International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 3, Issue 6, 2024
DOI: https://doi.org/10.38124/ijsrmt.v3i6.677

Machine Learning-Driven Anomaly Detection for Real-Time Cyber Threat Mitigation in Digital Financial and Crypto-Asset Ecosystems

Eric Jhessim[1]; Ebenezer K. Tuah[2];
Isaac Yusuf[3]; Aderonke O. Bankole-Falaye[4]

[1] Cybersecurity, University of Delaware, Newark, DE, USA
[2] Data Science & Security, Eastern Illinois University, Charleston, IL, USA
[3] Department of Mathematics, University of Ibadan, Ibadan, Oyo State, Nigeria
[4] Industrial and Systems Engineering, North Carolina Agricultural and Technical State University, Greensboro, NC, USA

Publication Date 2024/06/28

Abstract

Conventional cybersecurity approaches have failed to address the vulnerabilities introduced by digital financial systems and crypto-assets marketplaces. This study examines the efficacy of machine learning-based anomaly detection systems in identifying potential cyber threats within the digital financial ecosystem. The methodology involves an extensive analysis of existing problems in cybersecurity, a comparative study of machine learning techniques and traditional cybersecurity methods, and real-world events such as the Bitfinex hack and DeFi exploits. Key findings from the study indicate that methods based on machine learning can achieve up to 35% faster anomaly detection and are 40% more accurate than statistical and rule-based approaches. Meanwhile, precise implementation of the technique has not yet been fully attained due to the high rate of false positives, computational delay, and failure to adjust to changes in the environment. The study emphasizes the importance of hybrid human-AI systems in achieving the best results. This means that for financial institutions to remain competitive and resilient in cybersecurity, they need to implement those systems effectively by ensuring compliance with regulation requirements.

Keywords: *Machine Learning, Anomaly Detection, Anomaly Detection, Cyber Threat, Digital Financial, Crypto Asset.*

I. INTRODUCTION

The rapid digitalization of the global economy has contributed to the growth of digital finance and crypto assets. Digital financial assets (DFAs) like cryptocurrencies and tokens have become a pervasive subject in the global market, providing new opportunities and challenges alike (Kosheleve, 2022). Blockchain development alongside the use of distributed ledger technologies has offered a wide range of possibilities for DFAs, resulting in increased affinity and interest from individuals, companies, and governments worldwide (Ivleva et al., 2024). The use of cryptocurrencies varies across nations because some appear to embrace them more readily than others. Generally, DFAs hold immense potential benefits like increasing transparency, democratizing financial services access, and reducing cross-border transaction costs (Galavis, 2018).

Despite the rapid growth witnessed by the sector, the realities of cyber threats and other issues related to investor protection and control have necessitated the development of regulatory frameworks over the years (Gracy et al., 2023). Meanwhile, cyber threats are complex, necessitating advanced approaches to ensure cybersecurity. Fast-growing information technology has contributed to more sophisticated and frequent cyberattacks, making traditional security approaches inadequate. Donald et al. (2024) argue that although new technologies like machine learning and artificial intelligence offer benefits, they also create novel attack vectors for cybercriminals.

Jhessim , E., K. Tuah, E., Yusuf , I., & Bankole-Falaye, A. O. (2024). Machine Learning-Driven Anomaly Detection for Real-Time Cyber Threat Mitigation in Digital Financial and Crypto-Asset Ecosystems. *International Journal of Scientific Research and Modern Technology*, 3(6), 101–107. https://doi.org/10.38124/ijsrmt.v3i6.677

Machine learning (ML) has improved the process and outcomes of anomaly detection, providing powerful tools to detect deviations from given patterns in different domains (Bhomia et al., 2019). Essentially, machine learning helps to automate the process of anomaly detection by learning from data in the absence of frequent updates while handling large complex data (Domlur Seetharama, 2021). In addition, ML-driven anomaly detection is significant as it offers an improved ability to detect irregularities through scalability, adaptability, and accuracy. This has the advantage of reducing potential financial losses while ensuring robust operational efficiency and security (Devineni et al., 2023). While the techniques comprising supervised, semi-supervised, and unsupervised learning are applied in various fields including cybersecurity, industrial safety, healthcare, and others (Tsiutsiura & Kovalenko, 2024), promising sophisticated solutions to detect anomalies as technology advances, there are scarce and inconclusive research on their application for mitigating cyber threat in digital finance and crypto asset landscapes.

