National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

CERTIFICATE NO : NCARSEMH /2025/ C0725720

A Study on Mobile Payment Security Threats and Protective Measures

Amit Sahu
Research Scholar, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

The rapid growth of mobile payment systems has transformed the way financial transactions are conducted, offering convenience, speed, and accessibility to users worldwide. Technologies such as mobile wallets, near-field communication (NFC), QR code payments, and mobile banking applications have become integral to modern digital economies. However, the increasing reliance on mobile payment platforms has also introduced significant security challenges. Cybercriminals exploit vulnerabilities in mobile devices, networks, and applications to conduct fraud, data theft, identity theft, and unauthorized transactions. This study examines the major security threats associated with mobile payment systems and analyzes the protective measures employed to mitigate these risks. By exploring both technological and user-centric security strategies, the study highlights the importance of robust encryption, authentication mechanisms, regulatory frameworks, and user awareness in ensuring secure mobile financial transactions. The findings emphasize that while mobile payment technologies continue to evolve, security must remain a fundamental priority to sustain user trust and system reliability.

Keywords: *Mobile Payments, Security Threats, Cybercrime, Authentication, Data Protection.*

I. INTRODUCTION

We are seeing the slow but steady rise of a digital society as a result of the exponential growth of the internet and related technologies over the last decade. The widespread use of digital payment systems has transformed the way individuals shop and manage their money. One term for the movement of money from one location to another using the Internet and related technologies is a "digital payment."

Mobile wallets, internet banking, contactless payments, crypto currencies, QR codes, and peer-to-peer (P2P) transactions are just a few examples of the various digital payment options available today. Thanks to digital payment methods, cross-border purchases are now easier. International commerce and money transfers to many countries may be done more quickly and at cheaper rates than with traditional methods like wire transfers. When using digital payment methods, it is essential to keep your personal and financial information secure. Generally speaking, in today's networked world, digital payment systems provide security, speed, and convenience, and they have changed the way financial transactions are done. Capgemini reported a worldwide increase of 10.1% in non-cash transaction volumes in 2019, with a total of 708.5 billion transactions. The survey predicted that digital transactions would continue to grow in the years to come. The way individuals do business has been

National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

revolutionized, and it's becoming more popular globally. The rise of digital payment methods may be attributed to many factors, including advancements in technology, changes in customer expectations, and the need for secure and easy payment solutions.

Advancements in Technology: The rapid advancement and widespread usage of digital technology have substantially facilitated the worldwide deployment of digital payments. The proliferation of smartphones, the enhancement of internet access, and the development of more robust encryption and security protocols have all contributed to the success of digital payment systems. By 2022, the International Telecommunication Union (ITU) predicts that 66% of the global population, or over 5.3 billion people, will be online. With an expected 1.1 billion individuals being online during that time—a sizable user base for digital payment services—this is a 24% rise from 2019. In addition, the proliferation of mobile apps and the ease of access to high-speed internet have made digital transactions easier for both individuals and businesses.

Customers' Choices Are Shifting: Customer desire for convenience and increasing dependence on digital devices have substantially facilitated the expansion of digital payment systems. Customers have welcomed digital payment systems due to the speed, convenience, and efficiency they provide, which has been especially helpful with the growth of e-commerce, online shopping, and the sharing economy. Accessible and Secure Payment Options Must Be Offered: Worldwide, people are looking for more accessible, secure, and quick ways to pay, and this need has driven the rise of digital payments.

The security, traceability, and practicality issues with the two most prevalent modes of payment—cash and checks—are significant. Tokenization, encryption, and two-factor authentication are some of the security elements offered by digital payment systems that help to reduce the chances of fraud and deceitful entry.

The growth and development of digital payment systems in India has been phenomenal in the last few years. An effort to wean the country's economy off of cash has the backing of the Indian government, which has been pushing for digital payment systems. The usage of electronic payment methods has been encouraged by a variety of policies and programs.

Efforts by the government: Digital payments have been actively promoted by the Indian government through various programs and policies, such as the Pradhan Mantri Jan Dhan Yojana (PMJDY) for financial inclusion, the Goods and Services Tax (GST) for tax simplification, and the demonetization drive in 2016 for the purpose of reducing the circulation of high-value currency notes and promoting digital transactions. Keep in mind that new tools and services are sprouting all the time in India's digital payment ecosystem, so it's important to stay updated. Federal officials, banking institutions, and fintech companies are working together to create a safe and robust digital payment system in the country.

