Investigating Cybercriminal Strategies and Fraud Types in Modern Digital Payment Platforms

Pooja Solanki
Institute of Computer Science, Samrat Vikramaditya Vishwavidyalaya Ujjain, India

Ramji Yadav
Institute of Computer Science, Samrat Vikramaditya Vishwavidyalaya Ujjain

Umesh Kumar Singh
Institute of Computer Science, Samrat Vikramaditya Vishwavidyalaya Ujjain

ABSTRACT
The quick uptake of online digital payment systems contributed to a revolution in finance and financial dealings, providing never before seen convenience but at the same time, higher vulnerability to advanced cybercrime. The paper looks at the various types of fraud found in the modern digital payment systems and how cybercriminals have applied their tricks in exploiting the vulnerabilities in systems. The study undertakes both a quantitative and qualitative study, corporations outlined instances of frauds, technical flaws, and trends of action of the users to derive useful typologies of deceits, such as phishing, identity theft, account hijacking, and manipulating transactions. The paper also discusses the evolving practices of the cybercriminals, including; social engineering, malware exploitation and usage as well as exploitation of cursory authentication processes. There are some hints of an ensemble of technical vulnerabilities, human factor, lack of control over this problem to develop frauds on a great scale. The outcomes show that there exists a pressing need to introduce stronger cyber security tools and prompt fraud detection tools and user education to minimize risks. It is a well-developed study guiding comprehensively the nature of the e-frauds to schemes of cybercrime that would be valuable to financial service providers and policy-makers in the pro-active defence schemes. The article highlights the importance of creating an integrative approach to unite the technology, policy and user education to facilitate digital payment systems to withstand any emerging threats in the future.

Keywords
Digital payment fraud, Cybersecurity, Phishing, Identity theft, Account takeover, Social engineering, Fraud detection.

1. INTRODUCTION
The digital revolution has significantly transformed the way financial transactions are conducted, making payments faster, more convenient, and widely accessible through mobile wallets, internet banking, peer-to-peer payment systems, and contactless card technologies. The increasing adoption of smartphones and improved internet connectivity has led to a substantial rise in online transactions across the world. While these digital payment systems provide efficiency and enhanced user experiences, they have also created new opportunities for cybercriminals to exploit users and financial institutions. As technology and finance become increasingly interconnected, the digital payment ecosystem has become both highly efficient and vulnerable to sophisticated cyberattacks.

Digital payment fraud has emerged as a major concern in this rapidly evolving environment. Common forms of fraud include phishing, identity theft, account takeover, unauthorized transactions, transaction manipulation, and malware-based intrusions. Cybercriminals exploit both technical vulnerabilities and human behavior through social engineering techniques, making fraud detection and prevention increasingly challenging. Unlike traditional financial fraud, cyber fraud relies on interconnected computer networks and can be conducted across borders, which complicate monitoring, investigation, and prosecution. The anonymous and global nature of digital payment systems further increases the difficulty of controlling these fraudulent activities.

To address these challenges, financial institutions and regulatory agencies are adopting stronger security measures such as encryption, biometric authentication, blockchain technology, and AI-based fraud detection systems. However, implementation remains uneven across different regions, especially in developing economies. Existing research often focuses separately on technical security mechanisms or user awareness, leaving a gap in understanding how technological vulnerabilities, human error, and criminal strategies interact. This study aims to classify digital payment frauds, analyze the methods used by cybercriminals, identify the factors that contribute to successful attacks, and propose a balanced framework that combines technological safeguards, regulatory policies, and user awareness programs to reduce fraud risks and strengthen the security of online payment systems.

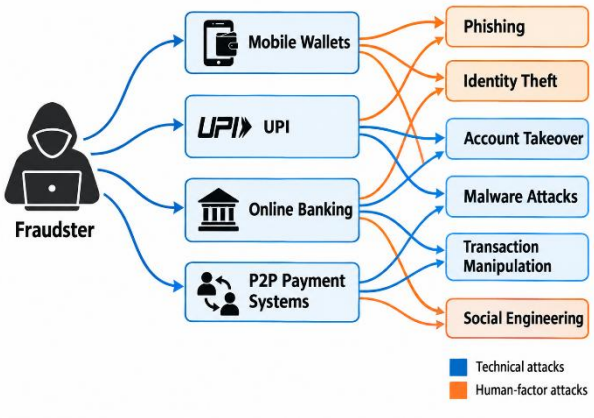


Fig1: Overview of Digital Payment Fraud Landscape

2. RELATED WORK
The growing number of online payment system has caught the attention of numerous scholars keen on carrying out a study in cybercrime and fraud detection. Kamblea et al. [1] emphasized the importance of digital-based tools in identification and reaction towards cybercrimes. In their work, special focus was made on forensic methodologies, such as data preservation, evidence collection, and post incident analysis as methods of

