The synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms

Abstract :

This study examines the role of artificial intelligence-driven security models in mitigating cybersecurity threats in cryptocurrency platforms, focusing on fraud detection, smart contract vulnerabilities, and regulatory implications. Using publicly available datasets, including the Elliptic Bitcoin Dataset, SolidiFI-Benchmark, CryptoScamDB, and CipherTrace AML Reports, the study applies anomaly detection, supervised machine learning (Logistic Regression), comparative performance analysis (Random Forest), and regression analysis (OLS) to evaluate fraud trends, AI-driven threat detection, and the impact of AI adoption on financial crime rates. The findings reveal that while AI-based models reduce false positives in fraud detection, they exhibit high false negative rates, with the AI-driven model achieving an ROC-AUC score of 0.512 compared to 0.500 in traditional rule-based methods. Regression analysis indicates a strong inverse correlation ($R^2 = 0.927$) between AI adoption and fraud cases, with each 1% increase in AI usage reducing fraud by approximately 37 cases. The study recommends integrating reinforcement learning to enhance AI adaptability, implementing standardized AI compliance frameworks, leveraging quantum-resistant AI security, and adopting federated learning for decentralized fraud detection.

Keywords: Cryptocurrency security, Machine learning, Fraud detection, Smart contracts, AI-driven cybersecurity.

1. INTRODUCTION

The rapid expansion of cryptocurrency platforms has created both financial opportunities and significant cybersecurity challenges. As decentralized finance (DeFi) and blockchain-based transactions gain adoption, cybercriminals exploit vulnerabilities, leading to increasing fraud, phishing attacks, deepfake scams, and smart contract exploits. Sarker et al. (2024) posits that traditional cybersecurity frameworks, which rely on rule-based methodologies, lack the adaptability and real-time responsiveness needed to counter these threats. Consequently, artificial intelligence (AI), particularly Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL), has

emerged as a key tool in strengthening cybersecurity. These AI-driven approaches enhance fraud detection, identify anomalies, and develop security mechanisms that evolve alongside emerging cyber threats (Ozkan-Ozay et al., 2024).

The decentralized nature of cryptocurrency platforms, combined with pseudonymity and regulatory gaps, presents unique security challenges. Cybercriminals employ sophisticated tactics, including AI-powered phishing attacks that closely mimic legitimate financial institutions. According to Javed et al. (2024), AI-generated phishing emails now account for a significant share of cyberattacks, surpassing traditional methods in effectiveness. Additionally, financial crimes in the cryptocurrency space have escalated, with global losses exceeding $5.6 billion in 2023, this shows that cryptocurrency-related fraud constituted nearly half of all financial fraud cases in 2023 (Lang, 2024). A growing concern is the proliferation of AI-generated deepfake scams, projected to account for 70 percent of cryptocurrency crimes by 2026 (McKenna, 2024). These fraudulent schemes exploit AI's ability to generate realistic synthetic media, deceiving investors and financial institutions.

Smart contract vulnerabilities further intensify security risks. DeFi platforms, which rely on automated smart contracts for financial transactions, are particularly susceptible to cyberattacks due to programming flaws. Khan et al. (2021) argues that exploits targeting these contracts have resulted in substantial financial losses, highlighting the need for AI-driven security solutions. According to Bresil et al. (2025) ML algorithms are adopted to analyze smart contract code, allowing for early detection of vulnerabilities before exploitation occurs. AI models trained on historical exploit data effectively identify patterns of potential weaknesses, adding an extra layer of security to blockchain transactions.

As cyber threats evolve, regulatory scrutiny has increased. In the view of Yadav (2022), governments and financial authorities are tightening oversight of cryptocurrency security practices, with agencies such as the United States Securities and Exchange Commission (SEC) prioritizing AI-driven cybersecurity solutions (Noguer&Chatzianastasiou, 2024). Compliance with evolving regulations has driven cryptocurrency platforms to adopt AI-powered fraud detection, Know Your Customer (KYC) verification, and automated transaction monitoring systems (Rane et al., 2023). However, regulatory challenges persist, particularly concerning user privacy and ethical concerns related to AI-driven surveillance. Striking a balance between security and privacy remains a central issue as policymakers attempt to regulate AI's role in financial security.

AI-driven cybersecurity mechanisms offer significant advantages over traditional security models. Ashfaq et al. (2022) contends that ML models have proven effective in

detecting fraudulent transactions by analyzing user behavior, transaction patterns, and blockchain data. A systematic analysis of AI applications in blockchain security found that nearly half of all research focuses on anomaly detection, emphasizing its critical role in securing digital assets (Fadi et al., 2022; Cholevas et al., 2024). Beyond fraud detection, ML algorithms support price prediction, address classification, and performance monitoring, further reinforcing security measures for cryptocurrency investors and traders.

Deep Learning has played a transformative role in fraud prevention by identifying intricate cyber threat patterns. Research by Nicholls et al. (2021) demonstrates that DL models such as Convolutional Neural Networks (CNNs), Artificial Neural Networks (ANNs), and Autoencoders have been effectively used to detect fraudulent cryptocurrency transactions. These models successfully identify money laundering schemes, double-spending attempts, and AI-powered phishing attacks (Stutz et al., 2024). Additionally, DL enhances phishing detection by analyzing linguistic patterns in emails, websites, and social media messages. Studies highlight the growing importance of DL in malware detection, intrusion prevention, and smart contract analysis, reinforcing its role in digital asset protection (Qureshi et al., 2024; Nicholls et al. 2021; Stutz et al., 2024).