In the future of cashless society, mobile devices will be the main means of payment. Furthermore, mobile payments are becoming more popular as a cashless alternative throughout the world and have huge potential. The term "mobilepayment" describes a kind of electronic payment that makes use of portable electronic devices with wireless capabilities, such as smartphones and PDAs. Research shows

a trend towards using mobile wallets and applications for mobile payments, which has been growing in popularity. The Worldpay Global Payments Report 2020 found that in 2019, the utilization of mobile payments increased by 36% worldwide.

Mobile payment solutions are beneficial for both companies and customers. With mobile payment services, customers have the convenience of fast and easy payment options at their fingertips. It is believed that mobile payment services would increase retailers' transaction volume, decrease transaction costs, and strengthen customer loyalty. The adoption and use of mobile payment systems by customers remains an issue, notwithstanding these benefits.

The increasing popularity of mobile payment apps and digital wallets was highlighted in a 2020 study by Statista, which found that 57% of respondents favored using these methods for in-store transactions. The convenience of using a digital wallet or smartphone to make a payment has attracted a large user base, particularly among younger generations who are more used to using digital technology.

Around one billion individuals throughout the globe do not have access to a bank account, but they do own a mobile phone, according to the World Bank's 2017 Global Findex Database. Among the most crucial pieces of data about the growth of mobile payments in India is the prevalence of mobile wallet services. Statista estimates that by 2020, the total value of mobile wallet transactions in India would have increased from 55 billion Indian rupees in 2016 to 1.49 trillion Indian rupees.

One of the most widely used mobile payment systems in India is the Unified Payments Interface (UPI). As of September 2021, UPI has seen tremendous growth, with the number of transactions growing from over 918 million in December 2018 to over 3.6 billion in August 2021, according to the National Payments Corporation of India (NPCI). This research provides further evidence that electronic payment methods may help more people get access to formal financial services. By using mobile and digital technologies, people in underprivileged regions may have access to financial services and participate in the digital economy.

II. REVIEW OF LITERATURE

Cavus, Nadire & Atanda, Adeoluwa. (2022). The technological revolution has changed many aspects of our daily lives, but one area that has been particularly impacted is the way we deal financially. Since these transactions are taking place over wired and networked systems, it is even more important to have secure mobile payment solutions in place to prevent hackers from gaining access to critical personal information. This article introduces the Secure Mobile Payment System (SMPS), a robust technology that may enhance the security and efficiency of mobile transactions. A number of high-tech security features are included into the SMPS to guarantee the safety of user data and the authenticity of transactions. Among these techniques are real-time fraud detection, encryption, biometric authentication, multi-factor authentication, and tokenization. The SMPS aims to build user trust and provide seamless, secure financial operations across multiple devices by offering a

comprehensive security architecture. In addition to identifying strengths and areas for improvement, the research takes a look at existing systems including CLIQ, PayPal, Apple Pay, Google Pay, and Samsung Pay. The SMPS solves these issues by providing a platform that is easy to use and available to everyone. Future enhancements to the planned system will include the incorporation of new technologies such as artificial intelligence and machine learning to detect and prevent fraud, which will improve both its security and the user experience. This project sets a new standard for digital transaction systems by advocating a secure, efficient, and cashless way of managing finances.

Hwang, Yoonyoung et al., (2021) Unique, specific, and individualized services are what set financial technology (fintech) services apart from more conventional financial options. The most important fintech service now is mobile payment service (MPS). There have been a lot of studies on the importance of security for service providers and users when it comes to financial transactions, but no one has looked at how users' different views of security relate to the factors that determine the success of MPS. Understanding how users respond differently depending on their perceptions about the MPS use environment is the primary goal of this research, which attempts to reveal the unique roles of platform and technology security. Two aspects of security (platform and technology) and three factors (convenience, interoperability, and trust) that determine the effectiveness of MPSs are proposed in this study's research model. Using data collected from an online poll of 356 participants, we conducted an empirical evaluation of the suggested model. User experiences with the chosen MPS are taken into consideration in the survey. The findings demonstrate that users' favorable views of the factors influencing the performance of a security-driven MPS during financial transactions may be significantly improved or diminished. This research offers theoretical insights into the functions of platform and technology security in order to further our understanding of how this shift in user perception of security impacts the entire MPS using experience. In addition, the possible consequences of users' subjective and objective views of the MPS security environment are used to provide managerial insights into the design strategies of MPS providers.

