International Journal for
Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2024.0803207

Research Article

Vol. 8 issue 3 Jul-Sep 2024

Information Systems and Mechanism for Prevention of Cyber Frauds

Aftab Ahmad Malik[1], Waqar Azeem[2] and Mujtaba Asad[3]

[1] University of Kent, England
[2]Faculty of Computer Science, South Eastern Regional College, Down Patrick Ireland,
United Kingdom.
[3]Department of Automation and Control, Shanghai Jiao Tong University, Shanghai, China.

Corresponding author: dr_aftab_malik@yahoo.com

Received: Aug 05, 2024; **Accepted:** Aug 22, 2024; **Published:** Sep 12, 2024

ABSTRACT

Cyber criminals are targeting online frauds, exploiting anonymity to deceive. They use fake websites, fake ads and stolen credit or debit cards for purchases. Bank frauds, despite high-speed processing and technical assistance, can damage a bank's reputation and operational efficiency, necessitating a strong emphasis on business ethics in the banking sector. The machine learning and artificial intelligence enhance online security of information systems. US enforces anti-trust laws and promotes stakeholder rights, addressing fraud and identity theft through safety tips and civil law implementation. Cyber criminals steal personal information for unauthorized purchases, identity theft, and fraudulent activities. Machine learning and artificial intelligence can enhance online security and user awareness. AI-based threat detection analyzes network activity for cyberattacks, limiting damage. Multi-Factor Authentication (MFA) combines traditional passwords with biometric authentication for enhanced security. The application of Big Data systems allows administrations for the collection and analysis of Data and its storage obtained from various sources, using platforms like Hadoop, Apache Spark, and

Kafka for real-time processing and data analytics. Digital devices are increasingly being used in banking frauds, posing significant risks to both customers and the banking sector, necessitating stricter regulations and enforcement measures. Common banking sector issues include negligent, fraudulent, and deviant behavior, affecting various functions of getting, gathering, transporting, disbursing, loaning, trading, capitalizing, replacing, and servicing money-claims domestically and internationally. This paper discusses machine learning and anomaly detection techniques for preventing fraud in online payment systems, including behavioral profiling and Bagged Decision Tree models along with other methods.

Keywords: Cyber frauds, Information Systems, INFOSEC, Cyber Security, Financial services

1. INTRODUCTION

Fraud and white-collar crime in businesses and banking are increasing due to outdated technology. This research paper emphasizes the need for secure software and networks. Thieves use sophisticated software and technology to track and hack private information, using deceit and dishonesty to harm others. Employees often aid in scams, and legislation seems naive. Criminals flee due to secret identities, lack of evidence, poor investigation, and naive prosecution. This paper presents practical suggestions for safeguarding organizations' networks. Malik et al., [1] have discussed various aspects of frauds and fraudulent behavior.

Fraudulent activities involve securities marketing, hacking personal information, and stealing money. Law enforcement struggles, and research in accounting, society, and organizations is crucial for effective prevention and prosecution. Fraudulent activities involve securities marketing, hacking personal information, and stealing money. Law enforcement struggles, and research in accounting, society, and organizations is crucial for effective prevention and prosecution. Over the past eight decades, white-collar crime research has evolved due to high-tech advancements and computer-related office changes, but few studies have explored cybercrime.

Cybercrime, a national threat, is more prevalent among younger criminals, with different trust signs. Banks aim to attract investors through stock market investments. It describes the methods to overcome White Collar Crimes in banking and other companies [2]. It emphasized on the use of digital devices in committing crime regarding Bank Frauds [3].

InfoSec refers to the strategies and methods used to safeguard sensitive business data from unauthorized access, modification, disruption, destruction, and inspection. An international standard is a globally recognized document developed by experts from various countries, containing rules, guidelines, and processes for consistent outcomes. Three information security standards on International Standards include technical specifications. Major points of InfoSec are confidentiality, integrity, and availability, authenticity and non-repudiation. Authenticity in information security refers to the verification that data, transactions, communications, or documents are genuine. InfoSec emphasizes confidentiality, integrity, availability, authenticity, and non-repudiation, ensuring the authenticity of data, transactions, communications, or documents [4].

