BLIND FOLD LEGAL JOURNAL

VOLUME 3 ISSUE 4
[MAR. 2024 - MAY 2024]

E-mail: blindfoldjournal@gmail.com
Website: www.blindfoldjournal.com

"FRAUD DETECTION TECHNIQUES IN ONLINE SHOPPING"

Author: Dr. Monika Rastogi, Dr. Vivek Rastogi,
& Mr. Durgendra Singh Rajpoot

ABSTRACT

E-commerce has become increasingly popular for online shopping, banking, financial institutions, and government. However, fraudulent activities are prevalent in various sectors, including telecommunication, credit card fraud detection, network intrusion, finance, insurance, and scientific applications. Billions of dollars are lost daily due to the increase in credit card transactions. To reduce losses, potent and efficient fraud detection algorithms are crucial. This paper discusses various approaches used in fraud detection in e-commerce. Fraud is an act of betrayal intended for personal use or loss, and can be physical or virtually. E-commerce fraud includes telecommunication, credit card, computer intrusion, bankruptcy fraud, theft, counterfeit fraud, application fraud, and behavioral fraud. Credit card fraud can be offline or online, and telecommunication fraud involves misuse of mobile phones and fixed lines. Computer intrusion involves unauthorized access to information. Bankruptcy fraud is difficult to predict and can lead to unwanted loans. Theft and counterfeit fraud involve using stolen cards without the owner's consent. Application fraud involves applying for a credit card with incorrect information, with detection ranging from duplicates to identity fraudsters. Behavioral fraud occurs when orders are made based on "cardholder present" details and legitimate card details are obtained. Credit card fraud is a common issue on the internet, with various techniques used by cybercriminals. These include credit card fraud generator software, which generates valid credit card numbers using the mathematical Luhn algorithm, and key logger and sniffers, which log user keyboard inputs for personal gain. Spam mail is used to infect users' computers, allowing them to unknowingly share their private information. Site-cloning, spyware, and merchant sites are also used by black-hat hackers to track user activities and steal personal information. Physically stolen credit card information is used for online buying and selling of products. CC/CVV2 shopping websites are used by cybercriminals without professional computer skills to fraudulently use hacked credit card information for goods and services on the internet. These methods can be used by fraudsters with little or no computer skills to steal credit card information. Credit card fraud detection methods include a Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning, which combines rule-based filters, Dempster-Shafer adder, and Bayesian learner to detect transactions based on current and past behavior. This approach has advantages like high accuracy,

processing speed, and reduced false alarms. However, it is expensive. Blast-Ssaha Hybridization, Hidden Markov Model, and Fuzzy Darwinian Detection are methods used for detecting fraud in telecommunications and banking. Blast-Ssaha Hybridization uses a two-stage sequence alignment system, HMM compares transactions to a threshold, and FDD uses an evolutionary-Fuzzy system for classification. Fuzzy Darwinian Detection (FDD) is an evolutionary-Fuzzy system that uses Genetic Programming to classify transactions into suspicious and non-suspicious ones. It has high accuracy and low false alarms but is not suitable for online transactions. Bayesian and Neural Network (BNN) is an automatic fraud detection system based on machine learning and Pattern Recognition. Other approaches include Decision Tree, Genetic Algorithm, Artificial Neural Network, K-Nearest Neighbor Algorithm, Stream Outlier Detection, Fuzzy Logic Based System, Fuzzy Expert System, Support Vector Machine, and Meta Learning Strategy. The Hybridization of BLAST-SSAHA approach is the best suitable for fraud detection in terms of cost and accuracy. By implementing rules from other approaches or advanced rule sets, it is possible to increase True Positive results and decrease false alarms.

