third-party payment systems. The chapter also identifies the research and knowledge gap that the current study seeks to fill. The methodology chapter describes aspects of the research methodology, data collection and analysis as well as the ethical concerns presented by the current study. The findings and discussion chapter presents the findings of the case study and the analysis of these findings based on insights from existing literature and theory. The conclusion chapter presents a summary of the key findings, discusses the implications of the study and also explores potential avenues for future research.

2 Literature Review

Researchers and practitioners alike have expressed significant interest in exploring the security risks and challenges presented by mobile payment systems. As a result of their wide acceptance and adoption in recent days, third-party systems have emerged as some of the studied payment systems, with particular focus being on the security and privacy risks they present to users and the acceptance of these technologies. Several relevant themes exist in the extant literature depicting important areas of focus that are relevant for the exploration of the security challenges presented by third-party digital payment systems such as Apple Pay.

2.1 Third-Party Mobile Payment Technology Adoption

Increased mobile phone penetration has resulted in the emergence of innovative mobile services, including mobile payment applications that offer a variety of banking and financial services such as payments, microfinance, mobile vouchers, loyalty cards and mobile banking (Iman, 2018). Researchers have employed different theoretical models such as the technology acceptance model (TAM) (Davis, 1989) to show that the adoption of new payment systems is determined by aspects of compatibility, perceived usefulness, interconnection, perceived ease of use, as well as perceived security and user habits. Since these factors tend to differ from one context to the next, the success of a mobile payment solution in one context may not be generalised to depict success in a different context (Masrom, 2007). The adoption of Apple Pay, for instance, has been shown to rely heavily on the EMV secure system, which is the baseline architecture employed in digital and mobile payment systems used in facilitating purchases. The TAM approach offers a viable framework for the assessment of the technology's compatibility with the existing PoS infrastructure as well as with perceived security, perceived usefulness, as well as perceived ease of use (Iman, 2018). A balance has to be established between these dimensions of the TAM model, with perceived security playing a central role.

2.2 Technology Acceptance Model (TAM)

TAM was proposed by Davis (1989) as an extension of the Theory of Reasoned Action (TRA) that had been introduced earlier by Ajzen and Fishbein (1980). TAM was aimed at offering more elaborations on the issue of human conduct as relating to the acceptance of certain technologies. TAM has four dimensions: perceived usefulness, perceived ease of use, attitude towards using, and behavioural intention to use (Davis, 1989).

TAM has over the years received increased acceptance among scholars seeking to explore the dynamics of the acceptance of digital technologies, including mobile payment systems. However, it has been expanded further to cover other important aspects that continue to influence the adoption of novel technologies. According to Hassan and Wood (2020), perceived risk (security) has also been introduced as an important factor to consider when determining the adoption of a given technology. Since this study seeks to explore the impact of security risks, the model of TUM adopted seeks to explore how the perceived risks of third-party payment systems relate to their adoption by focusing on the case of Apple Pay.

A user's perceived risk or security has a correlated impact in either adopting or rejecting a given technology or service (Hassan & Wood, 2020). Perceived risk has become an integral factor in analyses of the adoption of digital technologies (Johnson et al., 2018). In the study by Ozili (2018), it is determined that the need to expand financial inclusion through the adoption of mobile payment systems leads to the underestimation of the risks that are associated with the technology. Therefore, when it comes to analysing the risks associated with mobile payment systems, different types of risks are involved. Physical risk relates to the possibility that a given service may endanger the well-being of the user (Ozili, 2018). Performance risk relates to the possibility that the given technology or the ordered resource may not satisfy the user, which may limit the potential adoption of the technology. According to Johnson et al. (2018), performance risks impact the adoption of mobile payment technologies in the domain of management control. Psychological risks also have a significant impact on the user's sense of security while using a given technology. This means that the technology does not

necessarily have to present a physical risk to the use. According to Khwaja and Zaman (2020), in consumer information adoption research, the integration of mobile payment systems presents some psychological risks that have a significant impact on the adoption of these technologies by consumers. Wang et al. (2019) also establish that perceived risk could be at the aggregate or disaggregate level, whereby the aggregate categories are considered as more risk-averse, and therefore, less likely to adopt mobile technologies at the aggregate compared to the disaggregated levels.

Perceived trust is also closely linked to the risks that determine the adoption of third-party mobile payment systems. According to a study by Duane et al. (2014), trust is deemed as the most powerful factor influencing the willingness of consumers to use their smartphones in making financial transactions. This claim coincides with that of Dastan and Gurler (2016) who considered perceived trust to have a positive impact on the adoption of mobile payment systems such as Apple Pay, Google Pay, and Alipay among others. Gong (2016) also suggested that emotional trust in mobile payment systems is intricately related to perceived risks and consequently determines the willingness to adopt a given technology. Therefore, when considering the security risks associated with third-party mobile payment systems such as Apple Pay and the impact they have on the adoption of the technology, it is necessary to factor in aspects of perceived trust in the technology as demonstrated by the users.