effective investigation of digital financial frauds. Providing a general overview of forensic tools, the authors have already demonstrated that mentoring investigative activities are essential in order to identify and convert criminal minds to justice.

Ramani [2] presented a broad overview of the digital payment systems, its design, working principles and its vulnerability. This paper has brought out the quick proliferation of the electronic payment systems, and even security breach due to feeble authentication scheme and phishing transactions and fraudulent transactions. Likewise, Malik et al. [3] implied the significance of successful prosecution when taking advantage of the digital forensic evidence. They have indicated that not only was the use of technological equipment a means to ensure successful legal processes, but the correct attitude towards evidence, loyalty to the standards of the process adopted during the course of investigation and trial.

Acharya et al. [4] applied the e-payments systems in the real-life context by asking that, whether the technologies would be deployed to the hype and the reality of the user. Most of their work is in unison over the fact that even though this has been widely accepted, the majority of systems are yet to be resistant to cyber threats owing to the low level of security, and unawareness by the users themselves. A survey carried out by Priya and Ahmed [5] on progress of security in digital payments in the recent past with a focus on the recent threats like malware, ransomware and social engineering attack. They have shown new solutions, such as multi-factor authentication and real-time system to identify fraud and research blue oceans in integrating human and technology protection aspects of behavior.

The comparative analysis of the roles the digital forensic investigators that are presented by Singh et al. [6] showed that standardized approaches need to be considered to make the process of examining a digital crime scene both standardized and objective. This method is a way of supplementing the research done by Sharma and Sundararajan [7], who investigated the epidemiology of cybercrime on the UPI transactions carried out in India. Their results showed that because of fast digitalization and the high amount of transactions, there is a chance of becoming a victim of fraud, especially in cases where the vulnerability of the system and the irresponsibility of the user overlap.

A systematic literature review known as hyperlink fraud in electronic payment systems was carried out by Saha and Saha [8]. In their study, they have observed that there has been more usage of URL-based deception and phishing by attackers to defraud users and steal transactions. Topicality of cyber forensics to the investigations of the criminal cases was thus established by Singh and Rajpurohit [9], although they revealed the problems of the procedures, legal and technical specificities of the case that should be examined in order to discover the most appropriate evidence. To facilitate efficiency of investigating cyber fraud Hidayati et al. [10] suggested the conceptual model that enables the introduction of detecting mechanism, workflow models, and procedure regulations to maximize efficiency of the entire process.

The authors of Shahzad et al. [11] have explored existing models of digital forensics that specifically discuss digital payments, and identified major gaps of future aging interoperability and new age trends of fraud. Yet another model of forensics expounded by Lau et al. [12] points out the value of mobile payments wherein real time data collection and irregularity detection is used in an effort to mitigate risks brought about by mobile financial environment. Zia and Ali [13] and Shaikh and Singh [15] conducted studies in their respective papers discussing hyperlink fraud in e-payment systems, vectors of attacks, detection measures and prevention measures. Their publications mostly dwell on the upward trend in the cybercriminal activities, and the pressing need to use proactive forensic initiatives.

Lastly, Arora and Singh [14] suggested an inclusive guideline to study cybercrimes in online payment systems. Their paradigm takes into consideration the factors of technology, procedure and regulation to respond to the-evolving threat environment. In these analyses, a remarkable pattern stands out, that, although there is a tremendous presence of numerous frameworks and instruments that can be deployed to perform a digital forensic investigation, there exist still lapses in the translation of technical solutions, policing and preventive measures geared towards the user. This is why the current study encourages the systematic mapping of cybercrime activities towards certain types of fraud in order to seek a comprehensive coverage of how to secure digital payment systems today.