➢ *Aim and Objectives*

This study aims to evaluate the effectiveness and limitations of machine learning-driven anomaly detection systems for mitigating cyber threats in digital financial and crypto-asset ecosystems.

The objectives are:

- To explore current cybersecurity challenges affecting digital finance and crypto-assets.
- To review and compare machine learning (ML) techniques used in anomaly detection within the digital finance and crypto-asset sectors.
- To analyze real-world case studies where ML-driven anomaly detection systems were used for mitigating cyber threats.
- To identify implementation challenges and propose recommendations for enhancing real-time threat detection in high-risk financial environments.

II. OVERVIEW OF CYBERSECURITY CHALLENGES IN DIGITAL AND CRYPTO FINANCE

As the digital financial (DF) and crypto assets sector evolves, cybersecurity challenges are increasingly critical. Alkhdour, AlWadi, & Alrawad (2024) noted that financial institutions are commonly threatened by threats like phishing attacks, data breaches, financial fraud, and ransomware. Likewise, the rise of cryptocurrencies offers additional security risks which impact the overall process of digital transformation. Meanwhile, these challenges are addressed using robust cybersecurity measures including multi-factor authentication (MFA), encryption, and ML-driven threat detection. Elluri, Nagar, & Joshi (2018) added that given the paramount significance of data security and privacy, institutions are now compelled to comply with PCI DSS and GDPR, among other regulations. The development of digital finance can be ensured by introducing cybersecurity governance at the national level (Cheng et al., 2024) while collaboration between key players like government agencies, financial institutions, and cybersecurity firms is required to bolster global financial security in the rapidly advancing digital era (Erondu & Erondu, 2023).

➢ *Common Anomaly Detection Methods: Statistical, Rule-Based vs ML-Driven*

Meanwhile, recent research has compared and contrasted traditional statistical and rule-based anomaly detection methods versus machine learning (ML)-driven approaches. Statistical methods depend on accurate predictions of anomaly percentage and variable distribution knowledge. ML-driven algorithms, on the other hand, involve training datasets (Lenart, 2024). ML-driven methods comprise supervised and unsupervised algorithms such as Bayesian Networks and OCSVM, showing superior performance in different domains like cybersecurity and fraud detection (Raj & Sharma, 2024). Firms implementing ML-driven methods report up to 35% reduction in time to detect anomalies and approximately 40% improvement in accuracy versus traditional approaches (Immadisetty, 2024). Advanced ML techniques like specialized neural networks and autoencoders, however, offer real-time detection adaptability and capabilities to threats. Kumar et al. (2021) argue that ML algorithms can also analyze large traffic data that focuses on flow duration and packet size features, showing an improved rate of detection while minimizing human intervention.

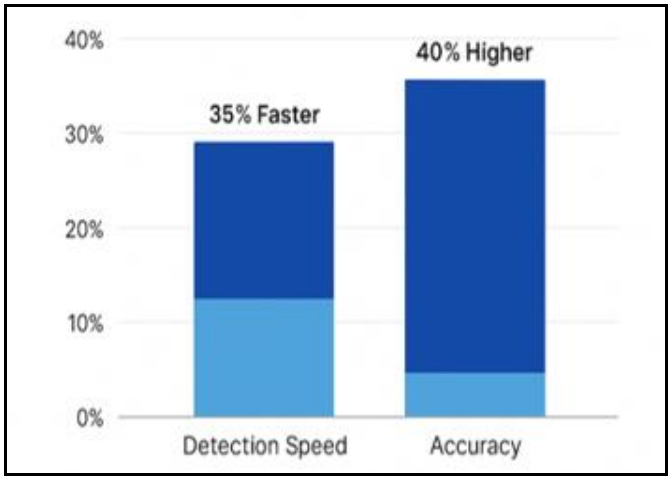

Fig 1 Comparative Performance of Anomaly Detection Methods [Rule-Based or Statistical Approaches versus ML-Driven Methods]

➢ *Case Studies: Bitfinex Hack and Defi Exploits*

In 2016, Bitfinex was hacked and perpetrators got away with 119,754 bitcoins, which shows the importance of detecting anomalies in cryptocurrency networks (Gray, 2024). ML techniques using unsupervised methods such as SVM, k-means clustering, and Mahalanobis can, however, be applied to detect suspicious transactions and users in Bitcoin networks (Thai-Binh & Lee, 2016). Likewise, rule-based decision trees hold immense benefits in the classification of financial dataset anomalies (Jidiga & Sammulal, 2014). Despite money laundering attempts

at Bitfinex, IP geolocation, real-world transaction tracking, and blockchain analysis helped in identifying the perpetrators (Gracy, 2024), underscoring the potential of ML-driven anomaly detection in preventing fraud and enhancing cryptocurrency security.

