OPEN ACCESS

Volume: 4

Issue: 1

Month: March

Year: 2025

ISSN: 2583-7117

Published: 19.03.2025

Citation:

Dr. Gurupada Das , Mr. Yeakub Afsan Ali , Miss Bhawna Singh and Miss Keya Nag "Digital Forensics in E-Commerce: Investigating Online Payment Fraud and Data Breaches" International Journal of Innovations in Science Engineering and Management, vol. 4, no. 1, 2025, pp. 262-268.

DOI:

10.69968/ijisem.2025v4i1262-268

Digital Forensics in E-Commerce: Investigating Online Payment Fraud and Data Breaches

Dr. Gurupada Das [1], Mr. Yeakub Afsan Ali [2], Miss Bhawna Singh [3] and Miss Keya Nag [4]

[1]Assistant Professor, Department of Commerce, Trivenidevi Bhalotia College, Raniganj, West Burdwan – 713347, West Bengal, India, Email: gurupadadas.dde@gmail.com
[2]Faculty Member, Department of Business Administration, Trivenidevi Bhalotia College, Raniganj, West Burdwan – 713347, West Bengal, India, Email: yeakubafsanali@gmail.com
[3]Faculty Member, Department of Business Administration, Trivenidevi Bhalotia College, Raniganj, West Burdwan – 713347, West Bengal, India, Email: bhawnasinghw@gmail.com
[4]Student, M.Com. Sem 3, Department of Commerce, Trivenidevi Bhalotia College, Raniganj, West Burdwan – 713347, West Bengal, India, Email: keyanag99@gmail.com

Abstract

The world market has changed due to the explosive rise of e-commerce, which provides consumers and companies with ease and accessibility. But the growth of the digital world has also brought up more dangers, especially with regard to online payment fraud and data breaches. This paper examines the function of digital forensics in the e-commerce industry with a particular emphasis on how it may be used to look into and stop fraudulent activity. The research illustrates how digital forensics helps in tracking, identifying, and prosecuting hackers responsible for payment fraud and illegal data access by examining real-world cases and using cutting-edge forensic technologies.

This research highlights the critical role that digital forensics play in ensuring the security of online transactions and the sustainability of the e-commerce industry in the digital age. It also discusses the challenges that businesses face in safeguarding their financial and customer data, preserving evidence, and maintaining consumer trust in the face of constantly evolving cyber threats. Finally, it looks at the legal and regulatory frameworks that govern digital forensic investigations in e-commerce and how businesses can adopt proactive forensic practices to protect their data.

Keywords: Digital forensics, E-commerce, Online payment fraud, Data breaches, Cybercrime, Forensic investigation, Cybersecurity

INTRODUCTION

The swift progress of digital technology has fundamentally transformed the worldwide trade environment, with electronic commerce emerging as a prominent player in the market. Online transactions' ease, accessibility, and effectiveness have revolutionized the way consumers and companies engage, leading to an unparalleled surge in digital commerce. But this growth also means more cyberthreats, especially in the form of data breaches and online payment fraud. While e-commerce platforms facilitate smooth transactions, hackers looking to take advantage of weaknesses have found them to be appealing targets.

Identity theft, phishing, and illegal transactions are examples of online payment fraud that puts businesses and customers at serious danger. Similar to this, e-commerce companies may suffer significant financial and reputational losses as a result of data breaches, which occur when private client information is accessed or stolen. These occurrences highlight the critical necessity for strong security protocols and forensic tools to identify, look into, and lessen the impact of cybercrimes of this nature.

The field of digital forensics has become indispensable in combating cyberattacks and e-commerce fraud.

Using cutting-edge methods to gather, store, and examine digital data, forensic specialists are able to track down fraudulent activity, identify offenders, and assist with court cases. Beyond just conducting reactive investigations, digital forensics plays a proactive role in e-commerce by identifying system weaknesses and providing guidance for the creation of more secure transaction environments.

This study examines the relationship between digital forensics and e-commerce, concentrating on how it might be used to look into data breaches and online payment fraud. It looks at the strategies and resources employed by forensic specialists to deal with these issues, draws attention to the technological and legal roadblocks that arise during forensic investigations, and talks about how companies might utilize digital forensics to safeguard their clients' data and operations. By doing this, this study hopes to provide light on how, in a world where cyber dependence is growing, digital forensics can protect the future of e-commerce.