Some authors have also suggested that perceived trust also influences other factors such as perceived usefulness and ease of use, in addition to perceived risk. According to Chen and Li (2016), for instance, perceived trust and perceived usefulness mediate perceptions of risk and together impact the decisions of users as to whether or not they would adopt a given technology. Gao and Waechter (2015) also highlighted the positive correlation that perceived trust has on perceptions of convenience and perceived benefit and how it impacts aspects of the decision to use mobile payment services.

2.3 Security Risks of Mobile Payment Systems

Researchers have also demonstrated significant interest in exploring the risks, challenges, as well as limitations presented by mobile payment systems such as Apple Pay. While some studies such as Williams et al. (2020) have addressed specific payment methods, others have undertaken a more generic approach that considers these risks, challenges and limitations from a general point of view without paying attention to the unique attributes of the different mobile payment systems.

Mobile payment systems such as Apple Pay have numerous advantages when it comes to ease of use as well as security. However, as noted by Chen and Li (2017), these platforms are still not doing enough to prevent stole credit cards, with vulnerabilities such as SSL interception, security gaps in the secure element, and the increased use of jail-broken smartphones being some of the common concerns. When a user adds a card, Apple Pay connects with the user's bank, sending them encrypted credit card information (Williams, 2020). The bank applies its measures to ensure authenticity, which may require making a phone call where the user has to provide additional information for the authentication process to be completed.

According to Williams et al. (2020), Apple Pay fails to implement a "rate limiting" service that protects its system from hackers who attempt to make PIN guesses to gain unauthorised access, which is deemed as brute force attacks. Hence, the existing research has revealed that numerous security risks are unique to third-party platforms, including Apple Pay. Even though, according to Kazan (2015), hackers have been able to attain the skills to hijack the transaction and manipulate the traffic before the server's decryption of the symmetric session key. In recent years, the SSL has, therefore, become vulnerable to the activities of hackers. For instance, according to Williams et al. (2020), an attack towards Apple devices may be carried out through the exploitation of jailbroken devices to inject malware and then intercept and carry manipulations on the SSL transaction traffic of users using payment applications such as Apple Pay (Williams et al., 2020). The hackers may intercept SSL transaction data and

tamper with the transaction data as well as change the amount or currency that is paid using third-party systems such as Apple Pay (Williams et al., 2020).

As noted by Rao and Deebak (2023), potential hackers seek to interfere with the data initially by stealing of payment tokens from an unsuspecting victim's mobile device. Some users are not aware of the involved risks associated with activities such as the use of public Wi-Fi (Williams et al., 2020). As noted by Williams et al. (2020) hackers seeking to steal information may set up a fake Wi-Fi hotspot and ask the users to create user profiles. This strategy allows the hackers to steal data such as the Apple Pay cryptogram, which is the key that encrypts the data (Liu et al., 2020). Given that the delivery information is sent as clear text, hackers may use the intercepted cryptogram to make payments on the same website where the victim has made prior transactions (Liu et al., 2020). Such vulnerabilities may result in additional damages including malware dispersed throughout an entire network where it is likely to spread even further. Williams et al. (2020) argue that to seal these vulnerabilities, users have to disable outdated SSL servers and also continuously upgrade their mobile devices to ensure that they are optimally compliant with up-to-date security measures.

2.4 Research and Knowledge Gaps

The extant literature offers notable and valuable insights related to the influence that perceived security risks have on the adoption of third-party payment technologies by employing theoretical models such as TAM. However, there are no studies that employ the model, with a specific focus on security risks to understand how they impact the dynamics of the adoption of the payment system. Also, while the existing studies explore in significant depth the vulnerabilities of third-party payment systems such as Apple Pay, they fall short when it comes to exploring the details of these risks as they relate to the unique infrastructural innovation and the partnerships facilitated by the Apple Pay system. This study seeks to fill the identified knowledge and research gaps.

3 Research Methodology

3.1 Research Design

This study employs the qualitative case study approach to investigate the network security risks associated with Apple Pay. A case study methodology offers a suitable approach for exploring complex phenomena within real-life settings, which allows for an in-depth examination of specific cases (Johansson, 2007). The focus of the study is essentially on Apple Pay, which is a quintessential example of a third-party payment platform, with an emphasis on understanding its architecture, vulnerabilities, and other broader implications for network security. The qualitative case study approach also allows for the in-depth investigation of a case by considering contextual details that may otherwise not be captured by other methods (Johnson, 2007).

The study adopts interpretivism as the research paradigm. Interpretivism is founded on the view that reality is socially constructed and that there are multiple realities as opposed to a single reality (Kelliher, 2011). The approach offers a useful basis for understanding the security risks related to third-party payment systems by focusing essentially on the perceived risks of these platforms.