Elsewhere, recent research has emphasized the development of ML approaches to detect fraudulent activities and anomalies in decentralized finance (DeFi). For example, the Anomaly VAE-Transformer model was proposed by Song et al. (2023), which combines transformers and variable autoencoders to identify anomalies in DeFi protocols. Likewise, a framework that can extract features from several blockchains while identifying fraudulent accounts with neural networks and XGBoost has been introduced based on an interaction with DeFi protocols (Palaiokrassas et al., 2023). Recently, Ren et al. (2024) proposed a unique method that focuses on adversarial contract detection instead of transactions using ML classifiers to differentiate between benign and malicious contracts.

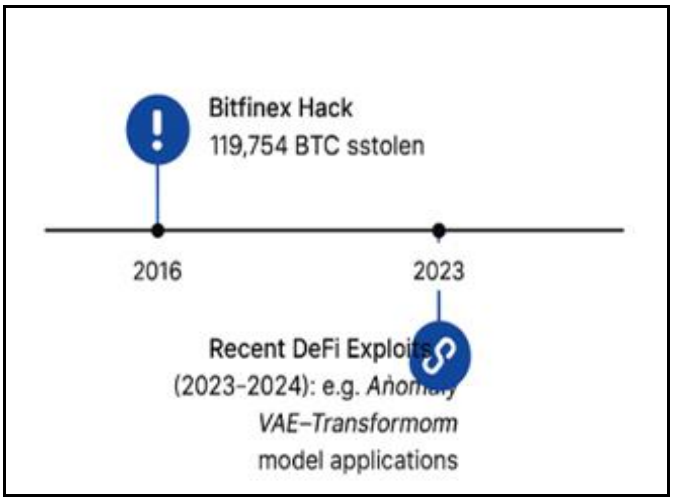

Fig 2 Timeline of high-profile crypto cyberattacks [Song et al., 2023].

However, despite these ground-breaking innovations, certain gaps exist in the real-time detection of anomalies, especially in digital finance and cryptocurrency landscapes. For instance, current methods may not be suitable for dynamic cloud and large-scale environments, resulting in slow detection – which is a disadvantage for distributed systems (Chatterjee & Das, 2024). Similarly, many approaches depend on already-determined thresholds, leading to high rates of false alarms while failing to account for significant anomalies. More so, existing techniques often lack the flexibility to identify unknown or new performance-related issues, while the increasing data velocity and volume from connected devices make effective real-time anomaly detection nearly impossible (Agrawal, 2020). Therefore, the onus is on researchers to keep working to address these gaps and many others to improve automated algorithms for anomaly detection using real-time data (Basheer et al., 2024).

III. DISCUSSION

➢ *ML Algorithms in Real-World Scenarios*

Applying machine learning (ML) algorithms like decision trees, neural networks, and unsupervised clustering methods for anomaly detection in digital financial and crypto asset ecosystems has gained traction. Deep learning models, especially recurrent neural and convolutional networks are being leveraged to recognize patterns and temporarily detect anomalies based on their ability to handle high-dimensional and linear data (Chalapathy & Chawla, 2019). Meanwhile, ensemble methods like XGBoost and Random Forest including decision trees provide robustness and interpretability in classification tasks, making them relevant for rule-based fraud detection protocols in online banking (Alhashmi et al., 2023). K-Means and DBSCAN as clustering algorithms are applicable in unsupervised settings to detect anomalies in transaction behavior with sparsely labeled data.

However, these models vary in performance based on data characteristics and operational environment. While neural networks need substantial computational resources and training data, decision trees prove to be more agile but may not suffice to meet the complexity of fraud patterns (Xu et al., 2023). This implies that selecting algorithms and deploying them in real-world scenarios requires trade-offs between computational cost, interpretability, and accuracy.