Understanding Digital Forensics:

Identification, gathering, analysis, and preservation of electronic data for use in court and investigative procedures is known as digital forensics. Digital forensics is becoming an essential part of the battle against online fraud, hacking, and other types of digital misbehavior as cybercrimes increase in number. The domain of digital forensics comprises an extensive array of methodologies and procedures intended to track illicit activity, retrieve misplaced data, and guarantee the authenticity of digital evidence. When it comes to e-commerce, digital forensics is essential for determining the real story behind data breaches and online payment fraud.

The main concepts of digital forensics concentrate around the preservation and integrity of digital evidence. For any evidence to be admissible in court, it must be authenticated and stay unmodified throughout the inquiry. Strict processes are followed by digital forensic investigators to guarantee the "chain of custody," which protects the data from manipulation and records every person who handles the evidence. This is especially crucial in e-commerce situations since those transactions frequently contain sensitive financial and personal data.

Digital forensics helps e-commerce companies be proactive in thwarting any risks, in addition to supporting criminal investigations. Businesses may identify vulnerabilities early, stop fraud, and gain the trust of customers by using forensic best practices, continually monitoring systems, and evaluating abnormalities. It is impossible to overestimate the significance of digital forensics in protecting sensitive data and guaranteeing transaction integrity as e-commerce grows.

E-Commerce Fraud - Types and Techniques:

Because e-commerce is convenient, accessible, and has a worldwide reach, it has completely changed the way firms operate. But fraudsters have also made it a top target, taking advantage of weaknesses to perpetrate fraud. E-commerce fraud can result in fines from authorities, harm to a company's brand, and a decline in customer confidence in addition to monetary losses. This section looks at the many kinds of e-commerce fraud and the methods hackers employ to carry them out.

Table -1

Types of Fraud	Techniques Used
1) <u>Payment Fraud</u>: Payment fraud is one of the most common forms of e-commerce fraud, involving unauthorized transactions made using stolen payment credentials, such as credit or debit card details. This type of fraud typically occurs when cybercriminals gain access to sensitive payment information and use it to make fraudulent purchases.	• **Credit Card Fraud**: Criminals use stolen credit card information to make unauthorized purchases. Credit card details are often obtained through phishing attacks, data breaches, or by purchasing them from the dark web. This type of fraud is challenging to detect until the legitimate cardholder notices the unauthorized transactions and reports them. • **Card-Not-Present (CNP) Fraud**: As e-commerce transactions often don't require a physical card, cybercriminals can make online purchases using stolen card details without needing the card itself. CNP fraud is prevalent in e-commerce due to the absence of direct card verification, increasing the difficulty of detection. • **Chargeback Fraud**: In this type of fraud, a legitimate customer makes a purchase and later disputes the charge with their credit card company, claiming they did not authorize the transaction. This results in the business losing both the goods sold and the payment, along with incurring chargeback fees. Some customers engage in this fraud deliberately, known as "friendly fraud." • **Interception Fraud**: Criminals place orders using stolen payment information and manipulate the delivery address to intercept the package. They may either reroute the shipment after it's dispatched or choose an address close to the legitimate cardholder's address to avoid detection.

