Security and Vulnerability in Digital Payment Systems

Yash KB
MCA
Surana College, Kengeri
Bengaluru
yashkb79@gmail.com

Gagan C
MCA
Surana College, Kengeri
Bengaluru, India
cgagan01@gmail.com

Ajay Kumar MS
MCA
Surana College, Kengeri
Bengaluru, India
ajaykumarms123@gmail.com

Prof.Bharathi Ramesh
MCA
Surana College, Kengeri
Bengaluru, India
bharathi.mca@suranacollege.edu.in

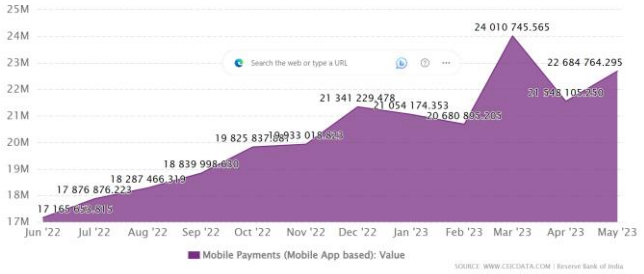
***Abstract*— This paper provides information on security threats in digital payments. Paper also addresses the threats of Trojan, which acts normally but can cause huge damage eventually compromising user's sensitive data. It consists of different types of Trojans, like backdoor and Banking Trojans. It also highlights other security threats like Denial of service (DOS), worms and phishing attacks which indicates to users that constant preventative measures and safety practices should be followed. practices such as up-to date software, using firewalls and users becoming aware of where to not download files. various authentication mechanisms like password-based have improved overall security. Moreover, the paper explains Encryption techniques like symmetric, asymmetric encryption to safeguard your data. The paper covers algorithms like AES, 3DES and RSA. Additionally paper covers hybrids which use both symmetric and asymmetric encryption. It also describes protocols that helps to avoid security risks. Tokenization replaces card details with tokens. With biometric authentication advances security. Mobile challenges are also discussed.**

Keywords—digital payment systems, security, vulnerability, authentication, encryption techniques, fraud detection, fraud prevention, secure transaction protocols.

I. INTRODUTION

The invention of digital payments methods has resulted in various methods that manage financial transactions. The various technologies like from online shopping to mobile banking are the technologies providing speed simplicity, they allow customers to make payments anytime and anywhere. However, the people depend on digital platforms, the sensitive user data and financial information will be secured. We will explain about the complexities of digital payments security threats and vulnerabilities. It sparkles the light on the possible threats created by malware, particularly trojan horses, which can penetrate user data and cause damage on digital platforms. It highlights some other security threats like DOS attacks, phishing, and malware that targets the user's personal information. underlining the necessity for ongoing monitoring and proactive security measures. Paper explores various authentication mechanisms in the digital payment system. It includes password authentication and two-factor authentication. It talks about the significance of strong passwords, the danger of weak passwords and installation of additional verification processes to improve security. Moreover, it investigates the role of one-time password and biometric authentication such as facial recognition, fingerprint, in bolstering the security of digital payment transactions. Encryption technique plays an important role in protecting the data during transactions. The paper looks into symmetric and asymmetric encryption algorithms, such as AES, 3DES, and RSA, stressing their relevance in preserving the security and integrity of sensitive information. It also explores the hybrid encryption technique which combines both symmetric and asymmetric encryption to increase security measures. Furthermore, the paper addresses the significance of fraud detection and prevention in digital payments. It helps to prevent fraud detection. It investigates the significance of secure transaction protocols such as tokenization in improving security and protecting sensitive data. Emerging technologies include block chain for secure transactions, artificial intelligence for fraud detection, and machine learning for pattern analysis. Finally, this paper presents a detailed summary of digital payments security threats and vulnerabilities. Stakeholders can assure the confidentiality, integrity and authentication of transactions

by identifying the risks and implementing suitable security measures, eventually generating trust and confidence among users.