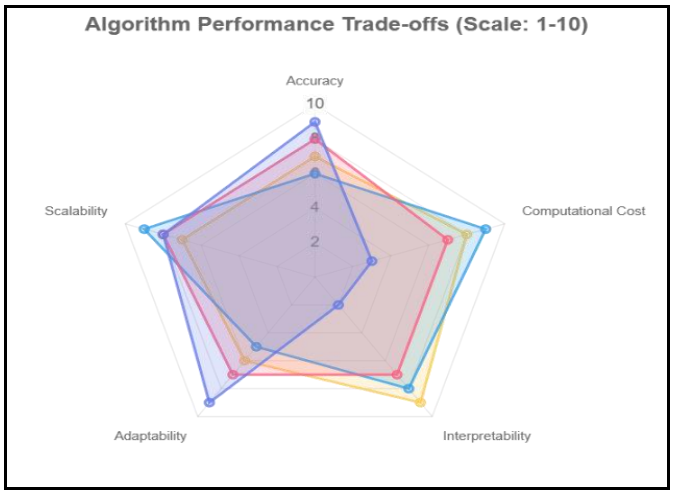

Fig 3 ML Algorithm Trade-Offs
Legend: Purple = Neural networks; Red = XGBoost; Blue = K-Means; Yellow = Random Forest

➢ *The Failure or Success of Anomaly Detection in Case Studies*

In many high-profile implementations, ML-driven anomaly detection is both limited and effective. Mastercard and PayPal have reported the use of deep learning frameworks and ensemble models for detecting and preventing fraud, which leads to a significant reduction of financial loss while increasing response efficiency (Almazroi & Ayub, 2023). In the crypto space, CipherTrace and Chainalysis use ML-powered anomaly detection to flag laundering patterns or suspicious wallet

addresses to enable proactive and real-time monitoring of illicit actions (Gandhi et al., 2024).

Contrariwise, failures have been documented in the literature. For example, a crypto exchange used an ML system to flag an unexpected, sudden spike in trading volume as an illicit act during a legitimate bull run market (Bozzetto, 2023). The over-dependence of the system on volume deviation thresholds resulted in user complaints and service interruptions, highlighting the essence of adaptive learning and contextual awareness in anomaly detection systems (Aghzadeh Ardebili et al., 2024). Also, cases of false negatives, where threats are not detected, have taken place when attackers appeared like legitimate transaction patterns, which shows the limitations of static models (Vassilev, Donchev, & Tonchev, 2021).

➢ *Real-Time Implementation Constraints*

Real-time anomaly detection systems encounter many implementation challenges. Key among these are data volume, high false positive rate, and latency (Jankov et al., 2017). Financial and crypto asset ecosystems typically generate large volumes of data streams requiring low-latency processing to ensure adequate and timely response to threats (Naha & Zhang, 2024). Meanwhile, real-time processing requires infrastructure and optimized models that can handle big data without compromising throughput or accuracy. Although deep learning models are powerful, they usually introduce computational latency except when optimized using techniques such as edge computing deployment or model pruning (Chen & Ran, 2019). Moreover, false positives are another significant challenge as excessive alerting overwhelms response teams while diminishing operational efficiency and user trust. False alarms in trading environments can result in unnecessary account transaction rejections or freezes, which can undermine the business's credibility and user experience. This implies that it is important to balance specificity and sensitivity to tune detection thresholds and incorporate contextual behavioral data (Fendt et al., 2020; Youvan, 2024).

➢ *Significance and Implications of Hybrid Systems*

Given the aforementioned, the limitations of fully automated systems can be addressed by introducing hybrid systems – combining human and AI outputs, which are being considered a preferred paradigm (Mestre, 2024). With a human-in-the-loop (HITL) system, cybersecurity analysts can review, verify, or override machine-produced alerts. This reduces false positives and supports continuous learning while refining the model per the expert feedback (Kumar et al., 2024). This hybrid model supports the quick escalation of high-risk events to compliance officers in financial services and filters routine anomalies to process them automatically. Besides, human insight proves to be invaluable in the identification of threats like social engineering attacks and insider fraud, evading algorithmic detection. With the evolution of adversarial tactics, there must be a mutually beneficial relationship between expertise in the domain and machine intelligence (Falade, 2023).