2) <u>Account Takeover Fraud</u>: Account takeover fraud occurs when a cybercriminal gains unauthorized access to a customer's e-commerce account. Once inside, the criminal can change account details, make purchases using stored payment information, or steal personal data.	• **Credential Stuffing**: Cybercriminals use large sets of stolen usernames and passwords obtained from previous data breaches to attempt logins on e-commerce sites. Many users reuse passwords across multiple sites, allowing criminals to successfully gain access to accounts. • **Phishing**: Fraudsters use phishing emails or fake websites designed to look like legitimate e-commerce platforms to trick users into revealing their login credentials or payment information. Once the cybercriminal has access to a user's account, they can make fraudulent transactions or steal stored credit card details. • **Social Engineering**: Cybercriminals manipulate individuals into divulging confidential information, such as security questions or passwords, by impersonating trusted sources like customer service representatives or bank officials.
3) <u>Refund Fraud</u>: Refund fraud targets the refund process of e-commerce platforms. Criminals exploit loopholes in the return policies of online retailers to get refunds for items they either didn't purchase or didn't return.	• **Returning Fake or Stolen Goods**: Fraudsters purchase items from an online retailer using stolen payment information and then return counterfeit or stolen goods for a refund. Alternatively, they may exploit a company's liberal return policies by sending back empty boxes or low-cost items that resemble the purchased product. • **Empty Box Fraud**: The fraudster claims they received an empty box instead of the product and demands a refund or replacement. Some e-commerce platforms may process refunds without a thorough investigation, especially when dealing with regular customers, making this technique effective. • **Refund Fraud via Chargebacks**: A combination of chargeback and refund fraud occurs when a fraudster first receives the refund from the merchant and then files a chargeback with their bank, essentially profiting from both the refund and the chargeback process.
4) Identity Theft: Identity theft in e-commerce occurs when cybercriminals use stolen personal information to impersonate legitimate customers. The fraudster can then make unauthorized purchases, open new accounts, or steal financial data.	• **Synthetic Identity Fraud**: In this technique, fraudsters create a fake identity by combining real and fictitious information, such as using a stolen Social Security number with a fabricated name and address. These synthetic identities are then used to open accounts and make purchases in e-commerce stores, often going undetected for long periods. • **Personal Information Harvesting**: Cybercriminals harvest personal data through data breaches, phishing attacks, or social engineering to impersonate customers. Once they gain access to an individual's account or financial information, they can make fraudulent purchases or resell the stolen data on the black market.
5) Affiliate Fraud: Affiliate marketing programs allow e-commerce businesses to pay affiliates for driving traffic or sales to their websites. Affiliate fraud occurs when criminals manipulate this system to earn commissions through dishonest means.	• **Cookie Stuffing**: Fraudsters use malware or browser vulnerabilities to inject affiliate cookies onto users' devices without their knowledge. When the user makes a legitimate purchase, the fraudster receives an affiliate commission, even though they did not refer the customer. • **Fake Traffic Generation**: Cybercriminals create fake websites or use automated bots to generate artificial clicks and visits to an e-commerce site. This falsely inflates traffic metrics, resulting in commissions being paid out for non-existent leads or customers.
6) Triangulation Fraud: In triangulation fraud, fraudsters create fake e-commerce stores offering high-demand products at deeply discounted prices. When an unsuspecting customer places an order, the fraudster uses stolen payment information to purchase the item from a legitimate retailer and ships it to the customer.	• **Fake Online Stores**: Fraudsters set up a fake storefront, often advertised on social media or other digital platforms, to attract buyers. Once the customer places an order, the fraudster quickly purchases the product from a legitimate e-commerce platform using stolen payment details and arranges for delivery to the customer. • **Multi-Layered Fraud**: In this scheme, the criminal profits on multiple fronts – they defraud the cardholder by using stolen credit card information, the legitimate retailer suffers financial losses, and the customer may unknowingly be complicit in receiving goods purchased illegally.
6) Friendly Fraud: Friendly fraud occurs when a legitimate customer makes a purchase and later disputes the transaction, claiming they didn't authorize the payment or never received the goods. While some cases may be genuine, others involve customers taking advantage of the system to obtain goods for free.	• **False Claims of Non-Receipt**: A customer receives a product but falsely claims that it never arrived. The e-commerce retailer may issue a refund or reship the product, leading to financial loss. • **Unjustified Chargebacks**: Some customers initiate chargebacks with their bank after receiving a product, often claiming the transaction was unauthorized. This leads to the e-commerce business losing the revenue from the sale and incurring chargeback fees.

Data Breaches in E-Commerce:

The surge in e-commerce in recent times may be attributed to the progress made in digital technology and the growing preference for online transactions. But this expansion has also resulted in an increase in data breaches, which makes e-commerce sites easy pickings for hackers. Unauthorized access to sensitive data, including payment card numbers, customer personal information, and company trade secrets, is known as a data breach in e-commerce. These breaches frequently cause financial losses and harm to a company's reputation. Because these companies manage a large quantity of sensitive data and attacker strategies are always improving, data breaches continue to pose a serious danger to e-commerce platforms. E-commerce platforms may reduce the risks of data breaches by investing in strong security measures and routinely upgrading their systems, protecting client data and preserving company operations.

Cybercriminals typically take advantage of a variety of vulnerabilities to create data breaches in e-commerce. Weak security procedures, which occur when platforms neglect to apply crucial security features like encryption, multi-factor authentication, and frequent upgrades, are a major contributing cause. This leaves these platforms vulnerable to hackers. Cybercriminals also frequently deploy phishing assaults to deceive clients or staff into disclosing financial information or login credentials, allowing them to gain illegal access to networks. In addition, hackers can use methods like malware and SQL injections to take advantage of holes in a website's coding, giving them access to private databases and the ability to steal financial and personal information. Relying on outside suppliers to provide services like payment gateways, cloud storage, and shipping carries additional risks since these partners could not have proper security in place, making them easy targets for hackers. Finally, poor data storage procedures raise the possibility of data disclosure following a breach. Examples of these practices include keeping client data for extended periods of time or storing sensitive information without encryption. These elements work together to show the several ways that e-commerce systems might be compromised by hackers.