II. LITERATURE REVIEW

Digital payments have changed dramatically how the way money is handled, providing convenience and efficiency to all users around the world. As the usage of digital payment systems grows. There are significant security concerns. The purpose of this overview of the literature is to provide a full understanding of the existing landscape and suggest future research topics on security risks in digital payments. It accomplishes this by evaluating the body of knowledge and scholarly contributions made in this field. In order to understand security challenges, it is critical to examine the features and operation of digital payment systems. Numerous studies have been conducted on various digital payment systems, such as mobile payments, internet banking, and crypto-currency exchanges. These studies highlight the procedures, protocols, and technologies employed in these systems, as well as any potential weaknesses that could be exploited by malicious actors. A wide range of security concerns and attacks are revealed by the literature review to be directed at digital payment systems. The vulnerabilities present in the communication channels used for digital payments are a prominent field of research. Studies indicates that we use encryption and authentication mechanism for unauthorised access or compromised system. Malware's most common threat are ransomware and banking Trojan, which can attack users on finance platform for their data . Researchers have looked into the methods, capacities, and effects of various malware strains, providing insights into how they change over time and proposing mitigation tactics to combat them. The study covers the topic of mobile payment systems and related security issues. It gives an overview of several mobile payment methods, including direct carrier billing, mobile payment platforms, independent mobile payment systems, mobile payment at the point of sale (POS), and mobile payment as the POS. The assessment underscores the usefulness and appeal of mobile payment systems but also draws attention to the security risks and difficulties they encounter. Additionally, the literature goes into great detail on the subject of fraud and identity theft in online transactions. Researchers have looked at phishing attempts, social engineering methods, and account takeover as examples of identity theft. To lessen the risks associated with identity-related attacks, they have suggested a variety of detection and prevention measures, including multi-factor authentication, bio-metric verification, and anomaly detection algorithms. The literature also focuses on user awareness and education. Researchers stress how crucial it is to inform users of the possible risks and the best procedures for safe online transactions. To encourage responsible conduct and reduce the frequency of security events, they suggest user-friendly security interfaces, training programs, and awareness campaigns. Malware, SSL/TLS vulnerabilities, and data breaches are the three primary security risks in mobile payment systems, according to the research. It explains the dangers that could result from compromised mobile payment accounts as well as how mobile devices are susceptible to virus attacks. The assessment also emphasizes the weaknesses in SSL/TLS encryption as well as the danger of data breaches that can expose private payment information. Detection of malware, multi-factor authentication, data breach prevention, and fraud detection and prevention are the other four security issues covered in the evaluation that pertain to mobile payment systems. In order to protect against data breaches and fraudulent activities, it underlines the necessity for efficient malware detection techniques, strong authentication procedures, and preventive measures. In the literature review along new technologies are also examined with the impact on electronic payment system security system. Block chain technology, Artificial intelligence and distributed ledger technology have been investigated for their prospective to increase the security of payment systems. They also high light the perspective as additional security dangers connected to these technologies such as privacy and scalability. Overall, the assessment of the literature shows that security risks associated with digital payments are many and changing quickly. Even though major efforts have been made to combat these risks, regulatory agencies, industry, and academia must continue to work together and conduct research in order to remain ahead of the continuously evolving danger landscape. This study intends to contribute to the creation of efficient security frameworks and procedures that protect the integrity and credibility of digital payment systems by identifying the research gaps and current knowledge gaps.

III. SECURITY THREATS AND SOLUTIONS

Security threats related to digital payment will evolve day by day. Some of common threats are Trojan. Trojan is malware

where is acts as genuine software of the users but behaves the way it wants. Trojan can reach users Personal computer(PC) or Phone through email along with PDF or downloadable links. It can track keystrokes, make system vulnerable to other attacks. It will change original data form, copy important information, update data if required, use system resources for its own task and hinder system performance. Comparing other viruses, Trojan don't have capability to duplicate itself . Trojan can act in multiple ways, Backdoor Trojan where it will not attack your system instead will open doors for other attackers to manipulate your system, it achieves this by loading variety of malware to victim system which makes system vulnerable. Rootkit will make sure that victim will not any malware on his/her system. Banking Trojans are those which captured screenshot during payment transaction with keystrokes capturing. Remote access Trojan gives attacker a way to access victims system remotely, similar to banking Trojan even this can capture screenshot of transactions. Trojan works in following, first it get downloaded to victim's system by escaping victim's awareness. Then Trojan gives remote working environment for attacker to deploy more malware to victim system. To this point victim system is under control of attacker. With respect to digital payment, attacker can target sensitive information like credit card details, transaction data, login and usage logs. They are good at hiding their presence on the victim system with the help rootkit type of virus. As mentioned earlier Trojan has capability to capture keystrokes which in turn leads to collect user credentials like username and password. In some cases it also captures screenshots, if you want context of screenshot with digital payment where attacker can take screenshot of transaction of victim.