Mitrea, Teodor & Borda, Monica. (2020). Thanks to new technology and the explosion of mobile devices, mobile payment and mobile commerce have changed the game on a worldwide scale in the last few years. The proliferation of security breaches, fraud, and associated cybercrimes necessitates that, despite many attempts, creating and growing mobile payment systems and services pay great attention to security problems. This article discusses security issues in three related areas: mobile device security, mobile transmission security, and network security. It also examines the classification of mobile payment security risks and attacks. Network security includes wireless local area networks (WLANs) and wide area networks (WWANs); transmission security includes wireless data transfer protocols (WAP, SMS, wave channel, USSD); and mobile device security includes operating system and hardware platform security.

Kang, Jungho. (2018). The convergence of finance and technology, or Fintech, is a relatively new phenomenon that has emerged as a result of advancements in information technology. The necessity for a mobile Fintech payment solution that facilitates seamless online and offline payment has grown, in

National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

particular, because to the ever-increasing supply of mobile devices and the fast expanding online market. The worldwide mobile payment market size was anticipated to increase from $45.1 billion in 2012 to $222.4 billion in 2017, with an average yearly growth rate of 38%, according to a 2013 analysis by market research firm Gartner. To help with future service improvements and security concerns, this research will examine current mobile Fintech payment patterns and classify them according to service formats. The research began by comparing and defining traditional payment services with Fintech payment services. It then examined new mobile Fintech payment services and used that data to categorize the companies offering these services into four groups: financial institutions, hardware manufacturers, operating system developers, and payment platform providers. Last but not least, it outlined the standards that mobile Fintech payment services should adhere to and the security issues that both current and future mobile Fintech payment services would face in relation to availability, privacy, integrity, authorization, and mutual authentication. It is believed that future mobile Fintech payment systems would be more secure thanks to the proposed research.

Esmaeili, Leila et al., (2012) Mobile commerce and mobile payment have been transformed globally in the last few years due to the proliferation of mobile devices and new technological developments. Despite numerous efforts, developing and expanding mobile payment systems and services must pay close attention to security concerns in light of the increasing prevalence of forgery, fraud, and related electronic crimes, as well as security attacks and threats. This article delves into the categorization of mobile payment security risks and assaults and addresses security concerns in three interconnected areas: mobile device security, mobile transmission security, and network security. Wireless local area networks (WLANs) and wide area networks (WWANs) are part of network security; wireless data transfer protocols (WAP, SMS, wave channel, USSD) are part of transmission security; and operating system and hardware platform security are part of mobile device security.

III. MOBILE PAYMENT SYSTEM

Several components make up this system. These include a mobile network, users and IT administrators, banks, base transceiver stations, databases, and servers. The servers in this system include telecom gateway servers like SMSGW and USSD, core servers, and web servers. In order to access the worldwide mobile network, it then establishes connections with various mobile network operators (MNO). wireless communication systems (GSM). Full commercial capabilities are not provided by the infrastructure alone; more platforms are required. The following internal MNO interfaces are available: the SMSC, the USSD Gateway, the Web Services, the Airtime In/Out Mediation Platform, and the IVR Gateway.

IV. MOBILE PAYMENT MODELS

Most mobile payment systems are built to withstand assaults from malware and ransomware. The four primary methods of safe mobile payment processing: QR-code, contactless, mobile wallet, and MP-based SMS. When it comes to making safe and easy mobile purchases, each model offers a somewhat different take. We can learn a lot about the many choices that companies and customers have when it comes to mobile payments by looking at these models.

National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

QR Code Payment

Quick Response Code is abbreviated as QR. In order to make a payment, the matching code is created wirelessly. Particularly for contactless transactions, they are now a popular form of payment. When it's necessary to deduct and credit funds, this is the tool to use. It is used by both the retailer and the buyer. This function of mobile payment apps makes it possible to make several purchases at once. When the seller creates the QR code with the price information, they may be used. The client may easily update their payment information as the amount is being transmitted, which is seen as a valuable feature.

Payments Through Contactless

One of the most prominent and widely used contactless payment methods is NFC Thought. Two devices may store, exchange, and transfer data over a link that follows certain norms and restrictions. Due of its short range, it is unlikely to be able to use advanced features like airdropping or Bluetooth in order to transfer data across a large number of devices that need to be connected beforehand. Having the NFC-enabled gadget in close proximity to the user's device ensures a successful transaction. Since the data is completely safe and exceedingly straightforward, users choose NFC over other payment options. Authentication on the protected website is done using a PIN. You may also use bitcoin as a contactless payment option right now.