INTRODUCTION

Now in the technology of days due to speedy development internet usage is everywhere. In today's evolution electronic world, many small and large companies have placed their businesses on to the WWW to provide services to customer. E-commerce uses technologies such as electronic transmission, online transaction processing, online banking and automatic data collection systems, etc. Online shopping is becoming more popular every day. Payment systems for online shopping have become popular due to the widespread use of online shopping and banking. Rapid increment of this era billions of dollars are lost every year due to credit card fraud. Fraud is an act of betrayal intended for personal usage or to harm a loss to someone. Fraudster only wants to know the personal information related to card (card number, card expiry date etc.). It can be possible physically or virtually. It is commonly understood as dishonesty to gain some advantage which is often financial, over another person. It can be seen in most common, acquiring or trading of property, including real property, Personal Property, and intangible property, such as stocks, bonds, and copyrights.

PROBLEM DEFINITION

Online shopping has become increasingly popular, but it also presents challenges in terms of security and fraud prevention. The problem of fraud detection in online shopping involves

identifying and mitigating fraudulent activities, such as unauthorized transactions, identity theft, and payment fraud, to protect both merchants and consumers.

1. Fraudster do not want to purchase anything from the shopping cart but still he/she giving the wrong information & make payment transaction as a Cash on delivery to harm to the merchant.
2. If the credit/debit card details are stolen or lost, then using the credit card number and cvv number, the fraudster can easily make the payment without the knowledge of the real user.
3. If a fraudster has hacked the original database of a bank or online store where all card-related information is stored, credit/debit card fraud may be possible.
4. Why is integrating and analyzing diverse data sources like transaction history, user behavior patterns, device information, geolocation data, and external threat intelligence crucial for identifying suspicious activities and patterns indicative of fraud in fraud detection systems?
5. What methods are involved in effective fraud detection, and how do they utilize historical data, predictive modeling, and real-time monitoring to detect and prevent fraudulent transactions?

TYPES OF CYBER FRAUDS

Cyber fraud encompasses a wide range of criminal activities conducted over the internet with the intention of deceiving individuals or organizations for financial gain. Some common types of cyber fraud include:

1. **PHISHING:** Phishing is a form of cyberattack where attackers disguise themselves as a trustworthy entity in order to deceive individuals into revealing sensitive information such as usernames, passwords, credit card numbers, or other personal data. This is often done through fraudulent emails, messages, or websites that appear legitimate. Phishing attacks can have serious consequences, including identity theft, financial loss, and unauthorized access to accounts or systems. It's important to remain vigilant and cautious when interacting with unfamiliar or unexpected online communications to avoid falling victim to phishing scams.

2. **IDENTITY THEFT:** Identity theft is a type of cybercrime where someone wrongfully obtains and uses another person's personal data in a fraudulent or deceptive manner, typically for financial gain. The stolen information may include the victim's name, Social Security number, date of birth, credit card numbers, bank account details, or other sensitive data.

Perpetrators of identity theft may use various methods to acquire this information, including phishing scams, data breaches, hacking into databases, stealing physical documents, or even using social engineering techniques to trick individuals into divulging their personal information willingly.

Once the perpetrator has obtained the victim's personal data, they can use it to commit various fraudulent activities, such as:

1. Opening new credit card accounts or bank accounts in the victim's name.
2. Making unauthorized purchases or withdrawals using the victim's financial accounts.
3. Applying for loans or mortgages using the victim's identity.
4. Filing fraudulent tax returns to claim refunds.
5. Obtaining medical services or prescription drugs using the victim's health insurance information.
6. Committing crimes and providing the victim's identity when apprehended.

Identity theft can have serious consequences for the victim, including financial losses, damage to credit scores, legal issues, and emotional distress. Detecting and recovering from identity theft can also be challenging and time-consuming for victims.

To protect against identity theft, individuals should take proactive measures to safeguard their personal information, such as using strong, unique passwords, being cautious about sharing sensitive information online, regularly monitoring financial accounts and credit reports for suspicious activity, and promptly reporting any signs of identity theft to the relevant authorities.

3. CREDIT CARD FRAUD: Credit card fraud is a type of financial fraud involving the unauthorized use of someone else's credit card information to make purchases or withdraw funds. It can occur in various ways, including:

- **STOLEN CARD:** If a physical credit card is stolen, the thief can use it to make purchases until the card is reported stolen or its funds are depleted.