Denial of service is the Cyberattack, where the third party tries to flood your system with hundred's of requests. This makes platform to break down and unable to provide service for users in turn recurring losses.

Worms are more dangerous because it does not need attacker intervention. It can act on its own, meaning it will duplicate itself and spreads across many devices. One way it attacks is using Distributed denial of service (DDoS).In which it compromises as many as devices in the network and will flood the network as many request to bring the system eventually making financial loss to platform, service being unavailable to users. In digital platform it can also take advantage of code not written properly, networks.

phishing attacks comes Cyber threat where attackers act as trusted platform to communicate with unsuspecting user via mail, text or website. attackers make sure he acts like trusted platform to get user credential or other sensitive information from the user.

Solution to prevent oneself from malware and attacks is keep antivirus up to date. This software detects and eliminate malware. Anti-virus companies releases software updates regularly so with those software updates software can perform and detect new viruses in the market. one more thing users can do is to use firewall which stands between device and foreign network ensuring logging of all activity. By enabling firewall will reduce the chances of system being compromised. users should be educated on where to download files; cause Trojan are usually hidden in the PDF upon which downloading can transfer it system directly. Make use of Encryption technique like SSL and TLS which encrypt connection between entity during transaction.

IV. AUTHENTICATION MECHANISMS

In an era where digital payment systems are transforming our transaction methods, it is crucial to prioritize the implementation of strong security measures. This article explores the world of authentication mechanisms utilized in digital payment systems, providing insights into their importance and influence. By comprehending the advantages, drawbacks, and implementation factors associated with different authentication techniques, developers and users of payment systems can make well-informed choices to enhance security without compromising the convenience of seamless transactions.

1.**Password-based:**

Aauthentication is an important safety feature in digital payment systems, making password strength an important factor in making sure security in general. This section addresses the importance of powerful passwords, the risks associated with weak ones, and ways for creating and managing strong passwords. In addition, it stresses the importance of password hashing n protecting user credentials, particularly in the event of data breaches.

Two-factor authentication, or 2FA for short, is an excellent way for improving security. Users must offer an additional form of verification in addition to their passwords in such a way. The paper examines several 2FA options, such as SMS codes, authentication apps, and bio-metrics, and assesses their usefulness in increasing security and limiting the risks of password leaks or theft.

2. **Two-Factor Authentication:**

To bolster security, incorporating two-factor authentication is highly recommended. This approach requires users to provide an additional form of verification beyond passwords. The article explores various 2FA methods, such as SMS codes, authentication apps, or bio-metrics, discussing their effectiveness in enhancing security and mitigating the risks of password breaches or theft.

3. **One-Time Passwords (OTP):**

One-time passwords offer an additional layer of security by generating unique codes for each transaction or login session. This section explains how OTP's work, their time-sensitive nature, and their resistance against replay attacks. It also explores the different methods of OTP generation, such as SMS, email, or dedicated mobile apps.

4. Bio-metric Identification:

Bio-metric authentication utilizes unique physical attributes, like fingerprints or facial features, to validate users' identities. The article discusses the advantages of bio-metrics, including their difficulty to replicate or forge. It highlights the integration of bio-metric authentication in mobile devices and payment apps, emphasizing the convenience and enhanced security it provides while minimizing the risk of credential theft.

V. ENCRYPTION TECHNIQUES

Encryption techniques play an important role in maintaining the security and privacy in digital payment systems. By applying many algorithms bland by doing so organizations can ensure the integrity, confidentiality, and authenticity of data during payment transactions. In this section, we will delve into the encryption techniques commonly utilized in digital payment systems, highlighting their significance in bolstering security and privacy.