3.2 Data Collection Methods

The data for this qualitative case study was collected from existing studies exploring the security risks of Apple Pay, industry reports, security advisories, Apple's documentation of Apple Pay, and other relevant reports. Through conducting desktop research, the data was obtained from these sources and used to make sense of recorded instances of security breaches impacting Apple Pay users. Document analysis was conducted on these sources to provide a comprehensive understanding of Apple Pay's security mechanisms (Bowen, 2009). The process of document analysis involves reviewing and evaluating documents, both printed and electronic in a methodical way (Bowen, 2009). As is the case with other methods of analysis, the process of document analysis

involves the examination and interpretation of data with the view of revealing meaning, gaining an understanding and coming to a given conclusion (Bowen, 2009). According to Bowen (2009), researchers tend to review prior literature as part of a document analysis to help with the identification of pertinent themes that allow for making sense of the information obtained from the sources. Document analysis produces data in the form of excerpts, quotations or even entire passages that may further be analysed using another data analysis approach such as thematic analysis. The latter approach was used to analyse the data in this study and identify important themes that offer direct responses to the primary research questions. As a research approach, document analysis is used in qualitative studies to produce rich descriptions of phenomena (Bowen, 2009).

3.3 Data Analysis

The collected data was analysed using thematic analysis as described by Braun and Clarke (2006). The process follows six steps, including data familiarization, initial code generation, theme identification, theme review, theme description, and report writing (Braun & Clarke, 2006). The familiarization stage involved examining the research data to become familiar with it. At this point, the activities include deciding on the codes to employ and which codes represent the data (Braun & Clarke, 2006). Initial code identification is the actual identification of the words or phrases that constitute the codes (Braun & Clarke, 2006). The other steps involve the identification of the relevant themes by combining different codes, reviewing and describing or summarizing these themes and creating the research report based on the identified themes. Thematic analysis offers a flexible and systematic approach to the exploration and interpretation of thematic data, generating a wealth of insights into the case under investigation (Braun & Clarke, 2006). The findings and analysis of these findings are presented in the results and discussion chapter, which is the next one.

3.4 Ethical Considerations

This study mainly involves the handling of secondary sources, which means that the most significant ethical consideration is to attribute sources to their original authors accordingly. APA style was used to appropriately reference the sources of information and to ensure academic integrity. All the secondary documents that were consulted in the process were also acknowledged using the APA referencing approach.

4 Results and Discussion

This chapter presents and discusses the findings of the Apple Pay case study. The findings of the study are organised based on the identified themes which correspond to the primary research questions presented in the introduction. The identified themes are security risks and their impact on technology acceptance, vulnerabilities in the Apple Pay security architecture, causes of recent security risks or breaches, and strategies for enhancing the security of Apple Pay transactions.

4.1 Key Network Security Risks and Their Impact on Apple Pay's Acceptance

The analysis of the identified documents established that in the case of Apple Pay, the main security risks that users of the system encounter include phishing attacks, man-in-the-middle (MitM) attacks and data breaches. Phishing attacks include risks whereby Apple Pay users encounter malicious actors who attempt to steal their information through deceptive communication methods such as emails (Nahapetyan et al., 2024). These attacks, whether they are successful or not, may impact the perceptions about the security and trust of the system, which may have a devastating impact on the acceptance of these systems. MitM attacks involve scenarios whereby user data is intercepted by malicious actors when the users connect to unsecured or compromised networks (Williams et al., 2020).

Among the most common incidents linked to SSL vulnerabilities include POODLE (CVE-2014-3566), BEAST (CVE-2011-3389), CRIME (CVE-2012-4928) and BREACH (CVE-2013-3587) among others (Williams et al., 2020). As noted by the National Vulnerability Database (NVD), the Padding Oracle on Downgraded Legacy Encryption (POODLE) was established in October 2014 and utilises two important vulnerabilities. The first one is that Apple users still use SSL 3.0 to attain operability and compatibility with earlier systems. In such a case, the potential victims tend to interact with the mechanisms of attack, which results in their disclosure of sensitive information that may be used by hackers to gain unauthorised access to their devices. A second vulnerability is associated with

Block Padding in SSL 3.0. POODLE employs non-deterministic Cipher Blocking Chaining (CBC) padding, making it possible for the conduct of man-in-the-middle attacks aimed at gaining access to clear-text data through a padding-oracle attack.

Kelly and Palaniappan (2023) establish that if a user initiates a handshake and sends a list of all the SSL versions that can be supported, the hacker may intercept the traffic and carry out a man-in-the-middle attack. The hacker may impersonate the server until the client opts for a downgraded version of the SSL, which is more vulnerable. Once the connection between the user and the server is established on the vulnerable version, the hacker can then attempt a POODLE attack. Additionally, such vulnerability can also be found in the CBC mode (Williams et al., 2020). Given that block cyphers have a limited length, padding can be used to fill the extra space. What this means is that the padding value may be ignored by the server which may fail to confirm the accuracy of the padding length through message authentication code (MAC) of the sent plaintext. As such, the sender of the information may not be able to decipher the plaintext value of the encryption block through the modification of the padding length and then considering the corresponding server's response.