Reinforcement Learning has emerged as a powerful tool for developing adaptive security systems capable of dynamically responding to cyber threats. Goel et al. (2024) posits that unlike traditional security measures, which rely on static rule sets, RL models continuously learn optimal defense strategies through simulated attack environments. A study on AI-driven cybersecurity found that the Actor–Critic RL algorithm achieved a high success rate in cyber-attack defense simulations, outperforming traditional threat mitigation strategies (Oh et al., 2024). RL is also being explored in self-healing network security, where AI models autonomously detect and counteract threats in real time. This capability is particularly relevant for cryptocurrency platforms, where security breaches require immediate response mechanisms.

Despite advancements in AI-driven security, cybercriminals increasingly exploit AI to develop sophisticated attack techniques. Wendt (2024) argues that threat actors leverage AI to enhance ransomware, adversarial AI attacks, and deepfake fraud. Bates (2025) indicate that nearly half of security professionals anticipate AI-driven ransomware to dominate future cyber threats, while over 60 percent of organizations have reported a sharp rise in deepfake-based cyberattacks. These developments highlight the urgency of ongoing research into adversarial AI defenses to ensure security mechanisms remain resilient against evolving threats.

Several emerging trends are expected to shape the future of AI-driven cybersecurity in cryptocurrency platforms. Quantum-resistant AI security solutions are under development to mitigate the potential risks posed by quantum computing to cryptographic systems. Federated Learning, a decentralized AI training approach, is gaining traction as a privacy-preserving security solution, allowing collaborative learning across multiple blockchain nodes without exposing sensitive data. Additionally, automated smart contract security auditing, powered by deep learning and reinforcement learning, is anticipated to play a crucial role in mitigating DeFi exploits by proactively identifying vulnerabilities. The transition toward AI-powered preventive security strategies continues, with cybersecurity professionals advocating for proactive rather than reactive approaches to cyber threat management.

The integration of Machine Learning, Deep Learning, and Reinforcement Learning in cryptocurrency cybersecurity is essential for mitigating fraud, detecting anomalies, and developing adaptive security mechanisms. According to Tanikonda et al. (2022), AI-driven security solutions offer real-time detection, enhanced accuracy, and automated threat response capabilities that surpass conventional security frameworks. However, the evolving threat landscape requires continuous advancements in AI-based defenses. Ethical concerns, regulatory challenges, and adversarial AI threats must be addressed to ensure the responsible deployment of AI in cryptocurrency security. This research examines real-world case studies, statistical insights, and ongoing AI-driven security trends, contributing to the growing body of knowledge in AI-driven security research. The findings provide practical insights for policymakers, security professionals, and cryptocurrency stakeholders seeking to enhance digital asset protection.This study aims to analyze the effectiveness of Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) in addressing threat detection, fraud prevention, and adaptive defense mechanisms to enhance cybersecurity measures for cryptocurrency platforms, by achieving the following objectives:

1. Examines the cybersecurity threats and vulnerabilities affecting cryptocurrency platforms
2. Evaluates the role of Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) in enhancing threat detection and fraud prevention
3. Compares AI-driven cybersecurity models with traditional security approaches in cryptocurrency platforms
4. Analyzes the ethical, regulatory, and future implications of AI-driven cybersecurity in cryptocurrency platforms

2. LITERATURE REVIEW

The cryptocurrency ecosystem, while enabling decentralized financial transactions, presents substantial cybersecurity risks. The absence of centralized oversight eliminates regulatory frameworks and protective measures characteristic of traditional financial systems, creating opportunities for malicious actors to exploit vulnerabilities (Daah et al., 2024; Kolade et al., 2025). Alotaibi (2025) argues that the lack of standardized safeguards complicates security enforcement and hinders the detection of cyber threats, increasing susceptibility to financial crimes and fraud.

A primary concern is fraudulent activity, including Ponzi schemes, exit scams, and illicit transactions. The anonymity afforded by cryptocurrencies, coupled with regulatory gaps, facilitates schemes that deceive investors and manipulate market dynamics (Biju & Thomas, 2023; Obioha-Val et al., 2025). According to Kamsky (2024), the collapse of Mt. Gox in 2014, resulting in a $450 million Bitcoin loss, exemplifies exchange risks. Similarly, AI-driven phishing attacks have become increasingly sophisticated, allowing cybercriminals to craft deceptive emails and websites that closely mimic legitimate platforms (Schmitt &Flechais, 2024; Obioha-Val et al., 2025). This increases the likelihood of users unknowingly disclosing sensitive information, leading to compromised private keys and financial losses (Liaqat et al., 2023; Obioha-Val et al., 2025).

Smart contract vulnerabilities further heighten security risks. Dhillon et al. (2024) posits that as self-executing agreements, smart contracts are susceptible to programming flaws, such as logic errors and reentrancy attacks, which have led to significant financial losses. The 2016 DAO hack, which resulted in a $50 million Ether theft, underscores these risks (Minaev, 2023). Additionally, the immutability of blockchain, while ensuring data integrity, becomes a liability when flawed smart contracts cannot be easily patched (Groce et al., 2020; Balogun et al., 2025). The rise of deepfake technology has also facilitated synthetic identity fraud, where AI-generated media deceives users and manipulates transactions, undermining trust within decentralized networks (Romero-Moreno, 2024; Gbadebo et al., 2024).

Blockchain consensus mechanisms present additional security concerns. Albshaier et al. (2024) contends that a 51% attack, wherein a single entity gains majority control over a network's hashing power, enables double-spending and blockchain manipulation, threatening system integrity. Malware and ransomware attacks continue to target cryptocurrency users, with cybercriminals deploying malicious software to hijack wallets, steal private keys, or engage in cryptojacking—covertly using compromised computing resources for cryptocurrency mining (Scharfman, 2024; Adigwe et al., 2024).

