



Journal of Economics Education and Entrepreneurship

Vol. 7, No. 1, April 2026, pp. 40-50

<https://ppjp.ulm.ac.id/journals/index.php/jee/issue/view/984>

ISSN: 2746-5438 (Print) | 2745-729X (Online)



Fraud Detection Methods in Addressing Cyber Threats: A Systematic Literature Review in the Banking Sector

^{1*}Willa Putri Malinda Buchori, ²Betanika Nila Nirbita, ³Muhammad Alif Nur Irvan,
⁴Nadia Husnaningtyas, ⁵Adila Durrotul Ghina

^{1,2,4} Universitas Negeri Yogyakarta, Indonesia

³ Universitas Sebelas Maret, Indonesia

⁵ Universitas Palangka Raya, Indonesia

Article Info

Keywords:

Cybercrime
Fraud Detection
Banking Security
Fraud Detection Methods

ABSTRACT

This research was conducted in order to determine the method of fraud detection. The method used in this research is Systematic Literature Review (SLR) with PRISMA Protocol. The steps taken include identification, screening, feasibility testing, and finalization of relevant studies from various leading databases such as Google Scholar, Scopus, Web of Science, Emerald, and IEEE Xplore. The results of the study identified eight main methods of fraud detection, namely big data analysis, machine learning algorithms, Natural Language Processing (NLP); Accounting Information Systems, Extremely Randomized Trees (ERT), rule-based systems, blockchain technology, Asexual Reproduction Optimization (ARO), Bayesian A/B testing, and authentication systems. These methods show varying degrees of effectiveness in detecting suspicious transactions and reducing the risk of digital fraud. The research findings not only discuss fraud detection methods but also analyze the weaknesses and advantages of each method. The findings can be used as a practical reference source in preventing fraud by conducting fraud detection based on the right method.

This is an open access article under the CC-BY-SA 4.0



*Corresponding Author:

Willa Putri Malinda Buchori

Vocational Faculty, Universitas Negeri Yogyakarta

Jl. Mandung Pengasih Kulonprogo Yogyakarta, Indonesia 55652

Email: willaputri@uny.ac.id

Submitted 12 February 2026; Accepted 27 February; Published 30 April 2026

How to cite: Buchori, W. P. M., Nirbita, B. N., Irvan, M. A. N., Husnaningtyas, N., & Ghina, A. D. (2026). Fraud Detection Methods in Addressing Cyber Threats: A Systematic Literature Review in the Banking Sector. *Journal of Economics Education and Entrepreneurship*, 7(1), 40-50. <https://doi.org/10.20527/jee.v7i1.18299>.

1. INTRODUCTION

Crimes that occur in cyberspace are increasingly prevalent. This crime is called cybercrime. Cyber-crime requires computer network technology to carry out its actions (Maimon et al. 2015). The increasing accessibility of the internet allows cybercriminals to target victims from various locations without geographical boundaries. Their modus operandi continues to evolve,

Journal homepage: <https://ppjp.ulm.ac.id/journals/index.php/jee>

<https://doi.org/10.20527/jee.v7i1.18299>

Copyright © Authors, 2026, ISSN: 2746-5438 (Print) | 2745-729X (Online)

ranging from technical attacks to psychological exploitation through social engineering. In addition, the complexity of security systems, which are not always able to keep pace with the speed of criminal innovation, further increases user vulnerability. The high rate of cybercrime is directly proportional to the increasing number of people who use digital technology (Suri et al. 2024). This group is considered to tend to be cashless because it is considered simpler when they want to make financial transactions. Of course, this requires the internet. The development of increasingly sophisticated technology is also accompanied by increasingly sophisticated crimes (Ahmad, Khan, and Iqbal 2024). Without an adequate security system, data will be more vulnerable to leakage. Digital crime has also entered the banking industry (Cele and Kwenda 2025). This condition makes it easier for criminals to commit data theft, hacking, and financial theft. If this is not addressed with maximum effort, it is possible that interest in using online transactions will decrease in the future period. This is due to the decline in the level of public trust in the banking sector due to the fear of cyber-crime (Lestari et al. 2024).