A. SYMMETRIC ENCRYPTION

Symmetric encryption stands as a foundational encryption technique widely embraced by digital payment systems. It operates by employing a single secret key for both encryption and decryption processes. This shared key between the sender and the recipient serves to establish secure communication channels and safeguard sensitive data. Notable symmetric encryption algorithms commonly employed in digital payment systems include:

- AES (Advanced Encryption Standard):} AES is widely called a symmetric block cipher due to its effective performance and strong security measures. It supports key lengths of 128-bit, 192-bit, and 256-bit, providing a high level of encryption to ensure secure data transfer from one place to another.
- 3DES (Triple Data Encryption Standard):} On the other hand, 3DES uses the Data Encryption Standard (DES) algorithm by adding additional three consecutive encryption operations in a cascade. This approach enhances security by adding multiple layers of encryption to the data. While DES may be deemed relatively weak, the utilization of multiple encryption rounds within 3DES significantly bolsters security.

Symmetric encryption techniques enable the encryption of sensitive information, such as credit card details and transaction data, thereby guaranteeing its confidentiality and impeding unauthorized access.

B. ASYMMETRIC ENCRYPTION

Asymmetric encryption, also widely called public-key encryption, is an important technique used in digital payment systems. It operates using a pair of keys: a public key for encryption and a private key for decryption. While the public key can be freely shared, the private key is securely kept by the intended recipient. This approach ensures secure and unscathed communication between senders and receivers involved in digital transactions. The following benefits are provided by asymmetric encryption:

- Secure Key Exchange: Asymmetric encryption helps in the secure exchange of keys between senders and receivers involved in a transaction. This ensures that session keys or symmetric encryption keys can be securely transmitted over any network, providing excellent protection against eavesdropping and unauthorized access.
- Electronic Signatures: When ensuring the authenticity and integrity of digital price transactions, digital signatures are absolutely necessary. When a digital signature is created using the sender's private key, the recipient can use the corresponding public key to validate the signature.
- Confidentiality: Confidentiality is another crucial feature provided by asymmetric encryption, which allows data to be encrypted using the sender's public key. Only the intended recipient, possessing the private key, can decrypt and gain access to the information, which significantly improves its confidentiality and privacy.

Prominent asymmetric encryption algorithms commonly utilized in digital payment systems include:

- RSA (Rivest-Shamir-Adleman): RSA stands as a widely recognized encryption algorithm celebrated for its security and versatility in key exchange and digital signatures.
- Elliptic Curve Cryptography (ECC): ECC offers robust security while employing shorter key lengths compared to traditional algorithms. This feature makes ECC particularly suitable for resource-constrained environments.
- By implementing these encryption techniques, digital payment systems can fortify their security measures and safeguard sensitive data, ensuring a trustworthy and protected environment for payment transactions.

C. Hybrid Encryption

To harness the advantages of both symmetric and asymmetric encryption, hybrid encryption procedures are commonly utilized in digital payment systems. In this approach, symmetric encryption is used to encode the actual payment data, while asymmetric encryption is used to securely exchange and safeguard the symmetric encryption keys.

By combining these encryption techniques, digital payment systems can ensure secure and confidential transactions, safeguarding sensitive data from unauthorized access, alteration, and interception.

In conclusion, encryption techniques are vital components in addressing security and privacy concerns in digital payment systems. Symmetric encryption provides efficient and secure data transmission, while asymmetric encryption facilitates secure key exchange, digital signatures, and confidentiality. By employing hybrid encryption approaches, organizations can leverage the strengths of both techniques to enhance the security and privacy of digital payment transactions, thereby building trust and safeguarding sensitive information.

VI. Fraud Detection and Prevention

Fraud detection is to take care of transaction occurring through internet. There are security concerns like unauthorized access is where person who does have any rights on platform access the platform like hackers and cyber criminals employ techniques like phishing and denial of service. Data breaches can happen when system is under control of attacker/ compromised, which attackers can get access to personal information like credentials . malware/ransomware will also cause a threat which can take control of victim's system.