Information security standards outline documented processes for implementing, managing, and monitoring security controls, mitigating risk, and reducing vulnerabilities, while also ensuring regulatory compliance. Application security involves identifying and addressing vulnerabilities in web and mobile applications to prevent network breaches. Network security involves implementing policies to protect data and infrastructure, while cloud security involves off-site deployment strategies. Meeting information standards is crucial for a company's best interest. It ensures regulatory compliance, prevents cyberattacks, and helps companies implement necessary measures, processes, policies, and controls. While compliance doesn't guarantee security, it serves as a starting point for companies to adapt to evolving cyber threats.

Financial Services Firms must register with FINRA, evaluating access management, branch controls, data loss prevention, employee training, incident response, risk assessment, supplier management, system change management, technical controls, and governance. Cybercrime and White-Collar Crime differ, with different tools used by hackers and fraudsters [4]. Banks must prioritize cybersecurity to protect against these threats. Government prioritizes cyber security to enhance national security, boost consumer confidence, and ensure system reliability. Each component must be individually considered to create an effective plan.

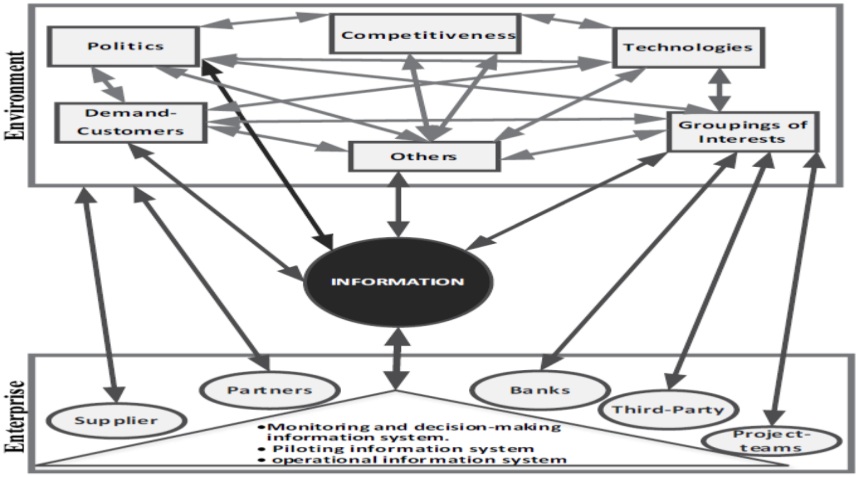

Figure 1: Modern Information System and I.T System

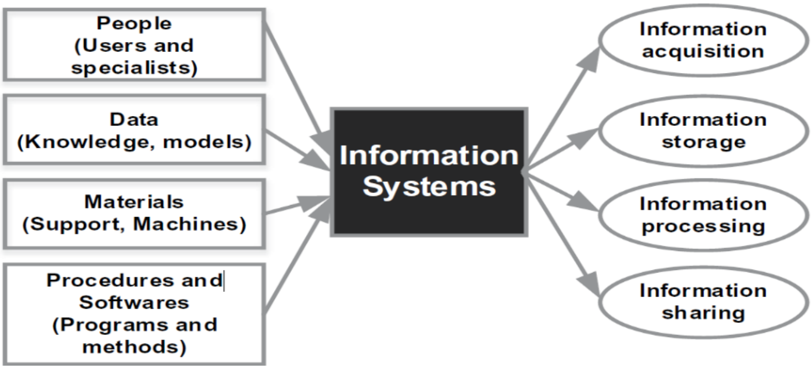

Figure 2: A systemic view of the company and the environment.