Mobile Wallets

Making a purchase is as easy as clicking a button using mobile wallets. It is easy to transfer funds from a bank account to an electronic wallet since the two are interconnected. When using a wallet for services and products like PayPal, Apple Pay, or Google Wallet, money may be sent or received.

MP Based on SMS

This method of payment is very easy to use and understand. Technical procedures for payments may be expedited. The need for additional user identification and the limitation on authenticity is two of the downsides of this payment option.

V. MOBILE PAYMENT SECURITY

Everyone involved in mobile payments, from consumers to service providers, must prioritize mobile payment security. All three phases of a payment's lifecycle—while stored, sent, and used—must be secure.

Mobile Payment Security Services

Mobile payment systems aim to provide the following security services: availability, nonrepudiation, secrecy, access control, and authenticity. User authentication and transaction data origin authentication are two distinct services that make up authentication. Both the user's identity and the data's origin must be able to be verified by a mobile payment system. The mobile payment system is protected by an

access control mechanism that only allows authorized users to access it. When making a purchase using a mobile payment, consumers may be asked to input additional security information, such as a fingerprint scan or a PIN or password, in addition to the usual credentials used to unlock the device.

Preventing passive assaults on transaction data is the purpose of confidentiality. Data integrity safeguards against tampering with transaction data while it is in use, in transit, or at rest. Neither the user nor the service provider is able to refuse the transmission of a communication thanks to nonrepudiation. A mobile payment system's availability determines how quickly and easily consumers may use it. Cryptographic operations—encryption, hashing, digital signatures, etc.—are crucial to many of these security services. Mobile payment methods that rely on near field communication (NFC), like Apple Pay and Google Wallet, also make use of the cryptographic processing capabilities inherent to mobile devices.

Mobile Payment Security Mechanisms

To guarantee the safety of mobile payments, several security measures have been implemented. Here is a brief overview of these mechanisms:

- **Fingerprint:** With Apple Pay and Samsung Pay, you may approve a payment with a simple touch of your finger to the device's fingerprint reader. Login credentials: The usage of a username and password is common practice for both integrated and standalone mobile payment systems that allow users to make purchases.
- **Multi-Factor Authentication:** The usage of multiple factors of authentication is also common in mobile payment systems. For instance, when a user logs into the service with a new phone, they are needed to provide an authentication code. Next, an email containing the authentication code is sent to the user's registered email account.
- **SSL/TLS:** Internet data is often protected using SSL/TLS. When transmitted over the Internet, mobile payment data can be protected with SSL/TLS, which also ensures its integrity and authenticity.
- **Secure Element:** The secure element on a mobile device is also used by NFC-based mobile payment systems for cryptographic processing and the protection of sensitive data. The secure element stores sensitive information, like fingerprints and the device's unique account number, in Apple Pay, for instance.

VI. MOBILE PAYMENT THREATS AND REMEDIATION

Cybercriminals attack mobile payment systems. Smartphones and tablets are vulnerable to a wide variety of attacks and threats. Even a mobile payment system is vulnerable to these kinds of assaults and threats. Users risk having their personal information exposed and losing money if their mobile payment account is compromised. Where you may get in-depth analyses of mobile device security risks and assaults is. Here we take a look at the most important assaults and threats to mobile payment security and try to summarize them.

National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

Malware

A mobile payment system is vulnerable to mobile malware. More than one million applications were deemed malicious by Symantec in 2014. The majority of mobile malware is involved in activities that might compromise sensitive information, such as secretly recording calls, instant messaging, GPS locations, and call records. The notorious Trojan horse Zeus targets banks' one-time passwords used to verify mobile payments. It guarantees that customers are safely connected into their bank's web portal and seems to be a component of Trusteer's Rapport program. All incoming SMS messages are monitored by Zeus and sent to a remote malicious website. The victim's money might be stolen from their bank accounts if a criminal from Zeus manages to steal their login details. Symbian, BlackBerry, and Android users may be at risk of having their one-time passwords supplied to them by their banks for mobile transaction authentication stolen by ZitMo, a mobile variant of Zeus.