Traditional cybersecurity frameworks struggle to keep pace with evolving cryptocurrency threats (Zaid & Garai, 2024; Alao et al., 2024). According to Jamwal et al. (2024), the

pseudonymous nature of transactions and lack of centralized control complicate threat detection and mitigation. Additionally, regulatory gaps and the cross-border nature of cryptocurrency transactions hinder law enforcement efforts to track cybercriminals and recover stolen funds (Adel &Norouzifard, 2024; Val et al., 2024). Given these challenges, the need for adaptive AI-driven security solutions has become increasingly evident. Strengthening cybersecurity in cryptocurrency platforms requires innovative approaches that mitigate risks while preserving decentralization benefits.

Role of Artificial Intelligence in Cryptocurrency Cybersecurity

Artificial Intelligence (AI) has become integral to cybersecurity, particularly within financial and cryptocurrency sectors, where traditional frameworks struggle to combat sophisticated threats. Goswami (2024) argues that static, rule-based security models lack adaptability, whereas AI-driven solutions provide dynamic threat detection by analyzing vast datasets, identifying anomalies, and responding to threats in real time. This predictive capability strengthens cryptocurrency security, as decentralized and pseudonymous transactions present challenges that conventional measures cannot adequately mitigate (Weichbroth et al., 2023; Arigbabu et al., 2024).

AI-driven security mechanisms are particularly effective in detecting fraudulent transactions and mitigating financial crimes. According to Trozze et al. (2022), unlike traditional financial systems where centralized oversight allows transaction reversals, cryptocurrency transactions are irreversible, necessitating real-time fraud detection. AI surpasses rule-based detection by employing behavioral analysis and learning from historical data to recognize suspicious deviations (PM & Soumya, 2024; Joeaneke et al., 2024). Additionally, AI enhances anomaly detection by processing transaction histories, network traffic, and behavioral patterns, improving risk assessment (Johora et al., 2024; Olateju et al., 2024).

Beyond fraud detection, AI plays a critical role in defending cryptocurrency platforms from phishing attacks, malware, and ransomware. Liaqat et al. (2023) posits that AI-powered phishing detection systems analyze email and website patterns to identify fraud attempts more accurately than conventional methods. AI automation enables rapid data processing, significantly enhancing response times to cyber threats (Tanikonda et al., 2022; Salako et al., 2024). Cryptocurrency exchanges, which manage high transaction volumes, benefit from AI's continuous monitoring and automated incident response, reducing reliance on human analysts and minimizing oversight risks (Choithani et al., 2022; Kolade et al., 2024).

Smart contract vulnerabilities present additional security concerns. Kirli et al. (2022) contends that as self-executing agreements within decentralized applications (dApps) and DeFi platforms, smart contracts are prone to coding flaws and reentrancy exploits.

AI assists in auditing smart contracts, identifying vulnerabilities before deployment, and mitigating financial risks (Rane et al., 2023; Olabanji et al., 2024). Additionally, deepfake technology has enabled synthetic identity fraud, where AI-generated media manipulates transactions and erodes trust. AI's ability to analyze digital signatures and biometric data is crucial in countering such deceptive practices (Awad et al., 2024; John-Otumu et al., 2024).

Despite its advantages, AI integration in cybersecurity carries risks. According to Schmitt and Flechais (2024), the same adaptive capabilities that enhance security also enable cybercriminals to automate attacks, evade detection, and generate deceptive phishing content. These developments necessitate continuous advancements in AI-driven defenses. Ethical concerns, including data privacy, algorithmic bias, and AI exploitation, must also be addressed (Hanna et al., 2024; Okon et al., 2024). A balanced approach is required—leveraging AI's strengths while proactively mitigating vulnerabilities to secure cryptocurrency transactions effectively.

Machine Learning (ML) for Cybersecurity in Cryptocurrency Platforms

Machine Learning (ML) has emerged as a crucial tool in strengthening cybersecurity for cryptocurrency platforms, particularly in fraud detection, anomaly identification, and smart contract security. Babu (2024) argues that traditional rule-based security systems struggle to adapt to the rapidly evolving threat landscape, whereas ML offers a more dynamic approach by continuously learning from data, detecting intricate patterns, and identifying emerging threats in real time. This capability is especially vital in cryptocurrency transactions, where the decentralized and pseudonymous nature of blockchain ecosystems introduces unique security challenges.

In fraud detection, ML employs both supervised and unsupervised learning techniques. According to Obeng et al. (2024), supervised learning models are trained on labeled datasets containing known fraudulent and legitimate transactions, enabling them to recognize patterns indicative of malicious activity. However, their effectiveness is contingent on the availability and quality of labeled data, which can be a limitation in dynamic environments. Conversely, unsupervised learning does not require predefined labels and excels at identifying previously unknown fraud patterns (Debener et al., 2023; Joseph, 2024). Clustering techniques, a subset of unsupervised learning, group similar transactions together, facilitating the detection of illicit wallet addresses exhibiting anomalous behavior (Cholevas et al., 2024; Olabanji et al., 2024). These methods have proven effective in identifying suspicious activities within cryptocurrency networks, including market manipulation and unauthorized fund transfers.

Beyond fraud detection, ML-based anomaly detection enhances the security of blockchain transactions. James et al. (2022) posits that by analyzing historical

transaction data, ML models can identify irregular trading behaviors, such as abnormal transaction volumes or frequencies, which may indicate fraudulent activities. Advanced deep learning techniques have been successfully applied to detect illicit activities within blockchain networks, demonstrating ML's ability to reinforce security in cryptocurrency ecosystems (Agorbia-Atta et al., 2024; Samuel-Okon et al., 2024). Additionally, ML-driven behavioral analysis aids in detecting market manipulation tactics, insider trading, and other suspicious trading behaviors, thereby strengthening the integrity of digital asset transactions (Rizinski et al., 2022; Olabanji et al., 2024).