2. REVIEW OF LITERATURE

Malik et al., [1] discussed and proposed a comprehensive plan to combat Online Cyber frauds and suggested fraud prevention Strategies. Malik et al., [2] have studied and the details of online cyber-crimes, specially, to fight with white-collar crimes occurring in Governmental organizations as well as entrepreneurs and focused on the need for Strong Legislation and Ethics. Frauds in banks with the help of Electronic Devices and importance of "Business-Ethics" in the banking sector is important [3]. Anderson and Moore [5] has discussed in depth the online Cyber Crime and frauds and other matters related to Information Security have been presented with solutions. Rapid Action Battalion, discussed the matter about the financing of terrorism activities in the context of global perspective [6]. Enders and Sandler [7] has successfully deliberated on the effect of terrorism and its impact on the domestic economy of the affected country. The terrorist offences badly damage the financial markets and also the small business organizations. The groups behind terrorism financing need to be investigated and taken to task. Kshetri [8] and Vanini et al., [9] talk about the existence of online banking frauds, worldwide cybercrime Business, economic and planned standpoints. Table 1 presents a comprehensive overview of advanced techniques being researched and implemented to combat online fraud in the financial and banking sectors.

2.1. Important Modern Information Systems

Key trends include AI and Machine Learning (ML) integration in analytics, blockchain technology for secure transactions, increasing data governance focus on GDPR, and server-less computing for flexibility and scalability. The structure of Information Systems (IS) has evolved significantly due to advancements in cloud computing, AI, data analytics, and cybersecurity. The new Information Systems (IS) are a sophisticated, modular, and cloud-driven architecture designed for large-scale data processing, business operations enhancement, and cybersecurity protection. In Table 1 below, we list currently developed methods applicable to Information Systems.

Table 1: Advance techniques to combat financial and banking frauds

Methods	
Online Payment Frauds	Encryption
Machine Learning	Anomaly Detection
Machine Learning	"Support Vector Machines (SVM)"
"Supervised and Unsupervised Learning Models"	"Recurrent Neural Networks (RNNs)"
Block-chain Method	Method of Multilayer perceptron (MLP)
Biometric Verification	Method of Random Forest and Gradient Boosting
Anti-Money Laundering (AML)	Emerging Trends in the Cyberber Crimes
Real-Time Fraud	Cryptocurrency related offences

GDPR compliance	Data mining Technique

Modern IS architectures are more flexible, scalable, and integrated across various platforms and services. Key components include data analytics, security, and data analytics. Modern Information System's structures utilize IaaS, PaaS, and SaaS models for cost-effective, scalable infrastructure without heavy on-premise hardware, offering flexibility in data, applications, and virtualized environments.

Modern Information System structures also utilize IaaS, PaaS, and SaaS models for cost-effective, scalable infrastructure without heavy on-premise hardware, offering flexibility in data, applications, and virtualized environments. cost efficiency, scalability, and accessibility to cloud services, but also pose security and regulatory challenges. Storing data in the cloud offers cost efficiency, scalability, and accessibility, but also raises security risks and compliance challenges, particularly in sensitive industries [4].

Modern information systems prioritize distributed databases, storing data across physical or cloud environments, often using NoSQL and relational databases based on data complexity and requirements. The edge computing is gaining popularity for IoT applications, utilizing edge devices and cloud services. NoSQL databases like MongoDB and Cassandra are widely used for managing large-scale, unstructured data, offering flexibility, scalability, and efficient storage, particularly useful in big data applications.

Modern Information System structures prioritize security through advanced encryption, MFA, and zero-trust architectures, employing AI tools for breach detection and compliance with GDPR and privacy regulations. Big data analytics platforms like Apache Hadoop, Spark, and Kafka enable real-time and batch processing of diverse data sources, providing data visualization, predictive analytics, and business intelligence. The Hybrid and multi-cloud environments are being used by organizations for workload optimization, risk mitigation, and regulatory compliance, while collaboration and workflow systems like Microsoft Teams are integrated. Develops culture and pipelines are crucial for modern IS development, ensuring continuous system updates, testing, and deployment, with automation tools like Jenkins and Kubernetes playing critical roles.