SSL/TLS Vulnerabilities

When it comes to protecting sensitive information online, many mobile payment systems rely on SSL/TLS. Malicious users might use weaknesses in SSL/TLS and its implementation to compromise security. One major flaw in the OpenSSL library's security is known as the Heartbleed Bug. The vulnerability allows malicious users to bypass SSL/TLS encryption and steal sensitive data. April 2014 was the month when the Heartbleed Bug was revealed. As of OpenSSL 1.0.1's release on March 14, 2012, however, the flaw has been available to the public. A man-in-the-middle (MITM) attack may also compromise SSL/TLS. The goal of a man-in-the-middle (MITM) attack against SSL/TLS is to compromise the security of the connection between a client and a server. The attacker has access to all of the unencrypted data sent between the client and server, even though this data should be encrypted to avoid network sniffing. All of the private data, including login credentials and financial details, is at jeopardy. If an attacker gains access to a user's account, they may either take funds from it or use it to commit fraud.

Data Leakage

In the mobile payment procedure, two additional actors are engaged compared to the standard payment card method. If we take a typical situation where a user uses their mobile wallet at a mobile point of sale, there are five parties involved: the user, the merchant, the acquiring bank, and the issuing bank. In order to make a purchase, all participants must gather the necessary transaction details. All participants in the payment process are obligated to adhere to the rules' criteria for the security of payment data. But things may still go wrong. Identity thieves were able to get their hands on customers' payment card details (names, addresses, phone numbers, etc.) in the Target and Home Depot data breaches. There was an impact on millions of consumers. The point-of-sale systems at Target and Home Depot were infiltrated with a specially developed piece of malware called Backoff. The lessons learned from these data breaches may help mobile payment service providers avoid similar problems in the future.

National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

Mobile Payment Threats Remediation

It is the shared responsibility of mobile payment users and service providers to safeguard sensitive information and forestall data breaches in order to reduce the likelihood of security incidents involving mobile payments. Users of mobile payment systems should take the following precautions: secure their devices with strong passwords, patterns, or pins; update their operating systems and install all recommended security patches; refrain from installing malware on their devices; exercise caution when receiving suspicious SMS or emails; avoid connecting to Wi-Fi hotspots; and do not proceed if messages like "can't verify the identity of the website" are displayed. In order to save the user's password for future usage, certain mobile payment applications may just need a single sign-in. Since a combination of a PIN, password, and screen lock pattern is the final line of defense against fraudulent purchases, users should exercise extreme care in such a situation.

The security of mobile payment apps, the protection of payment data, and the prevention of data breaches in the backend are all responsibilities of mobile payment service providers. Internet security protocols like SSL and TLS are used by a lot of mobile payment applications. The server-side validation of certificates is essential for these mobile payment applications. It is essential that mobile payment systems immediately halt and notify consumers of any suspicious activity upon receipt of an invalid certificate.

VII. MOBILE PAYMENT SECURITY CHALLENGES

The safety of mobile payments has been the focus of several security measures. On the other hand, there are security concerns with mobile payment systems, including the need to identify and prevent fraud, data breaches, malware, and multifactor authentication.

Malware Detection

When it comes to protecting mobile payments, malware is a major issue. There have been several precautions taken to identify and stop the spread of malware. The fact remains, however, that malware can and does spread on mobile devices. Detecting malware on mobile devices is a difficult task. The many approaches now used to identify malware include mobile forensics, static analysis, dynamic analysis, and more. On the other hand, not a single one of them can reliably identify mobile malware. The goal is to find a way to identify malware that is effective.

Multi-factor Authentication

When a customer logs into their mobile payment system account from a new device, multi-factor authentication may be used to stop fraud. An authentication code is sent to the user by another means of communication, such email, and the user must input it. Still, it's possible for people to misplace or steal mobile devices. The email account is vulnerable to malicious individuals who might impersonate the multi-factor authentication procedure.

National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

Preventing Data Breach

Data breaches may happen. Personal details including credit card numbers, transaction histories, and cell phone numbers might be revealed in the event of a data breach. A threat to user privacy exists. Identity theft is another possible outcome.

Fraud Detection and Protection

With mobile payment, you may make a purchase whenever and anywhere you choose. Because of this, thieves may also take advantage of mobile payment systems. Criminals may commit fraud or steal money by using hacked mobile payment accounts or stolen payment cards. It is critical to identify and stop fraudulent transactions when they occur. Users may feel more comfortable using a mobile payment system again if they know what to expect in the event that they incur monetary losses as a result of fraud.