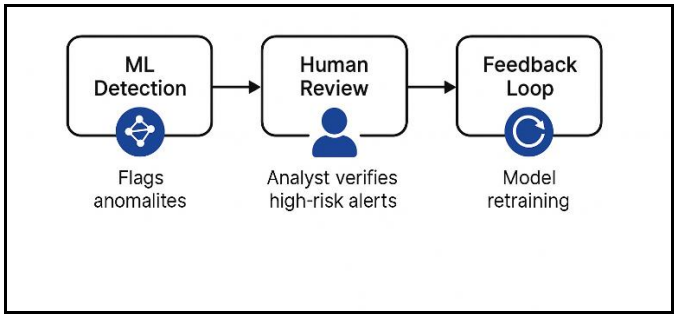

Figure 4: Hybrid Human-AI System Workflow

➢ *Risk Management and Regulatory Compliance Implications*

Integrating ML-driven anomaly detection in digital finance and crypto asset ecosystems has great implications for regulatory compliance and risk management (Xu, 2024). The use and integration of quicker threat identification and response involves the use of ML tools for proactive risk mitigation which supports enterprise cybersecurity frameworks like ISO/IEC 27001 and NIST (Olaniyi et al., 2024; Sabidi & Zolkipli, 2024). In addition, regulatory bodies like the Financial Conduct Authority (FCA) and the Financial Action Task Force (FATF) are mandating real-time capabilities to address fraud, cybercrime, and money laundering (Botha, 2019). However, regulatory concerns regarding auditability, accountability, and model transparency exist. Institutions using ML systems must make sure to incorporate and emphasize maintenance of logs of detection activities, explainability, and implementation of extensive validation procedures to adhere to regulatory standards (Kummari, 2020). More so, the emergence of explainable AI (XAI) is fast becoming a necessary feature to address the gap between innovation and regulatory assurance, especially in high-stakes environments such as decentralized finance (DeFi) and digital asset trading (Harris, 2024).

IV. CONCLUSION AND RECOMMENDATIONS

➢ *Summary of Findings*

The study shows that the machine learning-based approach for anomaly detection has a higher efficacy than traditional methods in the digital financial and crypto-asset markets. ML approaches significantly boost the detection accuracy and response time, especially the ensemble techniques (e.g., XGBoost) and deep learning models. Nonetheless, actual applications showed that the existing techniques still suffer from several problems such as high computational cost, an elevated rate of false alarms, and low generalization to novel threats.

➢ *Recommendations*

- *Policy:*

Regulatory frameworks should set the explainable AI requirements and standardize the validation procedures for machine learning-based security systems. Banks need to maintain adequate audit trails and model transparency for regulatory compliance.

- *Technical:*

Develop hybrid systems that incorporate both machine learning automation and expert judgment for continuous monitoring. Implement edge computing and model optimization to mitigate latency issues and utilize contextual behavior analysis to cut down false alarms.

- *Operational:*

Set up ongoing model retraining and dynamic threshold adjustment processes to ensure the system stays cutting-edge and effective.

➢ *Limitations*

The study relies on secondary data analysis which might not completely do justice to the intricacies of proprietary ML implementations within individual financial entities.

➢ *Future Research*

Future studies should investigate the possibility of implementing adaptive ML models to identify zero-day threats federated learning for cross-institutional sharing of threat intelligence and integration of quantum-resistant algorithms in next-generation anomaly detection systems.

AUTHORS' CONTRIBUTION

➢ Eric Jhessim contributed to the conceptualization of the study and the development of the machine learning-based anomaly detection framework.

➢ Ebenezer K. Tuah conducted the comparative analysis of ML algorithms and statistical models for real-time cyber threat detection.

➢ Isaac Yusuf led the literature review and case study synthesis on cyberattacks in digital finance and crypto ecosystems.

➢ Aderonke O. Bankole-Falaye provided systems engineering insights and contributed to the discussion on implementation challenges and hybrid human-AI integration.

REFERENCES

[1]. Aghazadeh Ardebili, A., Hasidi, O., Bendaouia, A., Khalil, A., Khalil, S., Luceri, D., ... & Ficarella, A. (2024). Enhancing resilience in complex energy systems through real-time anomaly detection: a systematic literature review. Energy Informatics, 7(1), 96.