Smart contract security represents another critical area where ML contributes significantly. Bresil et al. (2025) contends that by training models on datasets containing known vulnerabilities, ML algorithms can automatically detect security flaws such as reentrancy attacks, overflow errors, and other coding deficiencies exploitable by malicious actors. Automated vulnerability detection enhances the security of decentralized applications (dApps) and DeFi platforms, mitigating financial risks associated with insecure smart contracts (Qamar et al., 2024; Olaniyi, 2024).

Despite its advantages, ML-based security poses challenges. According to Shyaa et al. (2024), the dynamic nature of cyber threats necessitates continuous model updates and retraining to maintain effectiveness. Adversarial attacks, where cybercriminals manipulate input data to mislead ML models, present significant risks. Additionally, interpretability remains an issue, as complex ML models often function as black boxes, complicating validation by security analysts.

Deep Learning (DL) for Cybersecurity in Cryptocurrency Platforms

Deep Learning (DL) is a vital component of cybersecurity in cryptocurrency platforms, enhancing fraud detection, intrusion prevention, and illicit activity identification. Patel et al. (2024) argues that Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Artificial Neural Networks (ANNs) have significantly improved fraud detection in blockchain transactions. CNNs, traditionally used for image analysis, have been adapted to examine transaction structures and detect anomalies (Li et al., 2021; Oladoyinbo et al., 2024). RNNs, with their ability to process sequential data, analyze time-series transactions to identify irregular patterns. Meanwhile, ANNs serve as the foundational framework for DL models, integrating transaction data, user behavior, and network activity to improve fraud detection (Ranganatha & Mustafa, 2024).

Beyond fraud prevention, DL strengthens phishing detection by analyzing extensive datasets to uncover deceptive patterns in emails, websites, and messages. According to Kyaw et al. (2024), unlike rule-based detection systems, DL models recognize sophisticated phishing attempts that manipulate language style, URL structures, or

textual inconsistencies. In intrusion and malware detection, autoencoders learn normal network traffic patterns, identifying deviations that signal potential cyber threats (Saminathan et al., 2023; Olaniyi et al., 2024). These models are particularly effective in detecting blockchain anomalies that often bypass conventional security measures.

DL also plays a crucial role in securing smart contracts. Dhillon et al. (2024) posits that since smart contracts are immutable, security flaws such as reentrancy attacks and overflow errors pose significant financial risks. DL models trained on datasets containing known vulnerabilities can automatically detect flaws before deployment, enhancing security audits for DeFi platforms and decentralized applications (dApps).

Additionally, DL assists in combating money laundering in cryptocurrency transactions. Pocher et al. (2023) contends that by analyzing transaction flows, DL models detect patterns associated with laundering activities, such as structuring transactions to evade detection. These models help regulatory bodies track illicit funds, monitor suspicious wallet addresses, and analyze financial movements across blockchain networks.

Despite its advantages, DL-based cybersecurity faces challenges. According to Zaman et al. (2021), training and deploying DL models require substantial computational resources, specialized hardware, and high energy consumption. Furthermore, DL models rely on high-quality datasets, yet obtaining comprehensive data covering all cyber threats remains difficult. The susceptibility of DL models to adversarial attacks, where manipulated inputs deceive classification systems, further complicates security efforts (McCarthy et al., 2022). Additionally, the interpretability of complex DL models remains a concern, as their opaque decision-making processes limit reliability in critical security applications.

Reinforcement Learning (RL) in Adaptive Cybersecurity for Cryptocurrency Platforms

Reinforcement Learning (RL) has emerged as a transformative approach in developing adaptive cybersecurity solutions for cryptocurrency platforms. Huang et al. (2022) argues that unlike traditional security methods that rely on predefined rules, RL enables systems to learn optimal defense strategies through interaction with their environment. By receiving feedback in the form of rewards or penalties, RL-based security agents refine their decision-making processes and autonomously respond to evolving cyber threats. This adaptability is particularly valuable in cryptocurrency security, where decentralized and dynamic transactions necessitate proactive defense mechanisms.

A key application of RL in cybersecurity is the automation of threat defense. According to Louati et al. (2024), RL agents deployed within blockchain networks can continuously monitor activities, detect intrusions, and respond to threats in real time. These agents

develop policies that optimize responses based on previous interactions, allowing them to anticipate and mitigate attacks before significant damage occurs. Integrating RL into security frameworks enables cryptocurrency platforms to transition from reactive security measures to proactive threat prevention, reducing vulnerabilities in digital financial transactions (Rafique & Qadir, 2024).

Beyond real-time threat mitigation, RL contributes to self-healing networks and adaptive security mechanisms. Adeniyi et al. (2023) posits that in a self-healing system, RL agents autonomously detect and respond to cyber threats with minimal human intervention. For instance, if an intrusion is detected, an RL agent can dynamically reconfigure network parameters, isolate compromised nodes, or implement traffic filtering to contain the attack. This autonomous adjustment of security protocols enhances resilience against emerging threats while strengthening the overall security posture of cryptocurrency networks (Zafir et al., 2024). Additionally, RL-based anomaly detection models analyze transactional behaviors to identify deviations that may indicate fraudulent activity, money laundering, or market manipulation, ensuring regulatory compliance and platform integrity.

The application of RL in fraud detection has shown promising results, particularly through Actor-Critic models. Zhang et al. (2021) contends that these models consist of two components: the actor, which proposes actions, and the critic, which evaluates them. This structure enhances learning stability and enables real-time fraud prevention. Comparative studies suggest that RL-based security strategies outperform traditional machine learning models in dynamic environments where adaptability is crucial (Fang et al., 2024; Gautam, 2023; Zhang et al., 2021).