3. ADVANCED METHODS TO COMBAT OFFENCES

Advanced technological and procedural strategies are being employed to combat online fraud and terrorist activities targeting banking and entrepreneurship. Financial institutions are utilizing (ML- Models) Machine Learning models for detection of doubtful and illegal transactions. preventing fraud by analyzing large datasets for unusual behaviors. Artificial Intelligence (AI) enhances Anti-Money Laundering and Counter-Financing of Terrorism efforts by monitoring transactions, identifying threats, and enforcing regulatory compliance. Fraud detection systems use customer behavior data, like online activity patterns, to identify anomalies and abnormalities, forming profiles of normal user behavior to detect fraudulent actions. The hybrid models combine supervised learning for known cases and unsupervised methods to detect new types of fraud, ensuring system adaptation to evolving cybercriminal tactics.

The Payment fraud involves fraudulent or unauthorized transactions by cybercriminals, resulting in the loss of funds, personal property, interest, or sensitive information via the internet [9].

Ali et al., [10] reviewed the financial frauds detection, based on the technique of machine learning. Machine Learning techniques like SVM and ANN are of pivotal importance particularly when frauds are committed with credit; card fraud being the most common type. Meghana et al., [11] is another paper which explained the method od of prediction of Financial Crime Using Machine Learning. Linear regression KNN algorithm, KNN algorithm and the K-nearest Neighbor (KNN) algorithm are the simple and early classification algorithms used for recommendation engines and image recognition. Supervised learning algorithms iteratively learn to predict target variables. Nasteski [12] provided an overview of the supervised machine learning methods.

“Threat Advice” offers industry-specific cybersecurity solutions and packages to protect organizations from fraud detection and ensure the future of fraud prevention. Hassan et al [13] has proposed a valuable method for Fraud Detection in IoT-Based Financial Transactions Using “Anomaly Detection Techniques”. Online banking security is compromised due to vulnerable authentication schemes, allowing intruders to masquerade as legitimate users for unauthorized access Kiyani et al., [14].

No doubt Machine Learning has revolutionized data processing, enabling real-time, intelligent systems, particularly in fraud detection. Financial institutions invest in improving algorithms and data analysis technologies for accuracy. Abakarim et al., [15] has proposed a workable model in real time for the protection of frauds occurring regarding credit cards and an effective and efficient method indeed.

Block chain technology enhances security by providing transparency and immutability, making it harder for malicious actors to hide their activities across decentralized networks. Nowadays, the financial institutions are increasingly utilizing Multi-Factor Authentication (MFA) methods like facial recognition and fingerprint scanning to safeguard online accounts from unauthorized access. The regulations such as GDPR (General Data Protection Regulation) directives enforce strict standards for customer data handling, reducing fraud risk in the financial sector. They provide insights into advanced technologies for combating online threats. Malik et al., [1] have discussed various aspects of frauds and fraudulent behavior.

GDPR in banking mandates banks to

obtain explicit consent for data processing and marketing activities, ensuring it is free, specific, informed, and unambiguous. Baker [16] presented on impact of the GDPR: General Data Protection Regulation in banking.

Tanaka et al., [17] in their paper have discussed the “Gordon-Loeb-Model”, a crucial economics-based approach for organizations to determine the appropriate investment in cybersecurity-related activities. They further elaborated for facilitating malicious attacks. He has proposed empirical analysis on the issue of e-local governess. Gordon-Loeb Model is a crucial economics-based approach for organizations to determine appropriate investment in cybersecurity-related activities.

The Internet of Things (IoT) connects physical and virtual objects, enabling communication, data exchange, and personalization, but also poses a security risk due to increasing device numbers.

Altulaihan et al., [18] has published a useful paper regarding cybersecurity threats and discussed in detail about the countermeasures with justification all the techniques on the IoT. Zhu [19] in his valuable research paper uses Support Vector Machines for unsupervised financial data classification, combining histograms with Light GBM to fuse data from multiple sources for accurate company financial assessment.

Almazroi and Ayub [20] has introduced an applicable technique termed as “ResNeXt-embedded Gated-Recurrent-Unit model” which efficiently addresses financial fraud in real-time and financial transaction processing, enhancing security and efficiency in the environment of wireless communications.