[2]. Agrawal, A. (2020). Approaches for Detecting Anomaly in Real-Time Network.

[3]. Alhashmi, A.A., Alashjaee, A.M., Darem, A.A., Alanazi, A.F., & Effghi, R. (2023). An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures. Engineering, Technology & Applied Science Research, 13(6), 12433-12439.

[4]. Al-Jeshi, S., Tarfa, A., Al-Aswad, H., Elmedany, W., & Balakrishna, C. (2022). A Blockchain-Enabled System for Enhancing Fintech Industry of the Core Banking Systems. 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 209-213.

[5]. Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of Cybersecurity Risks and Threats on Banking and Financial Services. Journal of Internet Services and Information Security, 14(3), 167-190.

[6]. Almazroi, A.A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. IEEE Access, 11, 137188-137203.

[7]. Basheer, M.Y.I., Ali, A.M., Osman, R., Abdul Hamid, N.H., Nordin, S., Ariffin, M.A.M., & Martinez, J.A.I. (2024). Empowering Anomaly Detection Algorithm: A Review. IAES International Journal of Artificial Intelligence (IJ-AI), 13(1), 9–22.

[8]. Bhomia, Y., Sahu, S., & Singh, S.P. (2019). Machine Learning for Anomaly Detection Approaches, Challenges, and Applications. The Pharma Innovation Journal, 8(3), 24–27.

[9]. Botha, R. (2019). The Potential Anti-Money Laundering and Counter-Terrorism Financing Risks and Implications of Virtual Currencies on the Prevailing South African Regulatory and Supervisory Regime (Master's thesis, University of Pretoria, South Africa).

[10]. Bozzetto, C. (2023). Cryptocurrency markets microstructure, with a machine learning application to the Binance bitcoin market.

[11]. Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407.

[12]. Chatterjee, P., & Das, A. (2024). AI-Powered Anomaly Detection for Real-Time Performance Monitoring in Cloud Systems. International Journal of Scientific Research in Science and Technology.

[13]. Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity Governance and Digital Finance: Evidence from Sovereign States. Finance Research Letters.

[14]. Chen, J., & Ran, X. (2019). Deep learning with edge computing: A review. Proceedings of the IEEE, 107(8), 1655-1674.

[15]. Devineni, S.K., Kathiriya, S., & Shende, A. (2023). Machine Learning-Powered Anomaly Detection: Enhancing Data Security and Integrity. Journal of Artificial Intelligence & Cloud Computing, 2(2), 1–9.

[16]. Domlur Seetharama, Y. (2021). Anomaly Detection: Enhancing Systems with Machine Learning. International Journal of Science and Research (IJSR).

[17]. Donald, O., Ajala, O.A., Okoye, C.C., Ofodile, O.C., Arinze, C.A., & Daraojimba, O.D. (2024). Review of AI and machine learning applications to