- **CARD SKIMMING**: Criminals may install skimming devices on ATMs, gas pumps, or other point-of-sale terminals to capture credit card information when the card is swiped or inserted.
- **PHISHING:** Fraudsters may use phishing emails or websites to trick individuals into providing their credit card details, which are then used for fraudulent transactions.
- **DATA BREACHES:** Cybercriminals may hack into databases of retailers, financial institutions, or online merchants to steal credit card information stored on their systems.

4. CARD NOT PRESENT (CNP) FRAUD: Card Not Present (CNP) fraud refers to fraudulent transactions where a credit card is used for payment without the physical presence of the card itself. This type of fraud commonly occurs in online, mail order, or telephone transactions, where the cardholder provides the card details (such as card number, expiration date, and security code) to complete a purchase. CNP fraud can take various forms, including:

- **STOLEN CARD INFORMATION:** Fraudsters may obtain credit card details through data breaches, phishing scams, or other illicit means, and then use this stolen information to make unauthorized purchases online.
- **CARDING:** Criminals may use automated bots or manual methods to test stolen credit card information on e-commerce websites, attempting to make small purchases to verify whether the card is still valid before proceeding with larger transactions.
- **ACCOUNT TAKE OVER:** If a fraudster gains unauthorized access to a victim's online account (e.g., through phishing or hacking), they may add stolen credit cards to the account or change the billing information to facilitate fraudulent transactions.

CNP fraud poses significant challenges for merchants and financial institutions, as they must balance the need to provide convenient payment options for customers with the responsibility to prevent fraudulent transactions. To mitigate the risk of CNP fraud, businesses and consumers can take several preventive measures, including:

- Implementing robust fraud detection and prevention systems, such as address verification services (AVS), card verification value (CVV) checks, and machine learning algorithms to flag suspicious transactions.
- Using multi-factor authentication methods to verify the identity of customers during online transactions.

- Encrypting sensitive payment information to protect it from unauthorized access.
- Educating customers about online security best practices and warning signs of phishing scams.
- Regularly monitoring transactions for unusual or suspicious activity and promptly reporting any suspected fraud to the appropriate authorities or financial institutions.

By employing these strategies and staying vigilant, businesses and consumers can help reduce the incidence of CNP fraud and safeguard against financial losses and reputational damage.

ACCOUNT TAKEOVER: In some cases, fraudsters may gain unauthorized access to a victim's online account and change the billing address or add new credit cards to the account to make fraudulent purchases.

Credit card fraud can result in financial losses for both cardholders and financial institutions, as well as damage to the victim's credit score and reputation. To minimize the risk of credit card fraud, individuals should:

- Keep their credit cards secure and report any lost or stolen cards immediately.
- Regularly monitor their credit card statements for unauthorized transactions.
- Use secure websites for online purchases and avoid sharing credit card information over unsecured networks.
- Enable two-factor authentication and other security features offered by credit card issuers.
- Be cautious of phishing attempts and never provide credit card information in response to unsolicited emails or calls.
- Consider using virtual credit card numbers or mobile payment methods for added security.
- Check their credit report regularly for signs of unauthorized activity.

5. PAYMENT FRAUD: Payment fraud encompasses a broad range of fraudulent activities involving the unauthorized or deceptive use of payment methods to obtain goods, services, or funds. It can occur in various forms across different payment channels, including credit cards, debit cards, bank transfers, mobile payments, and digital wallets. Here are some common types of payment fraud like as Credit Card Fraud, Debit Card Fraud, Check Fraud, Bank Transfer Fraud, Mobile Payment Fraud, Online Payment Fraud etc. Preventing payment fraud requires a combination of security measures, including robust authentication mechanisms, transaction monitoring systems, encryption technologies, and customer education initiatives. Businesses and

individuals should remain vigilant, adopt best practices for securing payment transactions, and promptly report any suspected fraudulent activity to relevant authorities or financial institutions.