Data breaches have far-reaching effects on e-commerce that have an influence on both customers and businesses. One of the most obvious effects is financial loss; companies may have to pay for compensations, regulatory fines, and fraud expenses; if consumers' payment information is stolen, they may also incur financial losses. Furthermore, a data breach may seriously harm a business's brand and erode client trust, both of which are essential for surviving in the e-commerce sector. There are important legal and regulatory ramifications as well since e-commerce businesses must abide by data privacy regulations like the General Data privacy Regulation (GDPR), and violations can lead to costly fines and compliance expenses.Another significant effect is customer attrition, which results in a decline in revenue and a smaller client base as consumers are likely to go to rivals if they believe their data is not safe.

Enterprises engaged in e-commerce need to have strict security protocols to avoid data leaks. The use of tokenization and encryption is one important technique that makes sure sensitive data is encrypted both in transit and at rest, making it unreadable even in the event that it is intercepted. To find and address any possible system vulnerabilities, regular security audits and vulnerability assessments are crucial. Staff members need to be knowledgeable about data security best practices, such spotting phishing attempts and creating secure passwords, thus employee training is also essential. Lastly, in order to maintain strong security and stay out of legal hot water, companies need to make sure they are in compliance with all applicable data protection laws and industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

Role of Digital Forensics in Investigating Payment Fraud:

When examining payment fraud in e-commerce, digital forensics is essential since it may reveal the sources and techniques of fraudulent activity. Forensic specialists can track out illicit access to payment systems by looking through digital evidence, including communication data, transaction logs, and user authentication records. This method include tracking down questionable transactions, looking for irregularities in payment habits, and examining the digital traces that fraudsters have left behind. Digital forensics can ascertain the fraud's method of execution—phishing, malware, or social engineering attacks—through these inquiries. Businesses need this information in order to comprehend the extent of the fraud and implement remedial action to safeguard their systems.

Moreover, digital forensics offers crucial evidence for court cases in addition to helping identify offenders. The chain of custody is preserved because digital evidence is painstakingly preserved via the forensic process in a way that makes it acceptable in court. Cybercriminals may be prosecuted using this evidence, and compensation for monetary damages sustained may be demanded. Furthermore, by identifying holes in payment security

methods and system vulnerabilities, forensic investigations assist companies in strengthening their cybersecurity defenses. E-commerce businesses may strengthen their ability to safeguard their assets and clientele from future instances of payment theft by utilizing digital forensics.

Role of Digital Forensics in Data Breach Investigations:

Digital forensics plays a critical role in detecting data breaches by establishing how, when, and where illegal access happened inside an organization's systems. To determine the source of the breach, forensic specialists examine compromised servers, networks, and devices. They also go through logs, user credentials, and system settings to find weaknesses that attackers have exploited. This procedure include tracing malware or phishing activity, retrieving erased or modified files, and determining the amount of compromised data, including private customer data. Digital forensics helps companies comprehend the breach and supports legal procedures against the offenders by preserving digital data and upholding a clear chain of custody. The knowledge gathered from these investigations also helps companies improve their cybersecurity protocols in order to avert similar incidents in the future.

Challenges in Digital Forensics for E-Commerce:

The intricate and dynamic nature of cyber threats presents several obstacles for digital forensics in the e-commerce industry. One significant obstacle is the enormous amount of data produced by e-commerce platforms, which makes it challenging for forensic specialists to sort through and locate pertinent evidence. Because there are millions of transactions per day, it takes a lot of effort and sophisticated techniques to isolate questionable behavior. Furthermore, it can be challenging for forensic investigators to track down and identify the perpetrators of assaults since cybercriminals frequently conceal their identities and activities using advanced techniques like anonymization and encryption. Further complicating investigations is the use of several payment gateways, cloud services, and third-party suppliers. This is because data is frequently dispersed across many systems and jurisdictions, necessitating collaboration between diverse groups.

The quickly evolving field of e-commerce technology and the strategies used by cybercriminals provide another major obstacle. Emerging risks like AI-driven assaults introduce new vulnerabilities, and new payment methods like cryptocurrency might be challenging to track down and analyze. Furthermore, because there is a risk that important evidence may be lost or altered due to delays in identifying breaches, forensic investigators frequently struggle to secure timely access to essential data. Legal and regulatory restrictions complicate things even further since they might limit the capacity to gather and evaluate evidence. This is especially true for cross-border investigations because various nations may have differing data privacy rules. These difficulties show how important it is to keep improving digital forensic techniques and instruments in order to successfully fight fraud and data breaches in the e-commerce industry.