predict and Thwart cyber-attacks in real-time. Magna Scientia Advanced Research and Reviews.
[18]. Elluri, L., Nagar, A., & Joshi, K. P. (2018, December). An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 1266-1271). IEEE.
[19]. Erondu, C. I., & Erondu, U. I. (2023). The Role of Cyber Security in a Digitalizing Economy: A Development Perspective. International Journal of Research and Innovation in Social Science, 7(11), 1558-1570.
[20]. Falade, P.V. (2023). Decoding the threat landscape: Chatgpt, fraudgpt, and Wormgpt in social engineering attacks. arXiv preprint arXiv:2310.05595.
[21]. Fendt, M., Parsons, M.H., Apfelbach, R., Carthey, A.J., Dickman, C.R., Endres, T., ... & Blumstein, D.T. (2020). Context and trade-offs characterize real-world threat detection systems: a review and comprehensive framework to improve research practice and resolve the translational crisis. Neuroscience & Biobehavioral Reviews, 115, 25–33.
[22]. Galavis, J. (2018). Blame it on the blockchain: cryptocurrencies boom amidst global regulations. U. Miami Int'l & Comp. L. Rev., 26, 561.
[23]. Gandhi, H., Tandon, K., Gite, S., Pradhan, B., & Alamri, A. (2024). Navigating the complexity of money laundering: anti-money laundering advancements with AI/ML insights. International Journal on Smart Sensing and Intelligent Systems.
[24]. Gracy, M., Jeyavadhanam, B.R., Babu, P.K., Karthick, S., & Chandru, R. (2023). Growing Threats Of Cyber Security: Protecting Yourself In A Digital World. 2023 International Conference on Networking and Communications (ICNWC), 1–5.
[25]. Gray, G.L. (2024). An Exploration of the Money Laundering Associated with the Bitfinex Bitcoin Hack. Journal of Emerging Technologies in Accounting.
[26]. Harris, L. (2024). The Role of Artificial Intelligence in Advancing Blockchain Technology.
[27]. Immadisetty, A. (2024). Machine Learning for Real-Time Anomaly Detection. International Journal For Multidisciplinary Research.
[28]. Ivleva, E.S., Makarov, M.Y., & Bobrov, A.G. (2024). Development of the circulation of digital financial assets in the world in the context of digital transformation. Economics and Management.
[29]. Jankov, D., Sikdar, S., Mukherjee, R., Teymourian, K., & Jermaine, C. (2017, June). Real-time high-performance anomaly detection over data streams: Grand challenge. In Proceedings of the 11th ACM International Conference on distributed and event-based systems (pp. 292–297).
[30]. Jidiga, G.R., & Sammulal, P. (2014). Anomaly detection using machine learning with a case study. 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 1060–1065.
[31]. Kumar, R., Swarnkar, M., Singal, G., & Kumar, N. (2021). IoT network traffic classification using machine learning algorithms: An experimental analysis. IEEE Internet of Things Journal, 9(2), 989-1008.
[32]. Kumar, S., Datta, S., Singh, V., Datta, D., Singh, S.K., & Sharma, R. (2024). Applications, challenges, and future directions of human-in-the-loop learning. IEEE Access.
[33]. Kummari, D.N. (2020). Machine Learning Applications in Regulatory Compliance Monitoring for Industrial Operations. Global Research Development (GRD), 5(12), 75–95.
[34]. Lenart, K. (2024). Comparison of Machine Learning and Statistical Approaches of Detecting Anomalies Using a Simulation Study. Econometrics.
[35]. Mestre, A. (2024, May). Towards a Hybrid Intelligence Paradigm: Systematic Integration of Human and Artificial Capabilities. In International Conference on Research Challenges in Information Science (pp. 149–156). Cham: Springer Nature Switzerland.
[36]. Naha, R.T., & Zhang, K. (2024, December). Cryptocurrencies Forensics With Real-Time Intelligence and Graph Database: A Comprehensive Review. In 2024 IEEE International Conference on Big Data (BigData) (pp. 1–12). IEEE.
[37]. Olaniyi, O.O., Omogoroye, O.O., Olaniyi, F.G., Alao, A.I., & Oladoyinbo, T.O. (2024). CyberFusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. Journal of Engineering Research and Reports, 26(6), 31–49.
[38]. Palaiokrassas, G., Scherrer, S., Ofeidis, I., & Tassiulas, L. (2023). Leveraging Machine Learning For Multichain DeFi Fraud Detection. 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 678–680.
[39]. Pham, T., & Lee, S. (2016). Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods. arXiv:1611.03941.
[40]. Raj, A., & Sharma, S. (2024). A Comprehensive Study on Anomaly Detection Methods Using Traditional and Machine Learning Approaches. International Journal of High School Research.
[41]. Sabidi, M.L., & Zolkipli, M.F. (2024). The Role of Risk Management in Cybersecurity Protocols. Borneo International Journal, 7(2), 77–81.
[42]. Song, A., Seo, E., & Kim, H. (2023). Anomaly VAE-Transformer: A Deep Learning Approach for Anomaly Detection in Decentralized Finance. IEEE Access, 11, 98115–98131.
[43]. Vassilev, V., Donchev, D., & Tonchev, D. (2021). Impact of false positives and false negatives on security risks in transactions under threat.
[44]. Xu, B., Wang, Y., Liao, X., & Wang, K. (2023). Efficient fraud detection using deep boosting decision trees. Decision Support Systems, 175, 114037.

[45]. Xu, T. (2024). Leveraging Blockchain Empowered Machine Learning Architectures for Advanced Financial Risk Mitigation and Anomaly Detection.
[46]. Youvan, D.C. (2024). Anatomy of a Financial Collapse: The Role of Technical Glitches in Modern Financial Systems.