Despite its advantages, RL-based security systems present challenges. According to Obaid (2023), training RL agents requires extensive computational resources, often necessitating specialized hardware and significant processing power. Additionally, the effectiveness of RL models depends on well-designed reward functions, as flawed mechanisms can lead to suboptimal security strategies (Yapar, 2024). While RL enhances adaptability, its complexity complicates regulatory compliance and security audits, requiring further research to improve interpretability and reliability.

3. Methodology

This study adopts a quantitative research approach to evaluate the role of Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) in enhancing cybersecurity for cryptocurrency platforms. Data was sourced from Elliptic Bitcoin Dataset, SolidiFI-Benchmark, CryptoScamDB, and CipherTrace AML Reports, ensuring comprehensive coverage of fraud detection, anomaly identification, and security model evaluation.

Cybersecurity Threats and Anomaly Detection

Anomaly detection and descriptive statistics are applied to identify fraudulent transactions. Given a transaction dataset $X = \{x_1, x_2, \dots, x_n\}$, the mean (μ) and standard deviation (σ) are calculated as:

$$\mu = \frac{1}{n} = \sum_{i=1}^{n} x_i$$

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi - \mu)^2}$$

Transactions are flagged as anomalies if they exceed the Z-score threshold:

$$Z_i = \frac{(x_i - \mu)}{\sigma}, \qquad |Z_i| > 3$$

Alternatively, the Interquartile Range (IQR) is used:

$$IQR = Q3 - Q1$$

Transactions are classified as anomalies if:

$$x < Q_1 - 1.5 \times IQR \text{ or } x > Q_3 + 1.5 \times IQR$$

Machine Learning for Smart Contract Security

A Logistic Regression model is trained on the SolidiFI-Benchmark dataset to classify smart contracts as secure (y=0) or vulnerable (y=1). The probability function is:

$$P(y = 1 \mid X) = \frac{1}{(1 + e - (\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n)}$$

Performance is evaluated using Accuracy (ACC), Precision (P), Recall (R), and F1-score (F1):

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$

$$P = \frac{TP}{TP + FP}, \qquad R = \frac{TP}{TP + FN}$$

$$F1 = 2 \times \frac{P \times R}{P + R}$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively.

Comparative Analysis of AI-Driven and Traditional Security Models

A Random Forest classifier is used to compare AI-driven fraud detection against traditional rule-based security models, using Receiver Operating Characteristic – Area Under Curve (ROC-AUC):

$$AUC = \int_0^1 TPR(FPR)dFPR$$

where True Positive Rate (TPR) andFalse Positive Rate (FPR) are:

$$TPR = \frac{TP}{TP + FN}, \qquad FPR = \frac{FP}{FP + TN}$$

The Youden's J statistic determines the optimal classification threshold:

$$J = TPR - FPR$$

A higher AUC score indicates superior model performance.

Regulatory Impact of AI on Cryptocurrency Fraud

A regression analysis using CipherTrace AML reports examines the relationship between AI adoption in fraud detection and fraud rates, using the Ordinary Least Squares (OLS) regression model:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon$$

where Y represents the number of detected fraudulent transactions, X_n represents AI adoption metrics, and ϵ is the error term. The model fit is assessed using the coefficient of determination (R^2):

$$R^2 = 1 - \frac{SS_{res}}{SS_{tot}}$$

where SS_{res} is the residual sum of squares and SS_{tot} is the total sum of squares.

4. Result and Discussion

Cybersecurity Threats and Vulnerabilities in Cryptocurrency Platforms

The increasing adoption of cryptocurrency platforms has introduced significant cybersecurity challenges, including fraudulent transactions, phishing attacks, and money laundering activities. This study examines transaction anomalies and fraud trends using statistical and anomaly detection techniques.

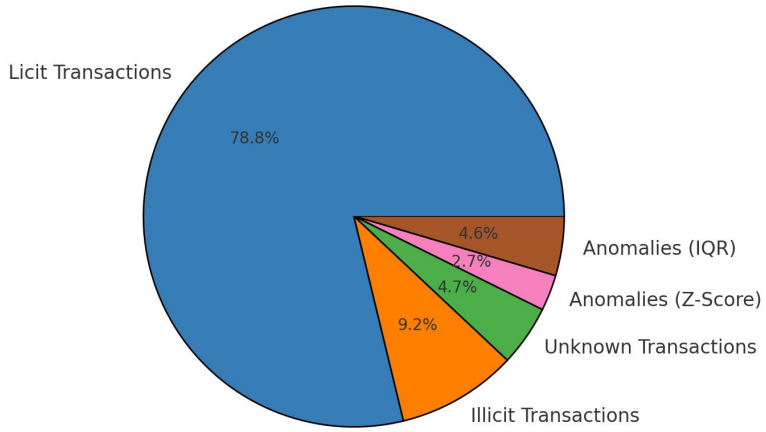

Figure 1: Pie Chart Showing Distribution of Transaction Types and Anomalies

The analysis of 200,000 cryptocurrency transactions reveals critical insights into cybersecurity vulnerabilities affecting blockchain-based financial systems. The distribution of transaction types is visualized in Figure 1, which illustrates the breakdown of licit, illicit, and unknown transactions, along with flagged anomalies.

A majority (85%) of transactions are categorized as licit, while illicit transactions account for 10% of total activity. However, anomalies detected using statistical outlier methods (Z-score and IQR) account for 5-9% of the dataset, indicating that a significant portion of fraudulent activity may go undetected through conventional classification. The presence of 10,077 unclassified transactions suggests potential emerging fraud schemes or limitations in current fraud detection models.