Mubarek and Adali [21] have discussed fraud detection in financial sectors, utilizing “machine- learning-algorithms” like Decision Trees and Naive Bayes to anticipate and quickly detect fraud. In the paper Kumar et al., [22] have highlighted and discussed the real-world credit-card fraud detection using Random Forest Algorithm (RFA), a “supervised-learning-algorithm” , which achieves 90% accuracy in detecting fraudulent transactions, both online and offline.

Banks are vulnerable to frauds, contributing to economic development. The study presented in Sood and Bhushan [23] explores bank fraud literature from 2000-2019, identifying major themes like regulatory and compliance-based studies and socio-psychological aspects. It is advised that future research should focus on customer vigilance and coping mechanisms. Teichmann and Falker [24] highlights the cryptocurrencies' role in financial crime, including money laundering and corruption, and proposes a more effective international regulation standard using Liechtenstein Blockchain as a benchmark. The research of Carneiro et al [25] discusses the development and deployment of a fraud detection system in an e-tail merchant, comparing “Machine Learning Methods” and manual classification, resulting in improved performance.

4. CONCLUSION

Banks and companies must establish a code of conduct, while adhering to the banking law, regulations, and international conventions. Trust companies and financial enterprises engage in illegal and unethical practices, such as money transfers, collection, exchanges, stock transfer services, and travel agents. There must be a strict check by the chief Executive. Commanding respect is very important due to reputation. Central banks manage money supply, influence monetary movement, and financial policy, becoming popular and trustworthy due to their reputation and measures. Incorrect trade-data is intentionally manipulated by businessmen to deceive and harm counterparts, causing damage to industry indices, business conditions, and investment opportunities There must be a strict check by the chief Executive. Spiritual, political, and social values influence business ethics, impacting economic values, investments, and productivity. Restlessness and irresponsible attitudes can negatively affect these values. Ethical maxims like prudence, benevolence, and equity are self-explanatory, applicable to human conduct, while aesthetic judgments, good faith, humanity, and social affection are also considered to be important for companies and banks.

Private banks, industrial, commercial, and holding companies frequently engage in unethical conduct, particularly in credit, savings, and securities business, often influenced by securities firms' new products and services.

Micro services break applications into independent services, offering flexibility, faster development, and resilience. Common protocols include REST and gRPC, essential for complex systems like e-commerce platforms.

The rise of IoT devices has boosted the need for edge computing, where data is processed for time-sensitive applications. reducing data transfer across networks, enabling efficient processing and storage of real-time data generated by IoT devices.

Modern information systems use robust cybersecurity measures, including Zero Trust Architecture, to protect sensitive data and maintain system integrity, requiring rigorous verification for access. Poor accounting methods, missing information, false declarations, goods in transit, and collaboration with auditors lead to significant errors in the banking business, resulting in fraud opportunities. Accountability is crucial for democratic order, requiring fair, non-favoritism processes and in the financial wrongdoings; which can be achieved by promoting business ethics and moral conduct. Businessmen often extract heavy loans from banks, often using hidden companies for bungling acts.

REFERENCES

[1]. A. A. Malik, W. Azeem and M. Asad, “Online shopping, Cyber frauds and Fraud Prevention Strategies’’, *International Journal for Electronic Crime Investigation*, vol. 8, no. pp. 49-56, 2024.

[2]. A. A. Malik, M. Asad and W. Azeem, “To Combat White Collar Crimes in Public and Private Sector and Need for Strong Legislation and Ethics”, *International Journal for Electronic Crimes Investigation*, vol. 4, no. 3, pp. 1-8, 2020.

[3]. A. A. Malik, M. Asad, W. Azeem, "Bank Frauds Using Digital Devices and the Role of Business Ethics", *International Journal for Electronic Crimes Investigation*" vol. 2, no. 4, 2018.

[4]. Y. Maleh, “I. T. Governance and Information Security”, *Tylor and Francis*, vol.6, no.5, pp. 34-42, 2022.

[5]. R. Anderson and T. Moore, "The Economics of Information Security." *Science and Engineering Ethics*, vol. 12, no. 4, pp. 609-632, 2006.