The cost of losses due to cybercrime globally is: \$190.00 every second, \$11.4 million every minute, \$684.9 million every hour, \$16 billion every day, \$115.4 billion every week, \$500 billion every month, also \$6 trillion per year (Cele and Kwenda 2025). These figures not only illustrate the magnitude of the financial impact, but also indicate the systematic and organized scale of cybercrime activities. These recurring and increasing losses further emphasize the urgency of developing more responsive and adaptive fraud detection and prevention systems. Cybercriminals generate an ever-increasing annual income, if left unchecked, by 2028 it is predicted to reach \$1.5 trillion (Ahmad, Khan, and Iqbal 2024). In 2018 in August until 2023 in February, it was found by the Indonesian Ministry of Communication and Information Technology, there were 1,730 cases of online fraud (Lestari et al. 2024). According to the UK Financial Fraud Report 2022, more than £1.2 billion was stolen through 78% online fraud, while the banking sector managed to prevent an additional £1.2 billion in losses, with remote purchase fraud, such as the use of stolen cards online accounting for £395.7 million in losses (Khalid et al. 2024).

Phishing and malware belong to the types of fraud that are carried out by utilizing the existence of the internet (Cole 2023). Phishing and malware have differences. Phishing deceives the victim by utilizing the website visited by the victim and that is where the victim's confidential information will be obtained by the perpetrator without the victim realizing it (Cole 2023). The hacker will carry out the action after he enters the system and attacks the victim. The perpetrator will share a link that needs to be accessed by the victim. It usually begins with a threatening sentence of lies as a social engineering tactic (Maimon et al. 2015). Forms such as prize draws, online ordering, and so on where the perpetrator will act as if the official party contacting the victim. In the end, the perpetrator will ask for important data such as the victim's password for this purpose. Meanwhile, the real practice carried out by the perpetrator is to use the password to access the theft needs carried out. For example, ATM pins and other pins. Phishing can be done through a variety of different media using different vectors, three media commonly used for phishing, namely the internet, short message service, and voice (Naqvi et al. 2023).

Since the appearance of the first Android malware in 2010 that tricked users into premium SMS subscriptions, the number of malware has exploded from 22,088 in 2012 to more than 33 million in 2023 (Sharma and Arora 2024). Malware often called malicious software is malicious code that is harmful and damaging to computer systems, digital systems, and mobile and electronic devices, its purpose is to damage digital systems and steal valuable information (Smmarwar, Gupta, and Kumar 2024). Its ability to damage the system causes errors on computers or even cell phones. This is done to intercept various information needed to penetrate

privacy access. Therefore, its position poses a threat to the security as well as the durability of data.

Financial services have been a target for fraud for many years, along with the high number of financial transactions conducted online, and the increase in online crimes as well (Sathisha and Sowmya 2023). Online financial transactions mean that many people have utilized digital transactions, so criminals can commit theft remotely without having to physically touch the victim. The crime needs to be committed with sufficient skill. Financial institutions have tried to find solutions to overcome these problems by utilizing fraud detection technology from various methods (Khatti and Singh 2018). For example, by utilizing Artificial Intelligence (AI) to detect fraud early by looking at unusual transactions (Bansal, Paliwal, and Singh 2025). The unusual transaction will be suspected by the way the bank will send a notification of proof of transfer to our e-mail or notification of the e-banking application.

Various cases are rampant, banks must strengthen the security system to protect the impact of the dangers that will be experienced by their customers (Ahmad, Khan, and Iqbal 2024). Special efforts are needed that are more serious in overcoming these problems. Although there are already systems that are considered capable of detecting fraud, the public still needs a more sophisticated system (Khatti and Singh 2018). The high number of cases that continue to occur indicates that detection techniques are not maximized. This research will explore methods of detecting fraud in financial transactions to fight crime in the banking sector. Therefore, it is important to know what methods are used to detect fraud in the banking sector.

2. METHOD

Qualitative approach is the approach adopted in the study. Qualitative research is research that is carried out by relying on humans on events in the form of facts that occur in the surrounding environment (Adiwijaya et al. 2024). The approach used the Systematic Literature Review (SLR) method. This approach is used to establish the identity and select studies related to a particular research question to be evaluated and summarized in a fair, thorough, and transparent manner (Monge and Domingo 2024). SLR enables researchers to systematically identify, assess, and interpret all relevant evidence in accordance with established protocols, so that the results of the review are scientifically accountable. In addition, the rigorous selection process in SLR also helps minimize bias and ensures that the previous studies used are truly representative and of high quality. SLR helps in synthesizing all available scientific research conducted by researchers in different cities and fields of study. It can provide clear evidence on research questions in a transparent manner, which can be reproduced for future research (Sneha and Kavitha 2024). This study intends to show fraud detection methods by compiling and reviewing various literature sources, such as books, journals, articles, and official reports. The focus of the data sources used in this research is using reputable journals.