6. ONLINE AUCTION FRAUD: In the landmark case of eBay v. Bidder's Edge, unauthorized web scraping and data aggregation were deemed unlawful, setting precedent against online auction fraud. This ruling underscored the importance of protecting website owners' property rights and established legal boundaries for accessing and using online auction listings. The decision highlighted the need for consent and authorization when aggregating online content, thereby deterring fraudulent activities such as unauthorized access to auction platforms for deceptive purposes. This case served as a foundational legal framework for addressing online auction fraud and safeguarding the integrity of e-commerce platforms, shaping subsequent litigation and regulatory efforts in the digital realm.

7. INVESTMENT FRAUD: In the case of United States v. Stanford, financier Allen Stanford was convicted for orchestrating a massive Ponzi scheme through his Stanford Financial Group. Promising high returns through bogus certificates of deposit, Stanford defrauded investors of billions of dollars. The case underscored the devastating impact of investment fraud on unsuspecting victims and highlighted the need for rigorous regulatory oversight in the financial industry. Stanford's conviction served as a landmark example of holding perpetrators of investment fraud accountable, emphasizing the importance of transparency, due diligence, and investor protection measures to prevent similar schemes and uphold the integrity of financial markets.

8. ROMANCE SCAMS: Romance scams, a deceitful ploy, exploit trust for personal gain. Perpetrators create fake personas to lure victims emotionally, often through online dating platforms or social media. They cultivate a deep connection, weaving tales of love and devotion, only to request financial assistance or gifts. Victims, ensnared by affection, may overlook red flags until it's too late. The aftermath leaves emotional scars and financial devastation. Awareness and vigilance are paramount in thwarting these schemes, ensuring love remains genuine and not a tool for exploitation.

9.TECH SUPPORT SCAMS: Tech support scams prey on unsuspecting individuals, masquerading as legitimate technical assistance. They employ various tactics, like pop-up messages, cold calls, or emails, claiming urgent issues with the victim's device. Perpetrators often impersonate reputable companies, instilling fear to coerce victims into sharing personal

information or granting remote access to their systems. Once access is granted, they may install malware or demand payment for fabricated services. These scams exploit trust in technology, leaving victims vulnerable to identity theft and financial loss. Staying cautious, verifying sources, and seeking assistance from trusted professionals are crucial in safeguarding against such deceitful schemes.

10. FAKE CHARITIES: Fake charities exploit goodwill for personal gain, deceiving donors with fraudulent appeals for support. They often mimic legitimate organizations, using emotional pleas and convincing narratives to solicit donations. Perpetrators may create fake websites, host events, or even go door-to-door to elicit funds. However, the money collected rarely benefits the stated cause, instead lining the pockets of scammers. Victims, driven by compassion, unwittingly contribute to these scams, only to discover their generosity was exploited. To avoid falling prey, donors should research charities thoroughly, verify their legitimacy through trusted sources, and prioritize direct donations to established organizations with transparent practices.

CASE LAWS REGARDING ONLINE FRAUD

Several case laws have set important precedents and established legal principles related to online fraud. Here are a few notable examples:

1. **UNITED STATES V. MITRA**: In this case, the defendant was charged with wire fraud for operating a scheme that involved sending deceptive emails to victims in order to obtain their personal and financial information. The court held that the defendant's actions constituted wire fraud under federal law, establishing precedent for prosecuting online fraud schemes involving electronic communications.

2. **EBAY V. BIDDER'S EDGE:** This case involved a dispute between eBay and Bidder's Edge, a website that aggregated and displayed eBay auction listings without authorization. eBay sued Bidder's Edge for trespass to chattels and breach of contract. The court ruled in favor of eBay, establishing that unauthorized web scraping and data aggregation can constitute unlawful interference with a website owner's property rights.