The time when the systems are patched, there is a need for mitigation steps to be undertaken when initiating an action plan (Williams et al., 2020). Patching against POODLE and keeping it from affecting users, all involved stakeholders such as consumers and merchants must implement intrusion prevention systems (IPS) as a way of integrating the necessary network traffic measures through processes such as network scanning (Williams et al., 2020).

BEAST (Browser Exist Against SSL/TSL) attacks impact SSL 3.0 and TLS 1.0 (Williams et al., 2019). In this type of attack, the hackers decrypt data exchanged between two or more parties by taking advantage of the vulnerability in the CBC mode implementation in TLS1.0 (Kelly & Palaniappan, 2023). This tool makes it possible for hackers to intrude or gain access to a secured system. As reported by the NVD, the SSL protocol is the one that encrypts the data that makes man-in-the-middle attacks possible and allows the acquisition of plaintext hypertext

transfer protocol (HTTP) headers through the use of Block-wise Chosen Boundary Attacks (BCBA) on HTTP or HTTPS sessions. The man-in-the-middle attacks allow hackers to attach packets to the SSL traffic. In this sense, the hacker may guess the initialisation vector that the user uses in XORing with messages and make comparisons with the results of the blocks that the hacker intends to decrypt (Williams et al., 2020).

Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) works in the same way as CRIME, only that it specifically targets HTTP compression, especially where TLS compression is not a requirement for an attack to be executed (Kelly & Palaniappan, 2023). The hacker forces the user's browser to make a connection to the TLS that is enabled by a third-party network and uses it to monitor traffic between Apple Pay consumer and the server by carrying out a man-in-the-middle attack. Together, several factors depict a vulnerable web application: 1) a server from a server that uses HTTP-level compression; 2) reflecting a user-input HTTP response body; and 3) reflecting a secret with HTTP response bodies (Kelly & Palaniappan, 2023).

Another form of vulnerability that characterises third-party payment platforms such as Apple Pay is the Heartbleed, which is an attack that works by compromising the TLS Heartbleed extension. The Heartbleed is located in the Heartbleed extension of the cryptography library OpenSSL (Williams et al., 2020). It is used as the intervening method between two parties to ensure that the closure of a connection does not occur. A payment system user, such as the Apple Pay user, may send a request to the merchant with a payload containing the data-size of data. The merchant then has to respond to the request with the same request that contains data and size that is the same as the one contained in the request by the user.

However, if a user sends false data length, the merchant may respond with the same data, which includes random data from the system's memory to meet the length requirements of the initial request (Williams et al., 2020). According to Williams et al. (2020), there have been instances whereby the private key belonging to the merchant is leaked through the Heartbeat vulnerability, meaning

that the hacker can decrypt all server traffic (Williams et al., 2020). Such a fault also makes it possible for an attack to be carried out remotely whereby the hacker can attack and retrieve the private memory of an application that relies on the affected OpenSSL library (Kwaja & Zaman, 2020).

Heartbleed attacks can be potentially avoided by ensuring that the iOS and SSL are constantly updated (Pour et al., 2023). Merchants can also implement TLS as a way of keeping data secure over a network. There are certain scenarios whereby servers that are badly configured expose Apple Pay users to risks that include the likelihood of having their information accessed by unauthorised individuals who may use such information to launch attacks. As such OpenSSL 1.0.1 has been adopted to allow for the patching of the damages, vulnerabilities as well and leaks that may result in attacks.

Most of the vulnerabilities discussed above were addressed in 2015 following the release of iOS 8.4 (Williams et al., 2020). These also include Masque attacks carried out on the Apple Pay platform. The two common Masque attacks are Manifest and Extension Masque Attacks. These attacks have the potential to demolish apps and other Apple resources, including Apple Pay and others bypass the iOS security measures and also allow for the hijacking of Virtual Private Network (VPN) traffic.

In the early years of Apple Pay, a third of Apple devices had not upgraded to the iOS version 8.1.3 or above (Williams et al., 2020). As such, five months into the release of the mobile payment platform, Ozili (2018) argues that these devices were vulnerable to Masque attacks. However, such vulnerabilities have since been adequately addressed. Other important risks that are faced by third-party mobile payment systems include distributed denial of service attacks (DDOS) (Nicholson et al., 2023). These attacks impact the availability of the resources of a network, which prevents users from accessing these assets, denying the use of important resources by the authorised users (Nicholson et al., 2023).

Additionally, DDOS attacks may also cause delays in time-critical operations that may make it impossible for a user or a merchant to effectively respond to request.