The flow of SLR uses the “PRISMA Protocol” to plan, identify, and evaluate, summarize data from various reading materials, and ensure the effectiveness of research that is transparent so that it can be used as a reference. The sequence of using the prism protocol includes identification, screening of readings, feasibility testing, and the final stage (Monge and Domingo 2024). Each stage is carried out sequentially.



Figure 1. PRISMA Control Stages

The first step in applying the PRISMA protocol is identifying potential literature sources. This process is designed to gather broad preliminary data from various reliable academic databases to ensure comprehensive study coverage. The identification phase involved an extensive search for harmonized literature across multiple databases (Emran and Rubel 2024). The identification stage involved an extensive search for relevant literature in various databases, including Google Scholar, Scopus, Web of Science, Emerald, and IEEE Xplore. The identification process is accompanied by entering relevant keywords, namely fraud detection methods. At this stage, a search with these keywords found 729,000 results in Google Scholar, 6,594 in Scopus, 4,057 in Web of Science, more than 4,000 in Emerald, and 3,042 in IEEE Xplore (see Table 1).

Table 1. Identification Stage

No	Publisher	Number of Articles
1	Google Scholar	729,000
2	Scopus	6,594
3	Web of Science	4,057
4	Emerald	>4,000
5	IEEE Xplore	3,042

Source: Created by the author, 2025

After the potential literature has been successfully collected, the next step is to screen it to ensure the quality and relevance of the studies to be analyzed. This process involves a systematic review of titles and abstracts based on predetermined inclusion and exclusion criteria. The next stage is to screen the readings. There are criteria set in conducting the screening process to determine the suitability of the reading title and abstract (Emran and Rubel 2024). The criteria in this research are peer-reviewed and focus on fraud detection in the banking system in the range of 2020 to 2025. The selection of this year is relevant to the current conditions. At this stage, a search with these keywords found 17,000 results in Google Scholar, 165 in Scopus, 134 in Web of Science, more than 1,000 in Emerald, and 253 in IEEE Xplore (see Table 2).

Table 2. Identification Stage

No	Publisher	Number of Articles
1	Google Scholar	17,000
2	Scopus	165
3	Web of Science	134
4	Emerald	>1,000
5	IEEE Xplore	253

Source: Created by the author, 2025

The next stage is to conduct feasibility testing. Due diligence focused on ensuring that the research addressed the research objectives and provided sufficient methodological detail (Emran and Rubel 2024). At the due diligence stage, 12 articles were found. The last step is the finalization stage that meets all the criteria. In the finalization stage, 8 articles were used. This was done to qualify based on thematic relevance to the research objectives (Emran and Rubel 2024). The eight articles were selected because they consistently discuss methods of detecting fraud in the banking context using a variety of approaches, ranging from big data analysis to rule-based systems. This finalization process ensures that the included studies are not only relevant but also make a substantive contribution to the understanding of developments in fraud detection technology. Thus, the synthesis of the results obtained can be used as a strong foundation for further analysis. This final selection also takes into account the balance between

breadth of coverage and depth of discussion, so that the resulting literature review is comprehensive and focused.

3. RESULTS AND DISCUSSION

3.1 Results

Fraud is often defined as a deception that violates the rules because it is wrong and is a criminal act because it is used for financial or personal gain, but harms others (Hashemi, Mirtaheeri, and Greco 2023). Fraud is an act of cheating. Fraud in modern financial systems is a perennial and growing problem, causing significant losses to individuals, institutions, and economies (Sathisha and Sowmya 2023). Financial fraud has harmed banking customers because the banking security system was successfully hacked by irresponsible people. The banking sector continues to be faced with threats to data security, ranging from phishing and ransomware attacks to malware attacks and data breaches that result in the risk of customer data theft (Johora et al. 2024). The rampant fraud in the banking industry requires further handling in the form of fraud detection systems without compromising data and still complying with legal regulations (Aljunaid et al. 2025). Online banks have embraced a variety of security measures, including encryption and multifactor authentication, to safeguard customers' finances, but concerns about hidden fees, account breaches, and perceived complexity of information remain (Lestari et al. 2024).

Modern banking transaction data is extremely complex and voluminous, making manual analysis unrealistic to perform efficiently. The limitations of conventional methods necessitate a computational approach that can process data automatically and intelligently. Artificial intelligence and machine learning-based technologies are considered solutions capable of overcoming these challenges by analyzing hidden patterns in large-scale data. Banking data has a large volume with datasets containing large amounts of transaction data, manually reviewing and searching for fraudulent transaction patterns is not possible or takes a long time, so machine learning-based algorithms can function in fraud detection and prediction (Hashemi, Mirtaheeri, and Greco 2023). Fraud that occurs involves sophisticated technology such as AI. The use of AI is empowered in auditing and fraud detection and has gained significant attention in recent years due to its potential to detect fraud patterns faster and with higher accuracy than traditional auditing methods (Qatawneh 2024). The advantage of AI lies in its ability to continuously learn from new data, allowing the system to adapt to ever-evolving fraud tactics. In addition, AI can operate in real time, enabling more proactive threat identification before financial losses occur. Thus, AI integration not only improves detection accuracy, but also strengthens the overall fraud prevention system in the banking sector.