3. **UNITED STATES V. GORSHKOV:** In this case, the defendant was charged with operating a sophisticated online fraud scheme that involved hacking into computers, stealing credit card information, and selling the stolen data on underground forums. The court found

the defendant guilty of multiple counts of computer fraud and identity theft, setting an important precedent for prosecuting cybercriminals engaged in large-scale online fraud operations.

4. **FACEBOOK V. POWER VENTURES**: Facebook sued Power Ventures for accessing its users' accounts without authorization and sending unsolicited messages on behalf of its users. The court held that Power Ventures violated the Computer Fraud and Abuse Act (CFAA) by accessing Facebook's computers without permission, establishing precedent for holding companies accountable for unauthorized access to online platforms.

5. **UNITED STATES V. ROSS WILLIAM ULBRICHT (SILK ROAD CASE):** Ross Ulbricht was convicted for creating and operating the Silk Road, an online black market that facilitated illegal drug sales and other criminal activities. The case raised important legal questions about the boundaries of liability for online platform operators and the regulation of anonymous online marketplaces.

These cases illustrate the evolving legal landscape surrounding online fraud and cybercrime, as courts grapple with complex legal issues arising from advancements in technology and the proliferation of online criminal activity.

CREDIT CARD FRAUD TECHNIQUES

Credit card fraud is a common issue on the internet, with various techniques used by cybercriminals. These include credit card fraud generator software, which generates valid credit card numbers using the mathematical Luhn algorithm, and key logger and sniffers, which log user keyboard inputs for personal gain. Spam mail is used to infect users' computers, allowing them to unknowingly share their private information. Site-cloning, spyware, and merchant sites are also used by black-hat hackers to track user activities and steal personal information. Physically stolen credit card information is used for online buying and selling of products. CC/CVV2 shopping websites are used by cybercriminals without professional computer skills to fraudulently use hacked credit card information for goods and services on the internet. These methods can be used by fraudsters with little or no computer skills to steal credit card information.

METHODS USED TO DETECT CREDIT CARD FRAUD

Fraud detection approaches include Dempster-Shafer Theory and Bayesian Learning, which combine rule-based filters, Dempster-Shafer adder, and Bayesian learner to detect transactions based on current and past behavior. This system has advantages like high accuracy, processing speed, and reduced false alarms. However, it is expensive. The Blast-Ssaha Hybridization is a two-stage sequence alignment system that uses profile and deviation analyzers to match incoming transactions and determine if they are genuine or fraudulent. This system is useful in telecommunication and banking fraud detection but does not detect cloning cards. The Hidden Markov Model (HMM) is a probability distribution system that compares incoming transactions to a predefined threshold value to determine legitimacy or fraud. It has two processing phases: Training and Detection. Unusual or unaccepted transactions are considered fraud, while normal transactions are allowed.

LEGAL PROVISIONS FOR ONLINE FRAUD IN INDIA

In India, online fraud is addressed by various laws and regulations aimed at protecting consumers and combating cybercrimes. Some of the key legal provisions related to online fraud in India include:

- **INFORMATION TECHNOLOGY ACT, 2000 (IT ACT):** The IT Act is the primary legislation governing cyber activities and electronic commerce in India. It defines cybercrimes and provides legal provisions for offenses such as hacking, identity theft, and phishing, which are common forms of online fraud.

- **THE PAYMENT AND SETTLEMENT SYSTEMS ACT, 2007:** This act regulates payment systems and provides provisions for the establishment, regulation, and oversight of payment systems in India. It includes measures to prevent fraudulent activities in online payments and transactions.
- **THE CONSUMER PROTECTION ACT, 2019:** This act aims to protect the interests of consumers and provides mechanisms for redressal of consumer grievances, including those related to online fraud. Consumers can seek compensation and relief for fraudulent transactions or deceptive practices by businesses.
- **THE RESERVE BANK OF INDIA (RBI) GUIDELINES:** The RBI issues guidelines and regulations to banks and financial institutions to ensure the security of online transactions and prevent fraud. These guidelines include measures such as two-factor authentication, fraud detection systems, and customer education initiatives.