3. METHODOLOGY

3.1 Research Design

This research was a mixed study aiming to explore strategies in cybercrime and the types of fraud in contemporary digital payment methods in capturing the qualitative and quantitative nature of digital payment fraud. This was done in a way that multiple data sources were involved e.g. case-studies, literature reviews, incident reporting, surveys so that the topic would be thoroughly comprehended. Through the combination of such-algorithms, the study attempted to triangulate their results and present meaningful ideas of how cybercrime operations, not mentioning how these systems are vulnerable to attacks. It has enabled the assessment of not only real-life scenarios, but also conglomeration of current academic and technical data to give a complete picture that encompasses both of the technical, behavioral and regulatory aspects of the online fraud.

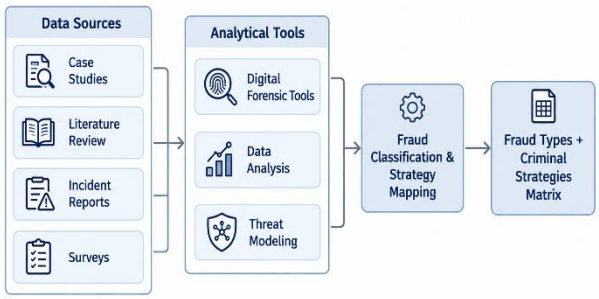


Fig 2: Methodology Workflow

3.2 Data Collection

a) Case study

The case studies were picked to analyze the example cases of high-profile cyber fraud in India, Europe and the United States that occurred in the past decade. The cases were analyzed to see how attacks were executed, weaknesses were used as well as the investigations by the authorities involved. There was also clear information on the various types of fraud, patterns of attack as well as methods used by Al-Qaida so that workings of various cases could be compared and contrasted. This provided them with the opportunity to correlate these data on the variations on cybercriminal activity and their modes of operation that are usually observed by succession in perpetrating fraud. Through studies of these real-world scenarios, the

research was in a position to put the technical results into a contextual situation.

b) Literature Review

The secure digital payments, the models of cybercrime and forensic investigation were also reviewed in a thorough literature review of peer-reviewed journal articles, conference proceedings and technical reports. The aim of the review was to establish the presence of existing methodologies, interventions that use technology and reported typologies of fraud and gaps in knowledge are available. A particularly keen attention was drawn to those works that included both technical and behavioral methodologies that would also enable them map a scheme of a typology of forms of fraud and methods used by cybercriminals. This generalization of the literature available facilitated the analysis scheme and mapping plans of attacks to fraud.

c) Incident Report

Financial institutions, cybersecurity organizations, and government agencies were reported on the incidents to get empirical knowledge of fraudulent activities. These were detailed reports like, abnormalities of transactions, phishing, account decolonization among others of digital payment frauds. A methodical examination was conducted which established trend in rates of frauds, targets to be chosen and leverages that was to be obtained. The incident reports were used to complement the case studies and literature review to identify the predominant patterns and appearance of threats to discover the common patterns and emerging threats of the operational environment of cybercrime.

d) Survey

Practitioners and technicians of the financial services industry and users of the digital payment systems, IT specialists and stakeholders (employees and managers of financial services companies) were also given structured questionnaires to complete. The opinions on the system vulnerability, awareness concerning cyber threat and personal experience of fraudulent transactions were captured in the surveys. Data gathered via the surveys was used to corroborate outcomes of the case studies and the literature review to ensure that trends in cybercriminal activities are aligned with realistic realities to which end-users and institutional players are subjected.

3.3 Analytical Tools

The analytical software was used to analyze the logs of the transactions in order to trace the fraudsters and reconstruct the attacks sequences. Pattern recognition techniques and descriptive statistical techniques were used in order to find correlations between the types of fraud and the strategies, which have been used by cybercriminals. Also, threat model-driven schemes would be employed to conduct comprehensive vulnerability analysis on digital payment mechanism, and to pre-empt the potential of attack vectors. By these analysis tools, the trends of the cybercriminals could be plotted in a systematic way in relation to a given type of fraud archetypes and on this basis effective insights could be generated in order to detect and prevent such archetypes of frauds.