Based on searches that have been conducted on Scopus, Web of Science, Emerald, and IEEE Xplore, and Google Scholar using PRISMA, 8 articles discussing fraud detection methods were finalized. The 8 articles span the years 2018 to 2024. The fraud detection methods vary from one article to another. In 2018, there was research conducted by Khattri & Singh (2018), resulting in the findings of fraud detection methods with authentication type. Then, in 2022, research conducted by Westland (2022), found that fraud detection methods can be done with A/B Bayesian testing. In the same year, Asexual Reproduction Optimization (ARO) can be a tool in detecting fraud (Ghahfarokhi et al. 2022). Developing again in the following year, namely in 2023, that Singh et al., (2023) found blockchain has the ability as well. Furthermore, research by Sathisha & Sowmya (2023), that rule-based systems can be utilized. Research conducted by Riskiyadi (2024), said that Extremely Randomized Trees (ERT) is a method in fraud detection. Qatawneh (2024), said that fraud detection would be easier if it was carried out with the help of an accounting information system. Finally, research from Emran & Rubel

(2024), that big data analysis, machine learning algorithms, and Natural Language Processing (NLP) are utilized in fraud detection. A summary of fraud detection methods is presented in the table 3.

Table 3. Fraud Detection Methods

No	Researcher	Methods
1	Emran & Rubel (2024)	Big data analysis, algoritma machine learning, and Natural Language Processing (NLP)
2	Qatawneh (2024)	Accounting information system
3	Riskiyadi (2024)	Extremely Randomized Trees (ERT)
4	Sathisha & Sowmya (2023)	Rule based system
5	Singh et al., (2023)	Blockchain
6	Ghahfarokhi et al. (2022)	Asexual Reproduction Optimization (ARO)
7	Westland (2022)	Pengujian A/B Bayesian
8	Khatti & Singh (2018)	<i>Authentication type</i>

Source: Created by the author, 2025

3.2 Discussion

The first method discovered was big data analysis, machine learning algorithms, and Natural Language Processing (NLP) (Emran and Rubel 2024). Big data analysis is the process of analyzing large and complex data sets using techniques such as data mining, machine learning, and predictive analytics to discover actionable patterns, correlations, and trends (Udeh et al. 2024). Big data analysis with clustering and outlier detection techniques enables institutions to identify subtle patterns that are not visible through traditional methods (Emran and Rubel 2024). Big data will analyze a person's mindset by collecting raw data, which is then used to make decisions in the form of solutions. Machine learning algorithms are capable of detecting fraud in real time by analyzing patterns and anomalies in historical transaction data and adapting to changes in fraud tactics, providing more effective defense than traditional rule-based systems (Obeng et al. 2024). Machine learning algorithms with clustering such as k-means and DBSCAN are often used to identify anomalies by grouping similar transactions (Emran and Rubel 2024). In addition, there is NLP. The use of NLP facilitates not only the extraction of relevant information in complex textual reports, but also improves analysis and trend recognition because NLP works by converting words into numbers and those numbers are used to create a program (Lázaro et al. 2025). One such program is fraud detection. Natural language processing (NLP) in handling large amounts of textual information from emails, contracts, and social media, and real-time analysis can be used as a tool to detect fraud instantly (Emran and Rubel 2024).

The second method is the Accounting Information System (AIS) (Qatawneh 2024). AIS plays an important role in detecting fraud because the system is capable of collecting, processing, and storing financial data, which can be analyzed to identify unusual patterns and anomalies that may indicate fraudulent activity (Qatawneh 2024). The process involves analyzing data on unusual transactions, then identifying potential fraud. Fraud detection using AIS will certainly minimize potential losses. AIS assists in fraud detection by collecting and analyzing financial data in real-time, finding suspicious patterns, and supporting internal controls and audits to prevent losses resulting from fraud (Qatawneh 2024). Real-time means that the system immediately checks transactions as they occur, while suspicious patterns refer to unusual habits such as irregular transactions and unusual locations. AI in SIA uses several indicators, such as data collection, data analysis, risk assessment, detection, prevention, and investigation (Qatawneh 2024). The involvement of technologies such as AI can be utilized to detect fraud more effectively (Emran and Rubel 2024). Fraud detection is necessary when a

fraudster attempts to carry out a fraudulent transaction (Hashemi, Mirtaheri, and Greco 2023). This is done to minimize the possibility of fraud occurring.