Legal and Regulatory Framework:

For the safety of customer data and the integrity of online transactions, the legal and regulatory framework around digital forensics in e-commerce is crucial. Important laws, including the California Consumer Privacy Act (CCPA) in the US and the General Data Protection Regulation (GDPR) in Europe, place stringent rules on how companies use personal data, including permission, data protection, and breach reporting. These rules specify the processes for carrying out forensic investigations in the case of a data breach and require businesses to put strong security measures in place to protect sensitive data. Furthermore, e-commerce platforms that handle payment card transactions must adhere to strict security guidelines established by a number of industry standards, including the Payment Card Industry Data Security Standard (PCI DSS). It is imperative to conform to these legal frameworks, since noncompliance may lead to severe legal fines, monetary losses, and harm to one's image. In addition, these standards serve as a guide for forensic investigators, guaranteeing the collection and preservation of evidence in a way that makes it legally admissible in court. This facilitates the prosecution of cybercriminals and the recovery of damages resulting from fraud or data breaches.

Preventive Measures and Best Practices:

To protect themselves against payment fraud and data breaches, e-commerce companies must implement best practices and preventive measures. Putting strong security measures in place, including tokenization and encryption, is one of the main tactics. Sensitive data should always be encrypted, both during transmission and storage, to prevent readable data from being intercepted by hackers. By substituting non-sensitive data components for sensitive data elements, tokenization improves security even further and reduces the chance of exposure. Additionally, organizations should utilize multi-factor authentication (MFA) to add an extra layer of protection, making it more

difficult for unauthorized individuals to access accounts even if they have hacked login credentials.

Regular security audits and vulnerability assessments are key components of a proactive security strategy. By carrying out these audits, possible system vulnerabilities are found and fixed before hackers can take advantage of them. Establishing a thorough incident response plan can help e-commerce companies make sure that every employee is aware of their obligations in the case of a security breach. This readiness can lessen the effects of a breach and drastically cut down on reaction times. Strict access controls and user activity monitoring can also aid in the early detection of questionable activities, allowing for prompt intervention before serious harm is done.

Another essential component in stopping fraud and data breaches is employee training. By training employees on data security best practices, such as spotting phishing attempts, making secure passwords, and appreciating the value of data protection, you may enable them to act as your first line of defense against online dangers. Companies can also encourage staff members to report suspicious activity without fear of retaliation by fostering a culture of security awareness. Ultimately, maintaining adherence to pertinent laws and industry standards, such the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), can improve security while simultaneously fostering consumer confidence in the e-commerce platform. E-commerce companies may greatly lessen their exposure to payment fraud and data breaches by implementing these best practices and preventive measures.

Future Trends in Digital Forensics for E-Commerce:

Because cyber threats are getting more complex and technology is continuing to progress, digital forensics in e-commerce is going to undergo substantial evolution in the future. The use of machine learning and artificial intelligence (AI) into forensic tools is one significant development. These tools, which automate data analysis, spot abnormalities, and discover patterns suggestive of fraud or security breaches, can improve the speed and accuracy of investigations. AI, for example, may be used to instantly evaluate enormous volumes of transaction data and identify questionable behavior that needs to be looked into further. The use of AI in digital forensics will be crucial to staying ahead of new dangers as e-commerce platforms use AI-driven payment systems more often.

The increasing focus on privacy and data protection, especially in reaction to new laws like the CCPA and GDPR, is another significant development. When conducting forensic investigations, e-commerce enterprises must emphasize compliance as customers grow more aware of their rights surrounding personal data. This delicate balance might result in the creation of novel forensic techniques that respect private rights and permit fruitful investigations. Furthermore, as decentralized technologies like blockchain gain popularity, digital forensics will have to change to look into transactions in a transparent yet safe way. In general, technology developments and legal frameworks will influence the direction of digital forensics in e-commerce, requiring ongoing innovation to successfully fight fraud and safeguard customer data.

CONCLUSION

In conclusion, digital forensics plays a key role in maintaining the integrity of e-commerce by detecting online payment fraud and data breaches. Robust forensic procedures are necessary to successfully tackle the difficulties posed by hackers as the e-commerce industry continues to grow. Using cutting-edge technology like artificial intelligence and machine learning, forensic specialists can improve their capacity to examine enormous volumes of data, spot questionable activity, and track down the source of fraudulent transactions.