3.4 Criteria for Fraud Classification and Strategy Mapping

The types of fraud were categorized by the type of attack e.g. phishing, malware, account takeover, and by area of attack e.g. mobile applications, web portal or banking infrastructure. The three approaches of cybercriminals (technical implementation, social engineering, and exploiting vulnerabilities in the systems) were categorized. Based on these criteria, a matrix was drawn between types of fraud and related criminal strategies that allows them to make a pattern, identify similarities and common vulnerabilities in various clinical incidents.

3.5 Ethical Considerations

The research was done in an ethical manner. All the sources of data were anonymized to provide their privacy to the individuals and organizations. The surveys informed the participants that they were taking part in the survey and provided them with voluntary participation and their rights such as the right to withdraw. The confidential information of the case study and incident reports was rightly handled and the overall findings were provided. The study has complied with institutional ethics of conducting research, and has not violated the laws on data protection and privacy.

4. CLASSIFICATION OF DIGITAL PAYMENT FRAUD TYPES

4.1 Phishing

The phishing attacks are done to deliver the suspect emails, SMS or Web sites in order to fool the users into giving worthy information, like a login account or payment card details. Phishing is considered to be one of the most prevalent e-frauds of digital payments since it is aimed at users of mobile banking and e-wallets. The recent attack in India signified how phishing attacks have had an impact on various UPI accounts that have led to unnecessary transactions.

4.2 Identity theft

One such crime is identity theft whereby a computer criminal gains and utilizes personal information of an individual with the intention of opening fraud accounts or carrying out money transactions. Phishing or social engineering is normally employed together with identity theft by attackers to achieve requisite information. The ones which lack effective real-time verification systems get affected particularly and the thieves can get away using the stolen identities before it is detected.

4.3 Account Takeover (ATO)

Account takeover is any unlawful method of an authorized access of an account, most of the time most people access accounts through hacked passwords or virus programs. Immediately they get access, attackers will be able to run the transactions, send money, or edit the account settings. Malicious attackers tend to attack online banking sites especially when these sites lack multi-factor authentication or when they are weakly secured in terms of authentication. The number of ATO incidents has skyrocketed with a quick uptake of digital wallets and UPI in the COVID-19 pandemic.

4.4 Malware Attacks

Malware attacks such as mobile phones, computers and bank server are aimed at the devices and information infrastructure comprising of digital payment. Keyloggers, trojans and

spyware intercept sensitive data, or disrupt a transaction process. Malware can be implemented along with phishing/social engineering to make it more effective. Indeed, in a few instances, mobile malware has been masqueraded as legal banking software that has stolen colossally in Asia and in Europe.

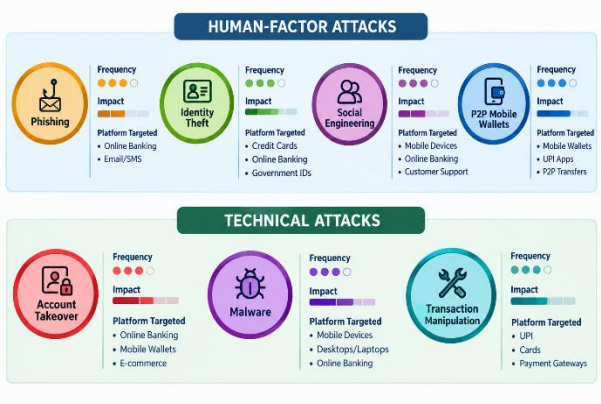


Fig 3: Classification of Digital Payment Fraud Types

4.5 Transaction Manipulation

There is transaction manipulation; fraud on transactions where a valid one is illicitly managed in either value or redirected funds or a system malfunction. The vulnerability is exploited by attackers in the procedures of carrying out transactions or on the internal financial controls. Although the manipulation of transactions is not widespread as phishing or malware, it can cause an enormous loss and functioning outage.

4.6 Social Engineering

Social engineering takes advantage of human psychology, and not technical vulnerabilities. The attackers pretend to be bank officials, people in the customer care or trusted persons to urge the user into providing confidential information and executing transactions. Social engineering is also quite diverse and is normally employed together with other types of attacks.

4.7 Statistical Trends and Illustrative Examples

Included in the reported frauds detected through analysis, phishing and account takeover show the most prevalence of digital payment frauds, as well as identity theft and malware attacks. Manipulation of transactions and social engineering is less prevalent but there is the opportunity to make decisions in regard to bigger losses. Within the UPI, mobile wallets and online banking websites case studies it is apparent that the attackers in most instances would employ a combination of several strategies to enhance the likelihood of their success. Such categorizations aid in comprehending the design of cybercriminals to specific kinds of fraud and teaches of the development of specified countermeasures decisions.