The third method is Extremely Randomized Trees (ERT) (Riskiyadi 2024). ERT is a more random version of Random Forest (RF) that randomly selects data divisions and uses all training data, making it faster and less prone to overfitting because it avoids excessive dependence on data (Kennedy et al. 2024). The results of the research conducted by Riskiyadi in 2024 show that ERT has the best performance compared to other models because it has the best performance for each treatment (Riskiyadi 2024). The Extremely Randomized Trees (ERT) model performs better than other machine learning models (Riskiyadi 2024). This is because ERT has scattered and random split points, resulting in more consistent predictions. This condition makes ERT faster, more accurate, and less prone to disruption.

The fourth method is the rule-based system (Sathisha and Sowmya 2023). Rule-based systems in fraud detection use fixed parameters such as transaction value, location, and user behavior to identify potential fraud. Although limited in capturing complex patterns, they offer the advantages of transparency and ease of interpretation (Khanum 2024). Rule-based systems use predetermined rules and criteria to identify suspicious transactions, statistical analysis to identify patterns and anomalies that may indicate fraud in large volumes, and expert systems that rely on human expertise and knowledge to identify fraud (Sathisha and Sowmya 2023). This system is better used to detect known fraud, not fraud that changes patterns too often. When a rule is violated, the system will immediately close access, but if the violation does not become a rule recorded in the system, the system will not close access.

The fifth method is blockchain, which is capable of detecting fraud because the system is considered secure and transparent (Singh, Singh, and Kajla 2023). Blockchain is a point-to-point distributed ledger based on cryptography and a network sharing system characterized by disintermediation, transparency, and openness (Liang et al. 2022). This system is like a digital cash book and can be accessed by each of its members, so that all parties involved can verify the validity of the transactions that occur. This condition makes it difficult to falsify transactions. When there is an outgoing or incoming transaction, the blockchain will first check and make a record in the appropriate ledger. Its encryption system will record all activities, including in the event of financial data theft. In addition, blockchain has the ability to detect counterfeit goods, and transaction records are difficult to delete using this method (Kayani 2025). This capability is vital in the supply chain to ensure product authenticity and absolute auditability. With a permanent digital trail, every stage of a product's journey can be tracked and validated, creating a more trustworthy environment. Blockchain improves data security through a decentralized system that guarantees integrity, permanence, and transparency, while simplifying the transaction process by reducing the risk of fraud (Kapadiya et al. 2025).

The sixth method is Asexual Reproduction Optimization (ARO) (Ghahfarokhi et al. 2022). ARO is an intelligent algorithm inspired by asexual reproduction (such as bacterial division) and works to detect fraud by cloning and mutating the best existing solutions to produce a variety of new solutions. ARO automatically detects fraud without the need for manual settings. Asexual Reproduction Optimization (ARO) is superior to SIA because it can reduce training time by up to 75% (Ghahfarokhi et al. 2022). The ARO process involves creating numerous identical branches to facilitate fraud detection.

The seventh method is Bayesian A/B testing, which is capable of calculating losses on sales and time (Westland 2022). This allows analysts to not only determine which option is superior, but also estimate the opportunity cost of making the wrong choice. Calculating these losses is a critical added value for risk mitigation-oriented business decisions. The Bayesian model is a statistical approach that combines prior knowledge with observational data to make more accurate predictions while measuring the level of uncertainty in the results (Buonaguidi

et al. 2022). The most important feature of Bayesian networks is their ability to encode qualitative and quantitative information with new data even when information is incomplete, and they are more transparent than other methods thanks to clear conditional probability diagrams (Mazal et al. 2025). Visualization through diagrams helps communicate problem structures and cause-and-effect relationships effectively. This level of transparency reduces interpretation bias and facilitates collaboration between teams with different expertise backgrounds.

The eighth method is the authentication type technique (Khattri and Singh 2018). Authentication type is an online transaction security system that has three levels of verification (high, medium, low) where the high level will strictly check all transaction parameters, while the low level only monitors several important parameters, with the system marking transactions as suspicious if they are found to be inconsistent with the user's normal transaction patterns (Khattri and Singh 2018). When a large transaction occurs and the transaction amount is not the usual amount, the system will request extra data verification to ensure that the transaction is not being carried out by a criminal. The figure of 12.73% in the research results shows that it is very important to have an identified system and a system with strong authentication (Ahmad, Khan, and Iqbal 2024). This means that a strong identity verification system is very important to stop fraud.