VIII. CONCLUSION

To their ability to streamline and simplify monetary transactions, mobile payment systems have become indispensable in today's digital economy. Users and service providers alike are increasingly vulnerable to a wide array of security dangers that have emerged in tandem with their fast adoption. The inherent weaknesses of mobile-based financial systems are brought to light by threats such as malware assaults, phishing, data breaches, and unauthorized access. The results of this research show that cutting-edge technical solutions, robust legal frameworks, and educated user behavior are all necessary to overcome these obstacles. To reduce the likelihood of security breaches, it is essential to include safeguards like encryption, MFA, biometric security, and fraud detection systems. A safe mobile payment environment also requires users to be knowledgeable and that businesses comply with regulations. To keep up with the ever-changing nature of cyber threats, security measures must be refined over time. In order to keep people's faith, keep financial data safe, and encourage the further expansion of digital payment systems, strong mobile payment security is essential.

REFERENCES

1) N. Cavus and A. Atanda, "Security and privacy concerns in mobile payment services," *Global Journal of Information Technology: Emerging Technologies*, vol. 12, no. 2, pp. 136–148, 2022, doi: 10.18844/gjit. v12i2.8264.
2) Y. Hwang, S. Park, and N. Shin, "Sustainable development of a mobile payment security environment using fintech solutions," *Sustainability*, vol. 13, no. 15, p. 8375, 2021, doi: 10.3390/su13158375.
3) J. S. Manoharan, "A novel user layer cloud security model based on chaotic Arnold transformation using fingerprint biometric traits," *Journal of Innovative Image Processing*, vol. 3, no. 1, pp. 36–51, 2021.
4) Sivaganesan, "A data-driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks," *Journal of Trends in Computer Science and Smart Technology*, vol. 3, no. 1, pp. 59–69, 2021.

National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

5) T. Mitrea and M. Borda, "Mobile security threats: A survey on protection and mitigation strategies," in *Proc. Int. Conf. Knowledge-Based Organization*, vol. 26, pp. 131–135, 2020, doi: 10.2478/kbo-2020-0127.
6) Galhotra, "Security concerns for mobile-based digital wallets with the use of IDS & IPS system," *Test Engineering and Management*, vol. 83, no. 3, pp. 16618–16623, 2020.
7) A. A. G. Deepti Sharma, "A study of consumer perception towards m-wallets," *International Journal of Scientific & Technology Research*, vol. 8, no. 11, pp. 3892–3895, 2019.
8) Eswaran, "Consumer perception towards digital payment mode with special reference to digital wallets," *Research Explorer – Blind Review & Refereed Quarterly International Journal*, vol. 7, no. 2, pp. 13–20, 2019.
9) J. Kang, "Mobile payment in fintech environment: Trends, security challenges, and services," *Human-Centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1–16, 2018, doi: 10.1186/s13673-018-0155-4.
10) S. G. S. Akanksha Bali, "Biometrics security in mobile application development and its applications," *International Journal of Scientific and Technical Advancements*, vol. 11, no. 2, pp. 51–60, 2018.
11) R. G. H. W. P. Beadle, "A review of internet payment schemes," in *Proc. ATNAC'96*, vol. 1, no. 1, pp. 1–6, 2018.
12) K. Paulson and P. Kuriakose, "Secured Android application using biometric authentication," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 4, pp. 7715–7719, 2017.
13) J. U. K. D. Fourcan Karim Mazumder, "Security in electronic payment transaction," *International Journal of Scientific & Engineering Research*, vol. 6, no. 2, pp. 955–960, 2015.
14) L. Dowland, N. C. Furnell, and M. Papadaki, "Active authentication for mobile devices utilising behaviour profiling," *Springer Journal*, vol. 13, no. 3, pp. 229–243, 2014.
15) V. Aggarwal, "E-commerce security issues and solutions: A survey," *Galaxy International Interdisciplinary Research Journal*, vol. 2, no. 1, pp. 159–163, 2014.
16) D. B. Pradnya and B. Rane, "Transaction security for e-commerce application," *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 3, pp. 1720–1726, 2014.
17) S. H. K. Ajeet Singh, "A review: Secure payment system for electronic transaction," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 3, pp. 236–243, 2012.
18) Esmaeili, Z. Borhani-Fard, and M. A. Arasteh, "A survey on mobile payment systems security," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 4, no. 20, pp. 4043–4050, 2012.
19) S. Karnouskos, "Mobile payment: A journey through existing procedures and standardization initiatives," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 4, pp. 44–66, 2004.