Such delays may be deliberately created and exploited through system exhaustion, which includes exhausting the available bandwidth, disk space and even memory. As noted by Williams et al. (2020), three threat types may result in the flooding of these services. These include the consumption of system resources, the malicious wasting of communication links through the repeated downloading of large files from the server and the use of structured query language (SQL) injections. Botnets, viruses or DoS tools may be used to disrupt the normal functioning of a network. According to Williams et al. (2020), hackers tend to send huge volumes of bogus requests to servers as a way of deliberately consuming the processing power from the user to the merchant, flooding the network bandwidth.

Third-party payment systems are also susceptible to connectionless volumetric attacks in which the attacks do not require a session for them to be created through the sending of data packets to users. Volumetric attacks are viewed as floods whereby they congest a system by sending large volumes of traffic on a network, which ends up overwhelming the bandwidth. According to Kelly (2023) such attacks remain common as they are mostly employed by individuals seeking to exact revenge.

As per the TAM framework, network security risks directly influence perceptions of ease of use and usefulness, which determines whether or not individuals are likely to embrace a given technology. If Apple Pay users perceive the system as insecure due to the potential for phishing, MitM attacks and data breaches, they may be unwilling to accept the technology. However, since Apple has invested intensively in enhancing the security features of its Apple Pay's architecture, these concerns are not as pronounced as they were in the early years of the technology's inception. This may explain the growing adoption of Apple Pay by users in different regions.

4.2 Vulnerabilities in the Security of Apple Pay

This case study reveals that the vulnerabilities in the security architecture of Apple Pay are realised in the tokenisation process, authentication mechanisms, and

collaboration with third-party services, which expand the points of attack. While tokenisation offers a strong security measure, flaws in its implementation or breaches in the token vault may result in vulnerabilities. According to Ashebli and Yeun (2024), system authentication measures, including biometrics, which are crucial to the security architecture of Apple Pay, also pose substantial risks if the biometric data is manipulated. Integrations with third-party services such as merchants and banking institutions can also introduce further vulnerabilities if the third parties do not adhere to stringent security standards. For instance, following the EU's antitrust charges against Apple, the company decided to allow third-party developers access to the NFC chip, and this has significant implications for system security and the broader technology ecosystem (Ashelbi & Yuen, 2024).

While there are established client-to-server relationships between the users of third-party payment systems such as Apple Pay and merchants, BEAST attacks can take place when the user browses on public Wi-Fi (Ferdous et al., 2023). For a successful hacking attack to be realised, the attacker has to gain control of the Apple Pay user's browser. However, measures such as hardening the TLS 1.1 and the ban of the Java Plug-in from a browser may protect a user from falling prey to an attack.

CRIME (Compression Ratio Info-lead Made Easy) refers to a vulnerability that is found in the TLS compression. This means that the connection may be created without any compression being involved (Williams et al., 2020). Such a feature is known to reduce the usage of the bandwidth while at the same time maintaining the integrity and security in the process of exchanging large volumes of information. An attacker may target the network used by a victim when carrying out this type of attack. For instance, according to Williams et al. (2020), the users of Apple Pay may have signed into a browser using a public Wi-Fi that has malicious JavaScript and that is in the control of hackers. The script is then likely to initiate a connection with a third-party attacker who then injects plaintext into the cookies of the victim's browser and then keeps track of the size of the response (Williams et al., 2020). If the response is considerably lower than the initial one, this may indicate that the character that the attacker has injected is

contained within the value of the cookie. By using this approach, a hacker may employ brute force on the cookie's value based on feedback from the merchant (Williams et al., 2020).

Based on the TAM framework, the perceived usefulness of Apple Pay may be hindered by the vulnerabilities in the system's architecture and business model. If users perceive the tokenisation of or biometric authentication as unreliable or prone to failure, they may deem the system less useful (Kelly & Palaniappan, 2023). Additionally, vulnerabilities stemming from third-party integrations can lead to a lack of trust, negatively impacting perceived usefulness and ease of use. Continuous evaluation and enhancement of these security measures are crucial to maintaining user trust and system reliability.

However, compared to its close competitors such as Google Pay and Samsung Pay, Apple Pay is widely regarded as a more secure mobile payment platform, often outperforming the others on critical areas. These include tokenisation, biometric authentication, Secure Element and end-to-end encryption (Rao & Deebak, 2023).While these other payment systems also use tokenisation and biometric authentication, Google Pay's reliance on Host Card Emulation (HCE) and Samsung Pay's use of Samsung Knox instead of the Secure Element makes it comparatively less secure against some of the more sophisticated attacks (Rao & Deebak, 2023).