- **THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016:** This act regulates the use of Aadhaar, a biometric-based identification system in India. It includes provisions to safeguard the security and confidentiality of Aadhaar data and prevent identity theft and fraud.

- **THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021:** These rules govern online intermediaries such as social media platforms, e-commerce websites, and messaging apps. They include provisions to prevent the spread of fake news, misinformation, and fraudulent activities on online platforms.

- **CYBERCRIME INVESTIGATION CELLS:** Various states in India have established cybercrime investigation cells or units to investigate and prosecute cybercrimes, including online fraud. These units work in coordination with law enforcement agencies and specialized cybercrime divisions.

It's essential for individuals and businesses in India to be aware of these legal provisions and take measures to protect themselves against online fraud. This includes implementing cybersecurity measures, exercising caution while conducting online transactions, and reporting suspected fraudulent activities to the relevant authorities

PROPOSED SOLUTION

The proposed solution for online merchants involves data collection and integration, machine learning models, anomaly detection, real-time monitoring and alerting, adaptive learning, and compliance with regulations. This comprehensive system combines advanced technologies, data analytics techniques, and domain expertise to identify and mitigate fraudulent activities. Computer intrusion, also known as cyber intrusion or cybersecurity breach, refers to unauthorized access into a computer system, network, or device with malicious intent. Common types of computer intrusions include malware, hacking, DoS and DDoS attacks, phishing, insider threats, SQL injection, Man-in-the-Middle (MitM) attacks, zero-day exploits, password attacks, and social engineering. Protecting against computer intrusions requires robust cybersecurity measures, including regular software updates, strong access controls, employee training, intrusion detection systems, and incident response plans. Additionally,

practicing good cyber hygiene, such as using complex passwords, avoiding suspicious links or attachments, and encrypting sensitive data, can help mitigate the risk of intrusions. By implementing these measures, online merchants can protect their businesses and customers from financial losses and reputational damage associated with online shopping fraud.

CONCLUSION AND SUGGESTIONS

In conclusion, fraud detection techniques in online shopping play a crucial role in safeguarding both consumers and businesses from the risks associated with fraudulent activities. Here are some key points to consider:

1. MACHINE LEARNING AND AI: Implementing advanced machine learning algorithms and AI systems can help detect patterns and anomalies in transaction data, enabling early identification of potentially fraudulent activities.

2. BEHAVIORAL ANALYSIS: Monitoring user behavior and transaction patterns can aid in detecting suspicious activities. Deviations from typical behavior, such as sudden large purchases or unusual login locations, can trigger alerts for further investigation.

3.IP GEOLOCATION AND DEVICE FINGERPRINTING: Verifying the geographic location of users and analyzing device fingerprints can help authenticate transactions and detect fraudulent attempts from unfamiliar or suspicious locations.

4. BIOMETRIC AUTHENTICATION: Incorporating biometric authentication methods, such as fingerprint or facial recognition, adds an extra layer of security by verifying the identity of users during transactions.

5. REAL-TIME MONITORING: Utilizing real-time monitoring systems allows for immediate detection and response to fraudulent activities as they occur, minimizing potential losses and mitigating risks.

6. DATA ANALYTICS: Leveraging big data analytics tools can help identify trends and patterns indicative of fraudulent behavior, enabling businesses to proactively adjust their fraud detection strategies.

7. COLLABORATIVE EFFORTS: Sharing information and collaborating with other businesses, financial institutions, and law enforcement agencies can enhance fraud detection capabilities by providing access to a broader network of data and expertise.

8. CUSTOMER EDUCATION: Educating customers about common fraud schemes, providing guidance on secure online practices, and encouraging vigilance when sharing personal and financial information can help reduce the likelihood of falling victim to fraud.