4. CONCLUSION

The development of digital technology is increasing, along with cybercrime. Especially for individuals who often conduct online transactions, such as the use of e-banking. Criminals will utilize the online media to absorb maximum profits regardless of the losses of the victim. The method usually used by criminals, namely phishing and malware, is to hit victims with fake links to obtain privacy data from victims. On the other hand, fraud cases in the financial sector are increasing rapidly. This condition encourages the banking sector to utilize technological assistance in the form of AI to detect transactions that are considered unusual. Therefore, banks need to have several options in detecting fraud to protect customers from the danger of theft.

Fraud detection methods continue to develop and vary. Based on the results of previous research, there are detection methods that are considered capable of working effectively. There are 8 articles used for finalization. These methods include big data analysis with machine learning and NLP algorithms (Emran and Rubel 2024), accounting information systems (Qataweh 2024), extremely randomized trees (Riskiyadi 2024), rule-based systems (Sathisha and Sowmya 2023), secure and transparent blockchain technology (Singh, Singh, and Kajla 2023), asexual reproduction optimization (Ghahfarokhi et al. 2022), A/B Bayesian testing to calculate losses (Westland 2022), and authentication systems (Khattri and Singh 2018). These types of methods have their own advantages and disadvantages. Therefore, it is better to use various detection methods as a layer of protection for a system.

REFERENCES

- Adiwijaya, Saputra, Anugerah Tatema Harefa, Santi Isnaini, Syarifa Raehana, Budi Mardikawati, Rudy Dwi Laksono, Saktisyahputra, et al. 2024. *Buku Ajar Metode Penelitian Kualitatif*. Pertama. Jambi: PT. Sonpedia Publishing Indonesia.
- Ahmad, Iftikhar, Salim Khan, and Shahid Iqbal. 2024. "Guardians of the Vault: Unmasking Online Threats and Fortifying e-Banking Security, a Systematic Review." *Journal of Financial Crime* 31, no. 6: 1485–1501. <https://doi.org/10.1108/JFC-11-2023-0302>.
- Aljunaid, Saif Khalifa, Saif Jasim Almheiri, Hussain Dawood, and Muhammad Adnan Khan. 2025. "Secure and Transparent Banking: Explainable AI-Driven Federated Learning