4.3 Causes of Recent Security Incidents or Breaches

The case study findings establish that recent security breaches encountered by Apple Pay users have involved human error, software vulnerabilities and insider threats. For instance, the study establishes that many of the recent security instances can be attributed to human errors, including activities such as the improper handling of Apple devices, the poor management of passwords, or even falling prey to instances of social engineering (Abelson et al., 2024). The study also establishes that vulnerabilities in the iOS or the payment application may provide entry points that can be exploited by hackers. Insiders with privileged access to sensitive information have also been established to be responsible for

some of the recent instances of Apple Pay security breaches (Abelson et al., 2024).

Among the issues that are attributed to the vulnerability caused on the iOS as a result of practices such as “jailbreaking” which are aimed at allowing for the inclusion of modification and customizations to add applications not supported by Apple (Mohd Saudi et al., 2023). The process, according to Mohd Saudi et al. (2023), undermines the original integrity of the iOS by limiting the operation of important security features, making them capable of being attacked through hijackings and malware installations.

Hackers may infect a jailbroken device with malware, which allows them to eventually gain access by attaining root privileges to the user’s device (Mohd Saudi et al., 2023). Tools such as Cycript, Snoop-it and GDB may be used to conduct runtime analyses and steal sensitive user data, including payment traffic data that is on its way to the Apple server (Williams et al., 2020). They may also damage the device and attack the network via FaceTime and other malicious activities.

Other significant vulnerabilities occur at the Secure Socket Layer (SSL) of these mobile payment platforms. SSL is the standard technology for securing internet connections and protecting sensitive information shared between interconnected systems (Rao & Deebak, 2023). It makes it hard for hackers to read and modify any information that is transferred, including all the user’s details. The SSL provides a secure connection through private, public as well and session keys. While encryption and decryption using private and public keys require a lot of processing power, it offers the only way of creating a symmetric session key during the SSL handshake (Williams et al., 2020). Upon the establishment of a secure connection, the session key is employed in the encryption of the transmitted data. As the device’s browser connects to the server to commence a transaction, it is secured by the SSL (Williams et al., 2020). A copy of the SSL certificate is then sent by the server along with its public key. Vulnerabilities in the SSL have been attributed to most of the security incidents and breaches.

Understanding the causes of security incidents is vital for improving the perceived security (and thereby usefulness) of Apple Pay. Human error and insider threats can be mitigated through comprehensive training programs and stringent access controls. Regular updates and patches to address software vulnerabilities can enhance system reliability. Addressing these causes not only improves the system's actual security but also its perceived security, thereby supporting higher adoption rates according to the TAM framework.

4.4 Strategies for Enhancing the Security of Apple Pay Transactions

Based on the findings of this case study, Apple Pay's security may be significantly enhanced by employing a variety of measures that address the vulnerabilities of the platform at the human, software as well and business model levels. While some of these suggestions have been undertaken and implemented to ensure improved security, others are yet to be adopted. For instance, while the Apple Pay system emphasises the use of biometric verification, an added level of security may be achieved through multi-factor authentication (MFA), which is the requirement of multiple forms of identification before granting access to the system (Alabdulatif et al., 2023). According to regulatory entities such as the European Central Bank (2024), these may include biometric verification, using face ID or Touch ID, PIN or password, and a one-time passcode (OTP). The latter involves the sending of a code to a device registered to the Apple Pay user, which has to be entered before access can be granted.

By requiring multiple forms of authentication, the MFA measure reduces the likelihood of unauthorised access, even when one of the factors is compromised. MFA also serves as a notable way of mitigating phishing attacks that capture user credentials as the odds of capturing all of them at once are significantly reduced (Alabdulatif et al., 2023). Measures such as MFA also help in the prevention of unauthorised transactions even when the user's device is lost or stolen. While MFA enhances security, it should also be designed in a way that minimizes inconveniences for the user. Streamlining the authentication process may involve offering options such as biometrics combined with OTPs as a way of balancing

usability and security (Shi et al., 2021). Device compatibility is also necessary for ensuring that all devices that support Apple Pay can seamlessly support MFA.

Other cutting-edge technologies such as artificial intelligence (AI) and machine learning may also be leveraged to continuously ensure that Apple Pay transactions are monitored for fraud and anomalies in real time (Kotagiri, 2023). For instance, the case study establishes measures such as behavioural analytics, real-time alerts, and adaptive learning techniques as necessary in facilitating fraud detection and enhancing know-your-customer measures for applications such as Apple Pay (Kotagiri, 2023).

5 Conclusion

5.1 Summary of Key Findings

This study investigated the security risks of third-party payment systems focusing specifically on Apple Pay. The study employed the Technology Adoption Model (TAM) framework to understand how network security risks, vulnerabilities, and incidents impact user acceptance. Key findings highlight that phishing, MitM attacks, and data breaches pose significant risks, affecting perceived ease of use and usefulness. Vulnerabilities in tokenization, biometric authentication, and third-party integrations were identified as critical concerns. Recent security incidents were largely attributed to human error, software vulnerabilities, and insider threats. Strategies such as Multi-Factor Authentication (MFA) and AI-driven continuous monitoring were found to be effective in enhancing the security of Apple Pay transactions.