Incorporating a multi-layered approach that combines various fraud detection techniques is essential for effectively combating the evolving threats posed by online shopping fraud. By staying proactive, leveraging technological advancements, and fostering collaboration within the industry, businesses can better protect themselves and their customers against fraudulent activities in the digital marketplace. Online fraud is a persistent threat in the digital age, characterized by various deceptive practices aimed at unlawfully obtaining sensitive information or financial assets from individuals or organizations. These scams can take many forms, including phishing, identity theft, credit card fraud, and investment scams. Despite advancements in cybersecurity measures, online fraudsters continually adapt their tactics, making it challenging to eradicate completely. To combat this menace effectively, a multi-faceted approach involving robust cybersecurity protocols, user education, legislative measures, and collaboration between governments, law enforcement agencies, and technology companies is crucial. Furthermore, individuals must remain vigilant, practicing safe online habits such as verifying the authenticity of websites and avoiding sharing personal information indiscriminately. Ultimately, while it may not be possible to eliminate online fraud entirely, concerted efforts can mitigate its impact and protect individuals and businesses from falling victim to these schemes.

REFERENCES

1. *Chan, P. K., Fan, W., Prodromidis, A. L., & Stolfo, S. J. (2001). Distributed data mining in credit card fraud detection. IEEE Intelligent Systems, 16(4), 67-74. DOI: 10.1109/5254.941352*
2. *Folorunso, O., & Misra, S. (2017). Credit card fraud detection using machine learning: A survey. Journal of Big Data, 4(1), 1-33. DOI: 10.1186/s40537-017-0091-8*
3. *Sun, J., & Meng, X. (2015). Credit card fraud detection: a novel approach using a reduced feature set. Knowledge-Based Systems, 89, 385-396. DOI: 10.1016/j.knosys.2015.08.027*
4. *Juszczyszyn, K., & Hoang, D. B. (2016). Fraud detection in e-commerce: A focused literature review and research agenda. Journal of Theoretical and Applied Electronic Commerce Research, 11(1), 22-39. DOI: 10.4067/S0718-18762016000100004*
5. *Khayati, M., Samé, A., & Boughanmi, M. (2018). A survey of credit card fraud detection techniques: Data and technique oriented perspective. Journal of Information Security and Applications, 39, 169-189. DOI: 10.1016/j.jisa.2018.03.008*

6. *Ma, Y., Liu, Y., & Wang, H. (2017). A survey of credit card fraud detection research. International Journal of Information Management, 37(5), 227-245. DOI: 10.1016/j.ijinfomgt.2017.03.007*
7. *Phua, C., Lee, V. C., Smith, K., & Gayler, R. (2005). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 24(4), 431-457. DOI: 10.1007/s10462-005-3569-4*
8. *Rosales-Pérez, A., Carrasco-Ochoa, J. A., Martínez-Trinidad, J. F., & Kittler, J. (2016). Credit card fraud detection using clustering and genetic programming. Expert Systems with Applications, 56, 180-194. DOI: 10.1016/j.eswa.2016.02.040*
9. *"Fraud Detection Techniques in Online Shopping: A Comprehensive Review", Smith, J., Johnson, A., & Williams, R.,Cybersecurity Research Institute, 2023*
10. *"Advancements in Fraud Detection: A Study of Techniques in Online Shopping", Gupta, S., Patel, R., & Singh, M., International Journal of Cybersecurity,2020*
11. *"Emerging Trends in Fraud Detection Technologies for Online Retailers", Lee, H., Kim, C., & Park, S.,Journal of Information Security, 2019*
12. *"Enhancing Security: Innovations in Fraud Detection for E-commerce Platforms", Chen, L., Wang, Y., & Liu, Q., IEEE Transactions on Dependable and Secure Computing, 2018*
13. *"State-of-the-Art in Fraud Detection Methods for Online Shopping Platforms",Rodriguez, M., Gonzalez, P., & Martinez, E., ACM Transactions on Internet Technology,2017*
14. *"A Survey of Fraud Detection Techniques in E-commerce: Trends and Perspectives", Kim, J., Lee, S., & Park, H.,Journal of Computer Security, 2015*