- Model for Financial Fraud Detection.” *Journal of Risk and Financial Management* 18, no. 179: 1–26. <https://doi.org/10.3390/jrfm18040179>.
- Bahnsen, Alejandro Correa, Djamila Aouada, Aleksandar Stojanovic, and Björn Ottersten. 2016. “Feature Engineering Strategies for Credit Card Fraud Detection.” *Expert Systems with Applications* 51: 134–42. <https://doi.org/10.1016/j.eswa.2015.12.030>.
- Bansal, Kapil, Aseem Chandra Paliwal, and Arun Kumar Singh. 2025. “Analysis of the Benefits of Artificial Intelligence and Human Personality Study on Online Fraud Detection.” *International Journal of Law and Management* 67, no. 2: 191–209. <https://doi.org/10.1108/IJLMA-08-2023-0198>.
- Buonaguidi, Bruno, Antonietta Mira, Herbert Bucheli, and Viton Vitonis. 2022. “Bayesian Quickest Detection of Credit Card.” *Bayesian Analysis* 17, no. 1: 261–90.
- Cele, Natile Nonhlanhla, and Sheila Kwenda. 2025. “Do Cybersecurity Threats and Risks Have an Impact on the Adoption of Digital Banking? A Systematic Literature Review.” *Journal of Financial Crime* 32, no. 1: 31–48. <https://doi.org/10.1108/JFC-10-2023-0263>.
- Cole, Tessa. 2023. “How Are Financial Institutions Enabling Online Fraud? A Developmental Online Financial Fraud Policy Review.” *Journal of Financial Crime* 30, no. 6: 1458–73. <https://doi.org/10.1108/JFC-10-2022-0261>.
- Emran, A. K. M., and Md. Tauhid Hossain Rubel. 2024. “Big Data Analytics and AI-Driven Solutions for Financial Fraud Detection: Techniques, Applications, and Challenges.” *Frontiers in Applied Engineering and Technology* 1, no. 01: 269–85. <https://doi.org/10.70937/fact.v1i01.40>.
- Ghahfarokhi, Anahita Farhang, Taha Mansouri, Mohammad Reza Sadeghi Moghaddam, Nila Bahrambeik, Ramin Yavari, and Mohammadreza Fani Sani. 2022. “Credit Card Fraud Detection Using Asexual Reproduction Optimization.” *Kybernetes* 51, no. 9: 2852–76. <https://doi.org/10.1108/K-04-2021-0324>.
- Halvaiee, Neda Soltani, and Mohammad Kazem Akbari. 2014. “A Novel Model for Credit Card Fraud Detection Using Artificial Immune Systems.” *Applied Soft Computing* 24, no. 1: 40–49. <https://doi.org/10.1016/j.asoc.2014.06.042>.
- Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. 2023. “Fraud Detection in Banking Data by Machine Learning Techniques.” *IEEE Access* 11, no. 1: 3034–43.
- Johora, Fatema Tuz, Rakibul Hasan, Jahanara Akter, Sayeda Farjana Farabi, and Md Abdullah Al Mahmud. 2024. “AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions.” *The American Journal of Management and Economics Innovations* 6, no. 6: 8–22.
- Kapadiya, Khyati, Fenil Ramoliya, Keyaba Gohil, Usha Patel, and Rajesh Gupta. 2025. “Blockchain-Assisted Healthcare Insurance Fraud Detection Framework Using Ensemble Learning.” *Computers and Electrical Engineering* 122: 1–18. <https://doi.org/10.1016/j.compeleceng.2024.109898>.
- Kayani, Umar Nawaz. 2025. “Exploring Prospects of Blockchain and Fintech: Using SLR Approach.” *Journal of Science and Technology Policy Management* 16, no. 1: 5–41. <https://doi.org/10.1108/JSTPM-01-2023-0005>.
- Kennedy, Robert K.L., Flavio Villanustre, Taghi M. Khoshgoftaar, and Zahra Salekshahrezaee. 2024. “Synthesizing Class Labels for Highly Imbalanced Credit Card Fraud Detection Data.” *Journal of Big Data* 11, no. 38: 1–22. <https://doi.org/10.1186/s40537-024-00897-7>.
- Khalid, Abdul Rehman, Nsikak Owoh, Omair Uthmani, Moses Ashawa, Jude Osamor, and John Adejoh. 2024. “Enhancing Credit Card Fraud Detection with Light Gradient-

- Boosting Machine: An Advanced Machine Learning Approach.” *Big Data and Cognitive Computing* 8, no. 6: 1–27. <https://doi.org/10.1109/ICKECS61492.2024.10616809>.
- Khanum, Arshiya. 2024. “Fraud Detection in Financial Transactions : A Machine Learning Approach vs . Rule-Based Systems.” *International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, 1–5. <https://doi.org/10.1109/IITCEE59897.2024.10467759>.
- Khattari, Vipin, and Deepak Kumar Singh. 2018. “Parameters of Automated Fraud Detection Techniques during Online Transactions.” *Journal of Financial Crime* 25, no. 3: 702–20. <https://doi.org/10.1108/JFC-03-2017-0024>.
- Lázaro, Flávio L., Tomás Madeira, Rui Melicio, Duarte Valério, and Luís F.F.M. Santos. 2025. “Identifying Human Factors in Aviation Accidents with Natural Language Processing and Machine Learning Models.” *Aerospace* 12, no. 106: 1–20. <https://doi.org/10.3390/aerospace12020106>.
- Lestari, Sri, Wiwiek Rabiatur Adawiyah, Arina Laksita Alhamidi, Joni Prayogi, and Ronald Haryanto. 2024. “Navigating Perilous Seas: Unmasking Online Banking Frauds, Perceived Usefulness, Fear of Cybercrime and Distrust in Online Banking.” *Safer Communities* 23, no. 4: 444–64. <https://doi.org/10.1108/SC-04-2024-0018>.
- Liang, Wei, Lijun Xiao, Ke Zhang, Mingdong Tang, and Dacheng He. 2022. “Data Fusion Approach for Collaborative Anomaly Intrusion Detection in Blockchain-Based Systems.” *IEEE Internet of Things Journal* 9, no. 16: 14741–51. <https://doi.org/10.1109/JIOT.2021.3053842>.
- Maimon, David, Theodore Wilson, Wuling Ren, and Tamar Berenblum. 2015. “On the Relevance of Spatial and Temporal Dimensions in Assessing Computer Susceptibility to System Trespassing Incidents.” *British Journal of Criminology* 55, no. 3: 615–34. <https://doi.org/10.1093/bjc/azu104>.
- Mazal, Jaber Awad, Arezoo Aghaei Chadegani, Mohammad Samir Dehirab Al-Rubai, and Mohammad Alimoradia Alimoradi. 2025. “Predicting the Manipulation of Financial Statements of Tehran Stock Exchange Companies Using the Benish Model and Bayesian Networks.” *International Journal Nonlinear Analysis and Applications*, 1–11.
- Monge, Calderon-Monge, and Ribeiro-Soriano Domingo. 2024. *The Role of Digitalization in Business and Managment: A Systematic Literature Review. Review of Managerial Science*. Vol. 18. Springer Berlin Heidelberg. <https://doi.org/10.1007/s11846-023-00647-8>.
- Naqvi, Bilal, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeki, and Jari Porras. 2023. “Mitigation Strategies against the Phishing Attacks: A Systematic Literature Review.” *Computers and Security* 132, no. 103387: 1–25. <https://doi.org/10.1016/j.cose.2023.103387>.
- Obeng, Shadrack, Toluwalase Vanessa Iyelolu, Adetola Adewale Akinsulire, and Courage Idemudia. 2024. “Utilizing Machine Learning Algorithms to Prevent Financial Fraud and Ensure Transaction Security.” *World Journal of Advanced Research and Reviews* 23, no. 1: 1972–1980 In.
- Qatawneh, Adel M. 2024. “The Role of Artificial Intelligence in Auditing and Fraud Detection in Accounting Information Systems: Moderating Role of Natural Language Processing.” *International Journal of Organizational Analysis*, 1–19. <https://doi.org/10.1108/IJOA-03-2024-4389>.
- Riskiyadi, Moh. 2024. “Detecting Future Financial Statement Fraud Using a Machine Learning Model in Indonesia: A Comparative Study.” *Asian Review of Accounting* 32, no. 3: 394–422. <https://doi.org/10.1108/ARA-02-2023-0062>.