5.2 Implications of the Study

The findings of the study underscore the importance of robust security measures in influencing user acceptance of third-party payment systems such as Apple Pay. Implementing MFA and continuous monitoring not only bolsters actual security but also enhances user trust and confidence. User education plays a pivotal role in reducing human error and increasing vigilance against phishing attacks. For practitioners, these insights provide a roadmap for developing secure and user-friendly payment systems that align with TAM principles, ultimately driving broader adoption.

5.3 Limitations of the Study

This study primarily relied on secondary data sources and document analysis, which may limit the depth of insights, compared to primary data collection methods such as surveys or interviews. Additionally, the rapidly evolving nature of cybersecurity threats means that some findings may become outdated as new

threats emerge and security technologies advance. The focus on Apple Pay may also limit the generalizability of findings to other third-party payment systems.

5.4 Future Research

Future research should explore longitudinal studies to track the evolution of security threats and user perceptions over time. Conducting primary research, including surveys and interviews with users and security experts, could provide deeper insights into user behaviour and preferences. Comparative studies across different third-party payment systems could also enhance the generalizability of the findings and identify industry-wide best practices. Investigating the impact of emerging technologies, such as blockchain and quantum cryptography, on payment system security could further contribute to the field.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., & Troncoso, C. (27.01.2024). Bugs in our pockets: The risks of client-side scanning. *Journal of Cybersecurity*, *10*(1), tyad020. Accessed on 06.06.2024

Agarwal, S., Qian, W., Tan, R., Agarwal, S., Qian, W., & Tan, R. (October 2020). Financial inclusion and financial technology. In *Household finance: A functional approach*, (pp. 307-346). Springer. Accessed on 02.05.2024

Ajzen, I. & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour.* Prentice Hall. Accessed on 03.05.2024

Alabdulatif, A., Samarasinghe, R., & Thilakarathne, N. N. (September 2023). A Novel Robust Geolocation-Based Multi-Factor Authentication Method for Securing ATM Payment Transactions. *Applied Sciences*, *13*(19), 10743. Accessed on 07.06.2024

Alshebli, S., & Yeun, C. Y. (2024, February). Examining the Security Landscape of Mobile Payment Systems. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-5). IEEE. Accessed on 08.06.2024

Arnold, D., & Jeffery, P. (28.11.2016). The digital disruption of banking and payment services. In *Research Handbook on Digital Transformations* (pp. 103-120). Edward Elgar Publishing. Accessed on 05.05.2024

Bowen, G. A. (03.08.2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27-40. Accessed on 30.04.2024

Braun, V., & Clarke, V. (January 2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. Accessed on 30.04.2024

Capital One Shopping Statistics. (Jan. 20, 2024). *Apple Pay statistics.* https://capitaloneshopping.com/research/apple-pay-statistics/ Accessed on 10.05.2024

Chen, X., & Li, S. (2017). Understanding continuance intention of mobile payment services: an empirical study. *Journal of Computer Information Systems*, *57*(4), 287-298. Accessed on 06.05.2024

Curry, D. (Jan. 8, 2024). *Mobile payment app revenue and usage statistics (2024).* https://www.businessofapps.com/data/mobile-payments-app-market/ Accessed on 10.06.2024

Daştan, İ., & Gürler, C. (February 2016). Factors affecting the adoption of mobile payment systems: An empirical analysis. *EMAJ: Emerging Markets Journal*, *6*(1), 17-24. Accessed on 11.05.2024

Davis, F. D. (September 1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340. Accessed on 04.05.2024

Duane, A., O'Reilly, P., & Andreev, P. (April 2014). Realising M-Payments: modelling consumers' willingness to M-Pay using Smart Phones. *Behaviour & Information Technology*, *33*(4), 318-334. Accessed on 03.05.2024

European Central Bank (07.03.2024). *Final recommendations for the security of payment account access services following the public consultation.* https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf Accessed on 08.06.2024

Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (October 2023). A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism. *IEEE Access*. Accessed on 08.06.2024

Gao, L., & Waechter, K. A. (June 2017). Examining the role of initial trust in user adoption of mobile payment services: An empirical investigation. Information Systems Frontiers *19*, 525–548. https://doi.org/10.1007/s10796-015-9611-0 Accessed on 08.05.2024

Gong, X., Zhang, K.Z., Zhao, S.J., & Lee, M.K. (July 2016). The effects of cognitive and emotional trust on mobile payment adoption: a trust transfer perspective. *Paper presented at PACIS 2016 Proceedings, Paper 350*. 11 January 2017. Accessed on 11.05.2024

Guo, J., & Bouwman, H. (08.08.2016). An ecosystem view on third party mobile payment providers: a case study of Alipay wallet. *Info*, *18*(5), 56-78. Accessed on 05.05.2024