Privacy concerns like data collection from user ensures that user on platform are legitimate. This can be ensured by collecting necessary details like transnational details, device information which are necessary for prevention and detection of frauds. Data security should be implemented so user's data is in tact so attacks on data is detected. secure storage devices, encryption can help data security. user should be consented for which data is collected from them so they understand why those data are collected. Data retention policies should be know to user and it is ethical role of data collectors to dispose data. User should have right to see, access, and update data collected by them to the platform.

Few measure are taken to prevent are Multi factor authentication and real time monitoring. Two factor authentication adds one more step on entering password which user know and user were asked to link something like email or phone number which are belonging of user, where it significantly reduces the unauthorized user into someone else account. conventional method like entering password is vulnerable to phishing, brute force attack or social engineering. In Two factor authentication, first part is user password or user pin that user knows and want to keep it secret but the problem password faces is that is can be easily compromised using phishing or key logging. It can be easily figured out by cybercriminal. Second part of Two factor authentication is thing which user owns and can be used to get entry to the platform. Commonly used factors are OPT, Notification sent to user phone. OTP (one time password) is sent to user's phone app, text or email which user can enter after entering password which send the second factor to you.

Real time monitoring tracks transaction currently happening over network or continuous monitoring of transaction either by collecting location, amount, user behavior. Key components of real time monitoring is transaction monitoring which use machine learning algorithm to analyze transaction. It includes velocity checks, outlier identification which helps to understand any behavior which is abnormal. Collects data from multiple sources where it includes data lie customer information, organization information which helps in fraud detection. Behavior analysis tries to read the history of user's transaction to verify their previous behavior and current behavior to identify any potential fraud and makes it easy to prevent it. Network monitoring is key component of real time monitoring where not only user's profile is monitored to prevent fraud but entire network is monitored to identify any distributed denial service of attack or any system breaches. But one more thing to remember is apart from the above key components constant improvement to identify new malware, new machine learning algorithms to analyses network or user

profile should be discovered to mitigate new fraud and prevent it from occurring.

VII. SECURE TRANSACTION PROTOCOLS

Encryption plays a crucial role in different applications, http is an extension it will add encryption for authentication laters. it will creates secure communication between client and server, it allows platforms exchange all the data during transactions through the network. encryption is a fundamental concept in modern cryptography. it will converts the data into unreadable form called cipher text. Symmetric key encryption is also called as secret key encryption. the employs shared a single key for the both encryption and decryption process. it will encrypts the large amount of data. asymmetric key is also known as public key encryption, the public key is freely distributed and used for encryption. private key is use for decryption, a sender can send a message using their private key, It is an authentication protocol developed by major payment card networks. It provides an extra layer of security for online card transactions. It allows the card holder's identity to be verified by providing an additional authentication step during the payment process. This protocol may use of combination of cryptography techniques and dynamic data exchange between the card holders. It helps to make the secure transactions. It reduces the danger card fraud attacks and improves the security of digital payments. It will add extra authentication to the payment process often mentioned as 3d secure authentication. it involves the three steps they are the issuer domain, the acquirer domain, the interoperability domain. when a card holder begins a online payment transactions, the merchant's website initiates the 3Ds process.

Tokenization is a technique during digital transactions it will substitute the sensitive card payment with unique tokens, it is a highly effective technique, and it offers a powerful solution by replacing sensitive data with unique tokens. tokenization offers various advantages for digital payments. it significantly reduces the risk and unauthorized access to sensitive payment card information, it enhances the security of data transmission during digital payment transactions. tokens are used as actual payment card data, the risk of compromising the data during transmission is greatly mitigated. Tokenization has become an accepted and widely adopted security measure in digital payment systems. it includes mobile payments, E-commerce, and recurring billing. By protecting critical payment card data and minimizing the possible effects of data breaches, it improves the overall security posture.