- Sathisha, H. K., and G. S. Sowmya. 2023. "Detecting Financial Fraud in the Digital Age: The AI and ML Revolution." *International Journal For Multidisciplinary Research* 5, no. 5: 1–12. <https://doi.org/10.36948/ijfmr.2023.v05i05.6139>.
- Sharma, Yash, and Anshul Arora. 2024. *A Comprehensive Review on Permissions-Based Android Malware Detection*. *International Journal of Information Security*. Vol. 23. Springer Berlin Heidelberg. <https://doi.org/10.1007/s10207-024-00822-2>.
- Singh, Satinder, Sarabjeet Singh, and Tanveer Kajla. 2023. "Checking the Effectiveness of Blockchain Application in Fraud Detection with a Systematic Literature Review Approach." In *Contemporary Studies of Risks in Emerging Technology: Part B*, 57–86. <https://doi.org/10.1108/978-1-80455-566-820231003>.
- Smmarwar, Santosh K., Govind P. Gupta, and Sanjay Kumar. 2024. "Android Malware Detection and Identification Frameworks by Leveraging the Machine and Deep Learning Techniques: A Comprehensive Review." *Telematics and Informatics Reports* 14: 1–18. <https://doi.org/10.1016/j.teler.2024.100130>.
- Sneha, Venkatesh, and R. Kavitha. 2024. "Exploring the Economy of Creativity and Culture in the Light of Industry 5.0: A Systematic Literature Review of the Setup of Creative Industries." *Journal of Strategy and Management*, 1–25. <https://doi.org/10.1108/JSMA-05-2023-0095>.
- Suri, Ankit, Yogesh Sharma, Lokesh Jindal, and Rajeev Sijariya. 2024. "Blockchain for Data Protection and Cyber Fraud Reduction: Systematic Literature Review and Technology Adoption Dynamics among Gen Y and Z." *International Journal of Quality and Reliability Management* 41, no. 8: 2181–98. <https://doi.org/10.1108/IJQRM-03-2023-0094>.
- Udeh, Ezekiel Onyekachukwu, Prisca Amajuoyi, Kudirat Bukola Adeusi, and Anwulika Ogechukwu Scott. 2024. "The Role of Big Data in Detecting and Preventing Financial Fraud in Digital Transactions." *World Journal of Advanced Research and Reviews* 22, no. 2: 1746–60. <https://doi.org/10.30574/wjarr.2024.22.2.1575>.
- Westland, James Christopher. 2022. "A Comparative Study of Frequentist vs Bayesian A/B Testing in the Detection of E-Commerce Fraud." *Journal of Electronic Business & Digital Economics* 1, no. 1/2: 3–23. <https://doi.org/10.1108/jebde-07-2022-0020>.