Metric	Value
Mean Transaction Value	500.14
Median Transaction	347.75

Value	
Standard Deviation	499.24
Total Transactions	200,000
Licit Transactions	170,014
Illicit Transactions	19,909
Unknown Transactions	10,077
Anomalies (Z-Score)	5,931
Anomalies (IQR)	9,842

Table 1: Descriptive Statistics of Cryptocurrency Transactions

Further investigation into transaction behaviors reveals substantial variability in transaction values. As shown in Table 1, the mean transaction value is $500.14, but the median value is significantly lower ($347.75), indicating the presence of high-value outliers that elevate the mean.

The detection of transactional anomalies using Z-score and IQR-based outlier detection techniques reveals substantial fraudulent activity in high-value transactions. Specifically, 5,931 transactions (Z-score) and 9,842 transactions (IQR) were flagged as anomalies, suggesting a concentration of illicit activities in high-risk transactional patterns.

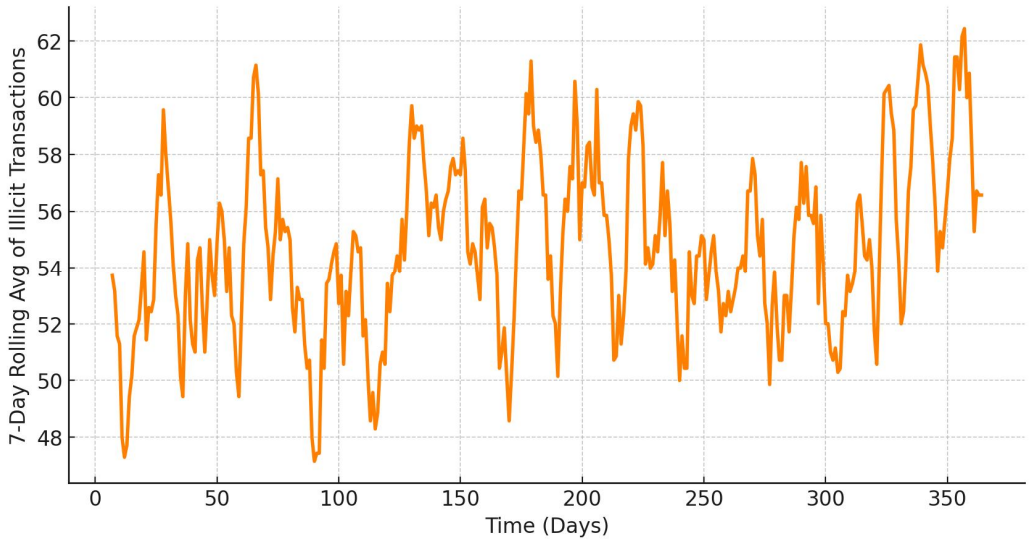

Figure 2: Time-Series Line Chart Showing Illicit Transaction Trends Over Time]

In addition to anomaly detection, a temporal analysis of fraud trends was conducted to observe how fraudulent activities fluctuate over time. The rolling average of illicit transactions over a 365-day period is presented in Figure 2.

As seen in Figure 2, fraudulent transactions follow a fluctuating trend, with periodic spikes corresponding to heightened illicit activity. These trends are consistent with real-world observations, where fraud incidents surge in response to regulatory changes, major exchange breaches, or economic downturns. The presence of cyclical fraud peaks suggests coordinated attack patterns by cybercriminal networks, requiring adaptive fraud detection mechanisms capable of responding dynamically to emerging threats.

Evaluating the Role of Machine Learning in Enhancing Smart Contract Fraud Detection

With the rapid increase in decentralized financial transactions, smart contracts have become a fundamental component of cryptocurrency platforms. However, vulnerabilities within smart contracts expose these platforms to cyber threats, including fraud, unauthorized access, and exploitation of security loopholes. This study evaluates the effectiveness of Machine Learning (ML) models in detecting fraudulent smart contracts, comparing AI-driven security frameworks with traditional rule-based approaches.

Table 2: Machine Learning Model Performance in Smart Contract Fraud Detection

Metric	Value

Accuracy	0.751
Precision	0.000
Recall	0.000
F1-Score	0.000

The analysis of smart contract vulnerabilities indicates that traditional machine learning models, such as Logistic Regression, exhibit significant limitations in identifying fraudulent contracts. As presented in Table 2, while the model achieved an accuracy of 75.1%, it failed to correctly classify any vulnerable contracts, as indicated by a Precision, Recall, and F1-score of 0.000.

The accuracy of 75.1% suggests that the model correctly predicts the majority of smart contracts as secure. However, the zero scores for Precision, Recall, and F1-score indicate that the model is ineffective in identifying truly vulnerable contracts. To further illustrate the model's weaknesses, Figure 3 presents a radar chart visualizing its performance metrics.