5. CYBERCRIMINAL STRATEGIES

5.1 Phishing and Credential Harvesting

One of the most prevalent techniques of online payment fraud has been phishing. Attackers generate the spoofed mail, SMS messages or spoofed Web sites which mimic the genuine finances services, SMS messages or institutions and payment services. The users will be blackmailed to give personal information such as login passwords, OTPs or credit cards. Multi-channel approach and targeted messages are more likely to be used in the phishing programs present in the day as they can prove more effective to ensure more users comply. These attacks are often a way of preceding identity theft or account takeover.

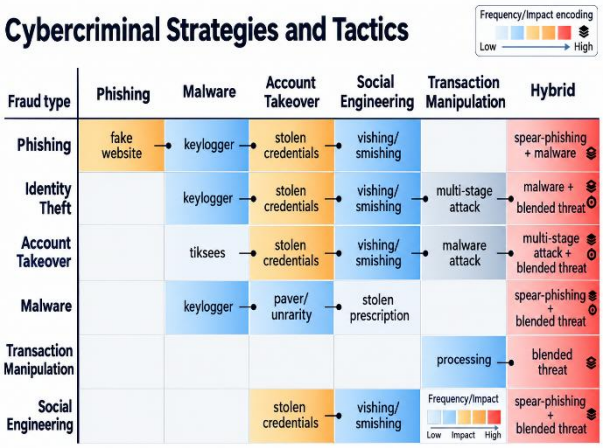


Fig 4: Cybercriminal Strategies and Tactics

5.2 Malware Deployment

Attack fermented by malwares is an important approach towards hacking into gadgets and stealing sensitive information. This includes the trojans, spyware and key loggers that follow the user actions and steal their transactions. Particularly weak areas will include mobile payment applications; rogue applications may masquerade as the legitimate applications. Upon being installed, malware may modify the transaction flow and operate silently and steal massively.

5.3 Account Takeover (ATO)

Account takeover is where stolen credentials are used to access user accounts without proper authorization or hijacking of a session. Attackers can initiate a fraudulent deal, modify account settings or even transfer money. Phishing or social engineering acquired information, ineffective authentication processes and foreseeable passwords are frequently used. The majority of victims of ATO attacks are online banking and online wallet.

5.4 Social Engineering

Social attacks are anchored on the psychology of man and not inadequacies on the technical front. They can also pretend to be bank personnel, customer care/service providers or even someone close to the heart of their life to scare them into providing confidential information or executing deals that were not expected to be done. Phishing and malware are often employed along with this strategy to make it more effective and therefore, diverse and long-lasting.

5.5 Transaction Manipulation

The targets of transaction manipulation are either the manipulation of valid transactions or legal weaknesses of the procedures used in the payment systems. The attackers can alter the values to the transactions, re-directing funds or taking advantage of loopholes in the authorization loopholes. Not so noticeable as phishing or malware, transaction manipulation can be traced to a big loss in finances and operational accidents in the workplace. It entails intricate expertise of the target system.

5.6 Hybrid and Multi-Vector Approaches

Hybrid techniques are a combination of one or more than one attack technique involving phishing, malware, social engineering as well as transaction manipulations as far as possible to improve the likelihood of success. An example will be phishing where one can acquire credentials that the attackers will use to employ malware that is used to stalk the users to operate on the continuum of access. There is an increase in the use of multi-vectors, particularly in mobile wallets and UPI platforms and this is the indication that cybercriminal actions are high-tech.

5.7 Emerging Trends in Cybercriminal Strategies

The most difficult part is that the new schemes take advantage of the mobile wallets, peer-peer payments and systems of fast money transfer in which a big number of transactions will give the chance to commit the real-time fraud. The automated concept, the use of botnets, and artificial intelligence are all on the increase where cybercriminals attack several accounts simultaneously. Knowing about these dynamic strategies is critical in developing proactive fraud detection systems, instituting powerful security systems, and making users aware about preventive measures.