It is an advanced security measure, Bio-metric authentication utilizes special physiological such as face recognition, finger prints. It is used to verify the identity during digital payment transaction. It will provide high level security of data. When bio metric authentication is used during the payment process, Unauthorized access risk can be minimized. It will protect the sensitive information. The user's payment account is connected to their bio metric data through bio-metric authentication. when starting a transaction the user is to provide their bio-metric sample.such as putting their finger on a fingerprint. It will offers several advantages for digital payments Users are no longer required to type or remember complicated PIN's or passwords. Instead, users may easily and rapidly authenticate themselves using their bio-metric traits, which are essentially individual to them. Replication of bio-metric authentication is challenging. Bio-metric traits are intrinsically linked to the individual and are therefore impossible to copy or transmit, in contrast to passwords that can be lost, stolen, or exchanged. if offers a highly secure and convenient method for verifying the identity of users in electronic payment exchanges. It improves security, lowers the possibility of unwanted access, and offers a user-friendly experience by utilizing special bio-metric traits. Bio-metric authentication is anticipated to play a bigger part in the future of secure digital payments as technology develops and bio-metric systems continue to advance. It is critical to address the security threats posed by these platforms given the growing use of mobile devices for digital payments. The secure storing of payment credentials, data encryption during transmission, and defense against malware and illegal access are the main concerns of secure transaction protocols for mobile devices. Some of the approaches used to strengthen the security of digital payments on mobile devices include mobile-based authentication apps, secure components, and device fingerprinting. It is concerned with safeguarding the data saved on the device. It helps to secure data by transforming it into an unreadable format that can only be viewed with a decryption key. It encodes the sensitive payment data store on the device. The information is still shielded from unwanted access. Application developers overview the Secure app development standards are essential for keeping mobile devices secure coding practices, conduct testing and include strong security measures into their applications. the apps should utilize encryption Implement safe authentication procedures for data transmission, and overview to industry security requirements. It includes secure network connections when connecting public networks like Wi-Fi, the user must be aware this network Eavesdropping and man-in-the-middle attacks are possible. use VPN network, it will establish secure and encrypted networks. It will protects the confidential data transmitted over the public network. It includes secure network connections when connecting public networks like Wi-Fi, the user must be aware this network Eavesdropping and man-in-the-middle

attacks are possible. use VPN network, it will establish secure and encrypted networks. It will protects the confidential data transmitted over the public network. Device authentication and user awareness are all examples of mobile device Mobile devices may be trusted platforms for completing secure digital payment transactions while protecting sensitive payment information and user privacy by applying strong security measures.

VIII. EMERGING TECHNOLOGIES

Digital payment systems continue to develop new technologies are being created to improve user ease, experience, and efficiency however . It will explore some emerging technologies like that aims to address the concerns and it will improve the security and privacy in digital payment systems. Tokenization is a technology, it replaces the sensitive data such as Credit card numbers, for example, can be replaced with unique tokens. Tokens are generated random there is no relationship between the original data, If an unauthorized entity intercepts the message. Tokenization can help digital payment systems limit the danger of disclosing sensitive information during transactions it enhance the security and privacy. using the bio-metric authentication technology such as facial recognize and fingerprint, it will add an extra layer of security for digital payment system. By utilizing distinct biological traits, these technology can verify the user identity with high level precision. Block chain is technology, this technology is originally developed for crypto-currency like bitcoin. has gotten a lot of attention because of its potential to change digital payment methods. It decentralize the nature enhances security and privacy. Block chain transactions are verified and it can not be altered, by providing the robust frame for secure and digital payments.

Artificial intelligence is a technology, AI is used for fraud detection system with the help of machine learning algorithms, it is used to analyze huge amount of transaction data and used to identify the fraud relevant activities. These algorithms may learn and adapt to new fraud patterns in real time, increasing their accuracy over time. digital payment system in AI can detect proactively and prevent fraud transactions, ensuring the security and privacy of users' financial information. Machine learning algorithms can continuously analyze and process the data. They are improving their comprehension of normal and deviant transaction behavior. It enables AI systems to keep up with emerging fraud tactics. Increasing their effectiveness in detecting and preventing fraudulent transactions.