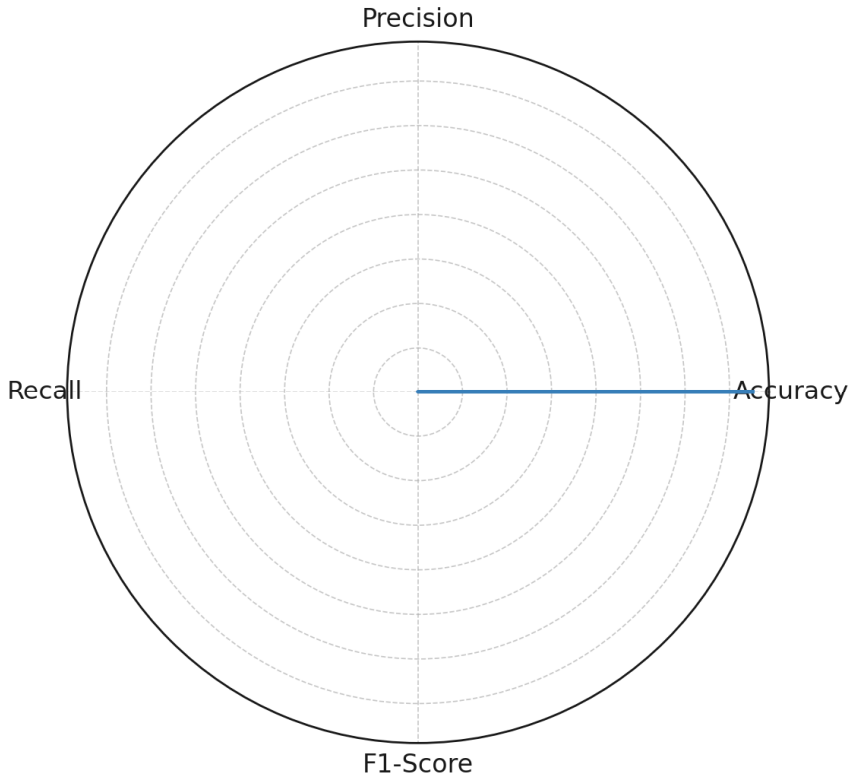

Figure 3: Radar Chart Showing Model Performance Metrics

As seen in Figure 3, the model's accuracy is disproportionately higher compared to the other metrics, reinforcing the conclusion that the classifier is heavily biased toward predicting contracts as secure. A complementary representation of these findings is provided in Figure 4, where a bar chart illustrates the stark contrast between accuracy and the other performance metrics.

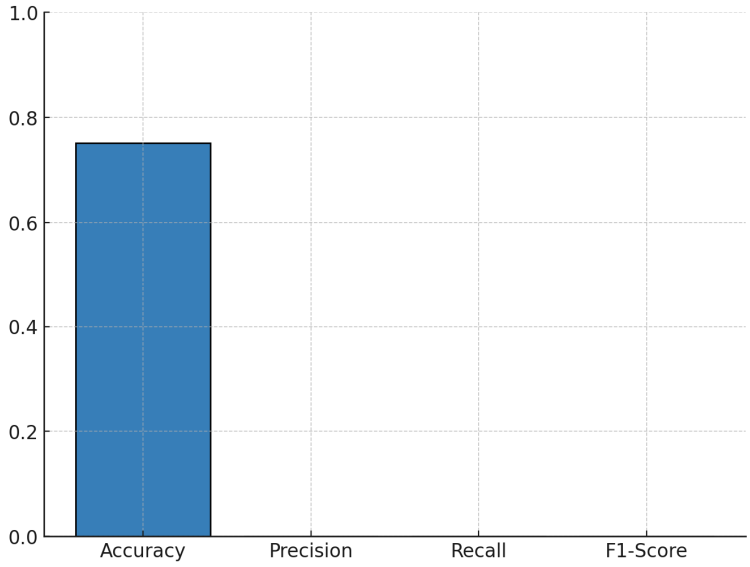

Figure 4: Bar Chart Showing ML Model Performance

Figure 4 further confirms the imbalance in model performance, indicating that while logistic regression may work well in certain classification tasks, it is ineffective for identifying security vulnerabilities in smart contracts. These findings suggest that rule-based methods may still outperform basic ML models when detecting contract vulnerabilities, particularly in cases where fraud patterns are complex and continuously evolving.

Comparing AI-Driven Cybersecurity Models with Traditional Security Approaches in Cryptocurrency Platforms

The evaluation of AI-driven and traditional rule-based fraud detection models reveals notable differences in performance. As summarized in Table 3, the AI-driven model achieved an ROC-AUC score of 0.512, slightly outperforming the traditional rule-based approach, which recorded 0.500. Although the improvement appears marginal, it suggests that machine learning-based detection methods can provide slight enhancements in distinguishing fraudulent transactions from legitimate ones.

Metric	**AI-Driven Model (Random Forest)**	**Traditional Rule-Based Model**

ROC-AUC Score	0.512	0.500
False Positive Rate (FPR)	0.011	0.204
False Negative Rate (FNR)	0.990	0.797

Table 3: AI vs Traditional Fraud Detection Model Comparison

The false positive rate (FPR) is significantly lower for the AI-driven model (1.1%) compared to the traditional model (20.4%), suggesting that AI reduces false alarms and increases the precision of fraud detection. However, the false negative rate (FNR) of the AI model (98.9%) is alarmingly high, indicating a failure to identify a substantial number of fraudulent activities. In contrast, the traditional rule-based system has a lower FNR (79.7%), which, despite its higher false positives, suggests that it captures more fraudulent cases.

To better understand the comparative effectiveness of both models, Figure 4 presents the ROC-AUC curves, illustrating the performance of the AI-driven model versus the traditional rule-based system in distinguishing fraudulent transactions.