6. MAPPING FRAUD TYPES TO CRIMINAL STRATEGIES

6.1 Phishing and Identity Theft Correlation

Phishing is also related with identity theft, which scammers apply personal data, including the log in details, credit cards or OTPS, by means of sending emails, SMS messages and websites that include foul play. It is also possible that this technique might be a prelude to other types of fraud like account takeover that may enable cybercriminals to gain unauthorized access to user accounts. The mapping analysis shows that phishing is best served in terms of where the least sophistication on cybersecurity is perceived by the users and where no multi-factor authentication is found to be in applicable use.

6.2 Account Takeover (ATO) Strategies

The form of attacks that are mostly applied in account takeover attacks is the stolen credentials and the session hijacking. The combination of phishing, malware, and social engineering can be used by a fugitive to gain access to legitimate accounts of the user. Pattern mapping illustrates that organizations are at a high risk of success in ATO attacks because of weak passwords, easy to answer security questions and slow security check systems. Internet and mobile wallet banking services are particularly susceptible because of a high volume of transactions and inability to track them in real-time.

6.3 Malware and Transaction Manipulation

Malware programs attack is highly linked with manipulations that occur in transactions since the programs can intercept the keystroke, access the financial information and alter the transaction flows. Malware is common with phishing and social engineering to gain access to the account or divert funds by the attacker. Manipulation of transactions or accounts takes advantage of technical flaws or flaws in procedures in payment systems and illustrates that moulded strategies using malicious programs as well as exploitation of systems are becoming more prevalent in advanced types of cybercrimes.



Fig 5: Mapping Fraud Types to Criminal Strategies

6.4 Social Engineering Linkages

Phishing, identity theft and account takeover social engineering methods are of various types of fraud. Hackers may bypass the protective features of technology by fraudulently accessing confidential information or permitting the transaction to be made by winning over human trust. Mapping researchers state that social engineering tends to become enabling tool and complement to other tricks of strategies and overall success of fraud activities.

6.5 Hybrid and Multi-Vector Approaches

There is an increase in the phishing, social engineering and transaction manipulation hybrid attacks that use malware. Mapping analyses show that these multi-vector strategies allow to increase the success of the attacks to the maximum by enlisting the support of technical as well as human vulnerabilities. The emergence of the hybrid attacks is a statement in itself of the necessity to approach the issue of security in multi-pronged approach, involving technical measures of protection of the system and educating and training the users.

6.6 Insights on Attack Patterns and Vulnerabilities

The diagrammatic presentation of the nature of fraud as per the techniques of the crimes illustrates the clear patterns and recurrents lapses. Phishing and malware along with social engineering are the most multi-tasking strategies that form the basis of various kinds of fraud. Frequently they are accompanied by an account takeover and modifying transactions, which accounts to the multifaceted and advanced elegance of cybercriminals. These correlations help financial organizations and the relevant regulatory bodies to concentrate on monitoring and implement certain defenses and educate users on safety strategies.

Table 1: Mapping Digital Payment Fraud Types to Criminal Strategies

Fraud Type	Phishing	Malware	Account Takeover	Social Engineering	Transaction Manipulation	Hybrid/Multi-Vector
Phishing	High Freq / Medium Impact	Low Freq / Medium Impact	Medium Freq / High Impact	High Freq / High Impact	–	High Freq / High Impact

Identity Theft	High Freq / High Impact	Medium Freq / Medium Impact	Medium Freq / High Impact	High Freq / High Impact		Medium Freq / High Impact
Account Takeover	Medium Freq / High Impact	Medium Freq / High Impact	High Freq / High Impact	Medium Freq / Medium Impact		High Freq / Very High Impact
Malware Attacks	Low Freq / Medium Impact	High Freq / High Impact	Medium Freq / High Impact	Medium Freq / Medium Impact		Medium Freq / High Impact
Transaction Manipulation		Low Freq / Medium Impact	Medium Freq / High Impact		Medium Freq / Very High Impact	Medium Freq / High Impact
Social Engineering	High Freq / High Impact	Medium Freq / Medium Impact	Medium Freq / High Impact	High Freq / High Impact	–	High Freq / High Impact

7. CONCLUSION AND FUTURE WORK

The systems of digital means of payment are the future of financial transactions, but has contributed to making it more vulnerable to cybercriminals due to the accelerated process. This paper has described the landscape of digital payment fraud, and in a descriptive way, has subdivided the major types of frauds documented, which include phishing, identity theft, account takeover, malware attacks, manipulation of transactions in an account and social engineering and overlaid against the tools available to the outlaws of cyberspace. The results show that phishing, social engineering, and hybrid attacks have the most diverse strategies and often are the foundation of various types of frauds. The combination with malware attacks, although less common, still exists in the form of account takeover, and transaction manipulation, yet the cost ramifications of such attacks are higher. With the help of the mapping system, it is possible to understand the patterns of attacks, the vulnerability of the most common, and the correlation of technical defects with humans, which could be employed to prevent a case of fraud, educate and research the user, and conduct a forensic analysis.