[6]. R.A. Battalion, "The Financing of Terrorism: A Global Perspective." *International Journal of Law and Management*, vol. 54, no. 4, pp. 246-258. 2012.

[7]. W. Enders and T. Sandler, "The Effect of Terrorism on the Domestic Economy: The Case of the United States," *Journal of Economic Perspectives*, vol. 10, no. 3, pp. 143-166, 1999.

[8]. N. Kshetri, "The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives," *Journal of Business Research*, vol. 63, no. 12, pp. 1255-1261, 2010.

[9]. P. Vanini, S. Rossi, E. Zvizdic and T. Domenig, “Online payment fraud: from anomaly detection to risk management”, *Financial Innovation*, vol. 9, no. 1, pp. 66-71, 2010.

[10]. A. Ali, S. A. Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser and A. Saif, “Financial fraud detection based on machine learning: a systematic literature review”, *Applied Sciences,* vol. 12, no. 19, pp. 37-48, 2022.

[11]. I. Meghana, B. P. Venkatesh, G. K. Ganesh, N. Sumant, and R. T. Teja, “Prediction of Financial Crime Using Machine Learning”, *International Journal of Innovative Research in Computer Science & Technology*, vol. 11, no. 3, pp. 96-100, 2023.

[12]. V. Nasteski, “An overview of the supervised machine learning methods”, *Horizons,* vol. 4, pp. 51-62, 2017.

[13]. M. Hassan, C. Veena, A. Singla, A. Joshi, and M. Lourens. “Fraud Detection in IoT-Based Financial Transactions Using Anomaly Detection Techniques”, *International Conference on Advances in Computing, Communication and Applied Informatics*, pp. 1-6, 2024.

[14]. A. T. Kiyani, A. Lasebae, K. Ali, and M. Ur-Rehman, “Secure online banking with biometrics”. *International Conference on Advances in the Emerging Computing Technologies*, pp. 1-6, 2020.

[15]. Y. Abakarim, M. Lahby, and A. Attioui, “An efficient real time model for credit card fraud detection based on deep learning”, *International conference on intelligent systems: theories and applications,* pp. 1-7, 2018.

[16]. L. Baker, “The impact of the General Data Protection Regulation on the banking sector: Data subjects’ rights, conflicts of laws and Brexit”, *Journal of Data Protection*

and Privacy, vol. 1, no. 2, pp. 137-145, 2017.

[17]. H. Tanaka, K. Matsuura and O. Sudoh, “Vulnerability and information security investment: An empirical analysis of e-local government in Japan”, *Journal of Accounting and Public Policy*, vol. 24, no. 1, pp. 37-59, 2005.

[18]. E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, “Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions,” *Electronics*, vol. 11, no. 20, pp. 33-40, 2022.

[19]. V. Zhu, “Research on Intelligent Financial Statement Analysis and Anomaly Identification Techniques by Fusing Multi-source Data”. *Journal of Electrical Systems*, vol. 20, no. 10, pp. 927-941, 2024.

[20]. A. A. Almazroi and N. Ayub, “Online Payment Fraud Detection Model Using Machine Learning Techniques”, *IEEE Access*, vol. 11, 188-203, 2023.

[21]. A. M. Mubarek and E. Adalı, "Multilayer perceptron neural network technique for fraud detection," *International Conference on Computer Science and Engineering*, pp. 383-387, 2017.

[22]. M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika and E. Aswini. “Credit card fraud detection using random forest algorithm”, *International Conference on Computing and Communications Technologies*, pp. 149-153, 2019.

[23]. P. Sood and P. Bhushan, “A structured review and theme analysis of financial frauds in the banking industry”. *Asian Journal of Business Ethics*, vol. 9, pp. 305-321, 2020.

[24]. F. M. J. Teichmann and M. C. Falker, “Cryptocurrencies and financial crime: solutions from Liechtenstein”, *Journal of Money Laundering Control*, vol. 24, no. 4, pp. 775-788. 2021.

[25]. N. Carneiro, G. Figueira and M. Costa, “A data mining based system for credit-card fraud detection in e-tail”, *Decision Support Systems*, vol 95, pp. 91-101, 2017.