Furthermore, it is impossible to exaggerate the significance of a robust legal and regulatory framework as it directs e-commerce companies' security procedures and guarantees adherence to data protection regulations. To reduce risks and increase customer trust, preventive steps are crucial. These include personnel training, frequent security assessments, and the adoption of strict security procedures. Digital forensics will remain a vital tool for e-commerce companies looking to safeguard sensitive data and ensure secure online transactions, eventually promoting a safer digital marketplace for both customers and businesses, as long as it continues to adapt to new technologies and regulatory requirements.

REFERENCES

[1] Robles, A., & Coloma, M. (2023). Cybercrime in E-Commerce: Trends and Preventive Measures. Journal of Cybersecurity and Privacy, 3(1), 20-40. https://doi.org/10.3390/jcp3010002

[2] Dhanraj, N., & Ahmed, E. (2023). Digital forensics in cloud environments: Challenges and solutions for e-commerce security. Journal of Cloud Computing: Advances, Systems and Applications, 12(1), 20-35. https://doi.org/10.1186/s13677-023-00342-4

[3] Reddy, P. K., & Sahu, P. (2022). Analyzing the effectiveness of digital forensics in preventing e-commerce fraud. Computers & Security, 122, 102849. https://doi.org/10.1016/j.cose.2022.102849

[4] Alenezi, M., Alabdulatif, A., & Alghannam, R. (2022). A survey on the impact of payment card industry data security standards on preventing e-commerce fraud. Journal of Information Security and Applications, 66, 103149. https://doi.org/10.1016/j.jisa.2022.103149

[5] Hassan, A., & Falah, A. (2022). The evolution of cyber threats in e-commerce: Implications for digital forensics. Journal of Cybersecurity and Privacy, 3(4), 98-112. https://doi.org/10.3390/jcp3040075

[6] Chaudhry, S. R., & Khanzada, A. J. (2022). A framework for digital forensics in cloud computing environments for e-commerce applications. Forensic Science International: Digital Investigation, 41, 301-310. https://doi.org/10.1016/j.fsidi.2022.301310

[7] Arora, A., & Khan, M. S. (2021). Analyzing the impact of cybersecurity measures on e-commerce fraud. Journal of Business Research, 124, 89-97. https://doi.org/10.1016/j.jbusres.2020.11.025

[8] Gupta, A., & Kumar, A. (2021). Cybersecurity regulations and their impact on e-commerce operations: A systematic review. Computers & Security, 109, 101431. https://doi.org/10.1016/j.cose.2021.101431

[9] Bada, A., & Sasse, M. A. (2020). Cybersecurity education: Addressing the growing skill gap in digital forensics. Computers & Security, 96, 101918. https://doi.org/10.1016/j.cose.2020.101918

[10] Frosch, R., & Kahn, M. (2020). E-commerce Security: An Overview of Online Payment Fraud Detection Techniques. Journal of Internet Commerce, 19(3), 287-307. https://doi.org/10.1080/15332861.2020.1782820

[11] Manharan Anant et al. 2024. An Empirical Study on Awareness of Cyber Security in Digital Banking Among College Going Students (With Special Reference To Korba District Of Chhattisgarh). *International Journal of Innovations in Science, Engineering And Management*. 2, (May 2024), 45–49.

[12] Phippen, A. D., & Sheehan, B. (2020). Online payment fraud: The role of digital forensics in recovery and prevention. International Journal of Information Security, 19(3), 251-261. https://doi.org/10.1007/s10207-020-00506-9

[13] Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. Annual Review of Criminology, 2(1), 191-216. https://doi.org/10.1146/annurev-criminol-032317-092011

[14] Williams, J. (2019). The role of digital forensics in mitigating online payment fraud. International Journal of Cyber Forensics and Advanced Threat Investigations, 1(2), 89-101. https://doi.org/10.1007/s12083-019-01019-5

[15] Alazab, M., & Khraisat, A. (2019). The impact of machine learning on digital forensics and online fraud detection. Digital Forensics and Cyber Crime, 13, 49-64. https://doi.org/10.1007/978-3-030-22813-4_4

[16] Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity and fraud prevention in e-commerce. Journal of International Technology and Information Management, 27(3), 14-22. https://doi.org/10.1007/s40550-018-0011-0

[17] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[18] Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. Journal of Economic Perspectives, 23(3), 3-20. https://doi.org/10.1257/jep.23.3.3