IX. CONCLUSION

Finally the security and privacy problems in digital payments are substantial and must be addressed Because security threats such as Trojans and phishing attacks are becoming more sophisticated, continues prevention measures and required user knowledge. It includes mechanisms like authentication, passwords-based and bio-metric methods plays an important role to verify the user identity and reduced unauthorized access. some of encryption techniques like symmetric and asymmetric encryption During transactions, maintain the confidentiality and integrity of sensitive data. Tokenization protects card information effectively while developing emerging technologies like block chain and Artificial intelligence contribute to improving the security and privacy of digital payment systems. Continuous research and development in these areas is critical for staying ahead of developing security risks and assuring the reliability and security of digital transactions.

X. REFERENCES

[1] Saxena, Sameer, et al. ”Survey on online electronic payments security.” 2019 Amity International Conference on Artificial Intelligence (AICAI). IEEE, 2019..

[2] Khando, Khando, M. Sirajul Islam, and Shang Gao. ”The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review.” Future Internet 15.1 (2022): 21.

[3] CEIC Data, (2023), Mobile Payments in India [Screenshot], Retrieved from https://www.ceicdata.com/en/india/mobile-payments

[4] Wang, Yong, Christen Hahn, and Kruttika Sutrave. ”Mobile payment security, threats, and challenges.” 2016 second international conference on mobile and secure services (MobiSecServ). IEEE, 2016.

[5] Alzoubi, Haitham M., et al. ”Cyber Security Threats on Digital Banking.” 2022 1st International Conference on AI in Cybersecurity (ICAIC). IEEE, 2022.

[6] Hassan, Md Arif, and Zarina Shukur. ”A secure multi factor user authentication framework for electronic payment system.” 2021 3rd International Cyber Resilience Conference (CRC). IEEE, 2021.

[7] Xia, Huosong, et al. ”Knowledge acquisition model of mobile payment based on automatic summary technology.” Electronic Commerce Research (2022): 1-24.

[8] Ali, Guma, Mussa Ally Dida, and Anael Elikana Sam. ”Two-factor authentication scheme for mobile money:

A review of threat models and countermeasures." Future Internet 12.10 (2020): 160.

[9] Chen, Chunyan. "Discussion on the Security Mechanism of Mobile Payment." 2021 7th Annual International Conference on Network and Information Systems for Computers (ICNISC). IEEE, 2021.

[10] Lal, Nilesh A., Salendra Prasad, and Mohammed Farik. "A review of authentication methods." vol 5 (2016): 246-249.

[11] Sun, Jiabin, and Nan Zhang. "The Mobile payment based on public-key security technology." Journal of Physics: Conference Series. Vol. 1187. No. 5. IOP Publishing, 2019.

[12] Ahmed, Waqas, et al. "Security in next generation mobile payment systems: A comprehensive survey." IEEE Access 9 (2021): 115932-115950.

[13] Seera, Manjeevan, et al. "An intelligent payment card fraud detection system." Annals of operations research (2021): 1-23.

[14] Diadiushkin, Alexander, Kurt Sandkuhl, and Alexander Maiatin. "Fraud detection in payments transactions: Overview of existing approaches and usage for instant payments." Complex Systems Informatics and Modeling Quarterly 20 (2019): 72-88.

[15] Ishak, Norhamiza. "Overview of cashless payment in Malaysia." International Journal of Accounting, Finance and Business (IJAFB) 5.27(2020): 11-18.

[16] Urs, Bogdan-Alexandru. "SECURITY ISSUES AND SOLUTIONS IN E-PAYMENT SYSTEMS." Fiat Iustitia 1 (2015).

[17] Dijesh, P., SuvanamSasidhar Babu, and Yellepeddi Vijayalakshmi. "Enhancement of e-commerce security through asymmetric key algorithm. "Computer Communications 153 (2020): 125-134.

[18] Bangera, Srishti, Pallavi Billava, and Sunita Naik. "A hybrid encryption approach for secured authentication and enhancement in confidentiality of data." 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2020.

[19] Moon, Iffath Tanjim, et al. "Towards the advancement of cashless transaction : A security analysis of electronic payment systems." Journal of Computer and Communications 10.07 (2022): 103-129.

[20] Ximenes, Agostinho Marques, et al. "Implementation QR code biometric authentication for online payment." 2019 International Electronics Symposium (IES). IEEE, 2019