Future efforts need to concentrate on implementing real-time monitoring structures together with artificial intelligence and machine learning to forecast and avert new trends in fraud. Of huge importance will be the development of dynamic security that will be adjustable to the ever-changing strategies of online offenders to address the threats in dynamic platforms of online payments. Additionally, how effective user-centric interventions (e.g., behavioral nudges and awareness campaigns) are in making people a bit more resistant to social engineering attacks and phishing attacks can be learned. The cross-jurisdictional work can potentially contribute to the existing knowledge about cross-border fraud patterns and educate a consistent risk regulation. Technological innovation, policy solutions, and human.

8. REFERENCES

[1] D. R. Kamblea, N. Jain, and S. Deshpande, “Cybercrimes Solutions using Digital Forensic Tools,” *Wireless and Microwave Technologies*, vol. 6, pp. 11–18, 2015, doi: 10.5815/ijwmt.2015.06.02.

[2] S. Ramani, “Reviews on Digital Payment System,” *International Journal of Computer Sciences and Engineering*, vol. 6, Special Issue 11, pp. 88–92, 2018.

[3] A. A. Malik, E. M. Asad, and W. Azeem, “Effective Prosecution to Support Digital Forensic Evidence during Investigation and Court Proceedings,” *Electronic Crime Investigation (IJECI)*, ISSN: 2522-3429 (Print), ISSN: 2616-6003 (Online).

[4] V. Acharya, S. O. Junare, and D. D. Gadhavi, “E-Payment: Buzz Word or Reality,” *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 3S2, 2019.

[5] N. Priya and J. Ahmed, “A Survey on Digital Payments Security: Recent Trends and Future Opportunities,” *International Journal of Computer Trends and Technology*, vol. 69, no. 8, pp. 26–34, 2021.

[6] K. S. Singh, A. Irfan, and N. Dayal, “Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks,” in *Proc. 2019 4th Int. Conf. Information Systems and Computer Networks (ISCON)*, Mathura, India, 2019.

[7] A. Sharma and A. Sundararajan, “Cybercrime and the Use of Digital Payment Systems: Evidence from UPI in India,” *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3350079.

[8] S. Saha and S. K. Saha, “Forensic analysis of hyperlink fraud in digital payment systems: A systematic literature review,” *Journal of Cybersecurity and Mobility*, vol. 10, no. 3, pp. 311–331, 2021.

[9] V. Singh and V. Rajpurohit, “Role of cyber forensics in criminal investigation,” *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 3, no. 6, pp. 170–175, 2022.

[10] A. N. Hidayati, I. Riadi, E. Ramadhani, and S. U. Al Amany, “Development of conceptual framework for cyber fraud investigation,” *Journal of Critical Reviews*, vol. 7, no. 2, pp. 125–135, 2021.

[11] F. Shahzad et al., “A review on digital forensics frameworks for digital payments,” *Future Generation Computer Systems*, vol. 97, pp. 80–94, 2019.

[12] L. M. Lau et al., “Digital forensics framework for cyber fraud investigation in mobile payment systems,” *Computers & Security*, vol. 87, 101578, 2019.

[13] T. Zia and H. Ali, "An Investigation of Hyperlink Fraud in E-Payment Systems," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 11, pp. 289–293, 2018.

[14] H. Arora and N. Singh, "A Framework for Investigating Cyber-crimes in E-Payment Systems," *International Journal of Computer Applications*, vol. 179, no. 31, pp. 18–24, 2020.

[15] F. A. Shaikh and Y. P. Singh, "Cyber Forensics Techniques for Investigating Hyperlink Fraud in Digital Payments," in *Proc. 2021 11th Int. Conf. on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 402–406, IEEE, 2021.