Hassan, H. E., & Wood, V. R. (2020). Does country culture influence consumers' perceptions toward mobile banking? A comparison between Egypt and the United States. *Telematics and Informatics*, *46*, 101312. Accessed on 05.05.2024

Heggestuen, J. (2015, April 21). *Payments security is undergoing a revolution and Apple Pay is leading the way.* Business Insider. https://www.businessinsider.com/apple-pay-leads-new-security-protocols-2015-4 Accessed on 05.05.2024

Iman, N. (May 2018). Is mobile payment still relevant in the fintech era?. *Electronic Commerce Research and Applications*, *30*, 72-82. Accessed on 09.05.2024

Johansson, R. (01.09.2007). On case study methodology. *Open House International*, *32*(3), 48-54. Accessed on 05.05.2024

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (February 2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior*, *79*, 111-122. Accessed on 05.05.2024

Kazan, E. (January 2015). The innovative capabilities of digital payment platforms: A comparative study of Apple Pay & Google Wallet. In *Proceedings of the 14th International Conference on Mobile Business, ICMB 2015* (p. 4). Association for Information Systems. AIS Electronic Library (AISeL). Accessed on 11.05.2024

Kelliher, F. (2011). Interpretivism and the pursuit of research legitimisation: an integrated approach to single case design. *Leading Issues in Business Research Methods*, *1*(2), 123-131. Accessed on 02.05.2024

Kelly, A. E., & Palaniappan, S. (May 2023). Using a technology acceptance model to determine factors influencing continued usage of mobile money service transactions in Ghana. *Journal of Innovation and Entrepreneurship*, *12*(34), 1-24. Accessed on 01.05.2024

Kelly, D. (2023). Denial of Wallet: Analysis of a Looming Threat and Novel Solution for Mitigation using Image Classification. *PhD Thesis Submitted at the School of Computer Science College of Science and Engineering University of Galway.* Accessed on 09.06.2024

Khwaja, M. G., & Zaman, U. (October 2020). Configuring the evolving role of eWOM on the consumers information adoption. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(4), 125. Accessed on 07.05.2024

Kotagiri, A. (13.12.2023). Mastering fraudulent chemes: A unified framework for AI-driven US banking fraud detection and prevention. *International Transactions in Artificial Intelligence*, *7*(7), 1-19. Accessed on 09.06.2024

Liu, W., Wang, X., & Peng, W. (January 2020). State of the art: Secure mobile payment. *IEEE Access*, *8*, 13898-13914. Accessed on 05.05.2024

Masrom, M. (January 2007). Technology acceptance model and e-learning. *Technology*, *21*(24), 81-91. Accessed on 04.05.2024

Mohd Saudi, M., Husainiamer, M. A., Ahmad, A., & Idris, M. Y. I. (May 2023). iOS mobile malware analysis: a state-of-the-art. *Journal of Computer Virology and Hacking Techniques*, 1-30. Accessed on 09.06.2024

Nahapetyan, A., Prasad, S., Childs, K., Oest, A., Ladwig, Y., Kapravelos, A., & Reaves, B. (2024, February). On SMS Phishing Tactics and Infrastructure. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 169-169). IEEE Computer Society. Accessed on 09.06.2024

Nicholson, T., Hayes, D., & Le-Khac, N. A. (2023, January). Forensic Analysis of the iOS Apple Pay Mobile Payment System. In *IFIP International Conference on Digital Forensics* (pp. 3-19). Springer Nature Switzerland. Accessed on 11.06.2024

Ozili, P. K. (December 2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329-340. Accessed on 01.05.2024

Pour, M. S., Nader, C., Friday, K., & Bou-Harb, E. (May 2023). A comprehensive survey of recent internet measurement techniques for cyber security. *Computers & Security*, *128*, 103123. Accessed on 04.06.2024

Rao, P. M., & Deebak, B. D. (March 2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. *Ad Hoc Networks*, 103159. Accessed on 02.06.2024

Shi, S., Wang, X., & Lau, W. C. (June 2021). Breaking and Fixing Third-Party Payment Service for Mobile Apps. In *International Conference on Applied Cryptography and Network Security* (pp. 3-26). Cham: Springer International Publishing. Accessed on 15.05.2024

Solat, S. (January 2017). Security of electronic payment systems: A comprehensive survey. *Journal of Network Security, 1*(3), 12-24. Accessed on 11.05.2024

Williams, D., Hu, Y. H., & Hoppa, M. A. (2020). Follow the money through Apple Pay. *Journal of The Colloquium for Information Systems Security Education,* 8(1), 11-21). Accessed on 29.04.2024

Yang, W., Li, J., Zhang, Y., & Gu, D. (October 2019). Security analysis of third-party in-app payment in mobile applications. *Journal of Information Security and Applications*, *48*, 102358. Accessed on 02.05.2024