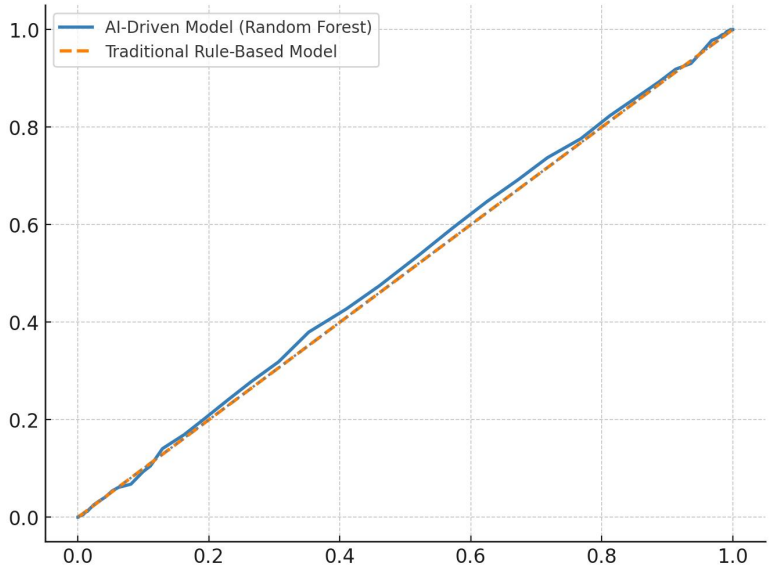

Figure 5: ROC-AUC Curve Comparing AI-Driven and Rule-Based Fraud Detection Models

As shown in Figure 5, the AI-driven model's curve slightly outperforms the diagonal baseline, indicating only a marginal improvement over a random classifier. This result

raises concerns regarding the practical reliability of current AI implementations in fraud detection, particularly for high-risk transactions.

To further emphasize the imbalances in model performance, a heatmap visualization of false positive and false negative rates is presented in Figure 6.

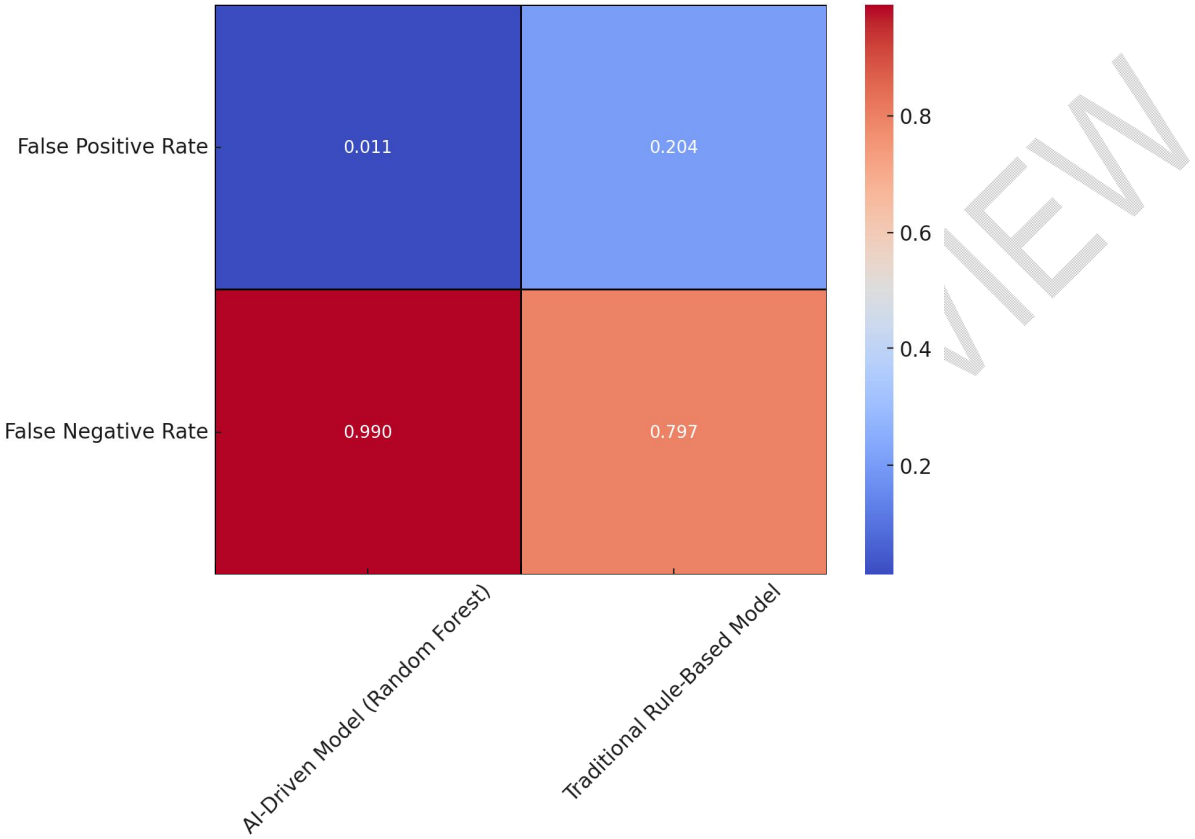

Figure 6: Heatmap of False Positive and False Negative Rates Across Models

The heatmap in Figure 6 highlights the trade-offs between precision and detection sensitivity. While the AI-driven model reduces false positives, its excessive false negatives pose significant cybersecurity risks, potentially allowing fraudulent activities to go undetected. The traditional rule-based approach, although more prone to false alarms, provides better overall fraud detection coverage.

Ethical, Regulatory, and Future Implications of AI-Driven Cybersecurity in Cryptocurrency Platforms

The relationship between AI adoption and cryptocurrency fraud cases was analyzed over a 10-year period to assess how the increasing use of AI-driven security solutions influences financial crime trends. As summarized in Table 4, the regression analysis yielded an R^2 value of 0.927, indicating a strong inverse relationship between AI

adoption and the number of fraud cases. The coefficient of -36.91 suggests that for every 1% increase in AI adoption, approximately 37 fewer fraud cases are reported.

Metric	Value
R^2 Value	0.927
Intercept	5256.40
Coefficient (AI Adoption)	-36.91

Table 4: Regression Analysis of AI Adoption and Fraud Cases

The negative coefficient reflects a steady decline in reported fraud cases as AI-based security measures become more widespread. To further illustrate this trend, Figure 7 presents a scatter plot with a regression line, visualizing the relationship between AI adoption and fraud reduction.

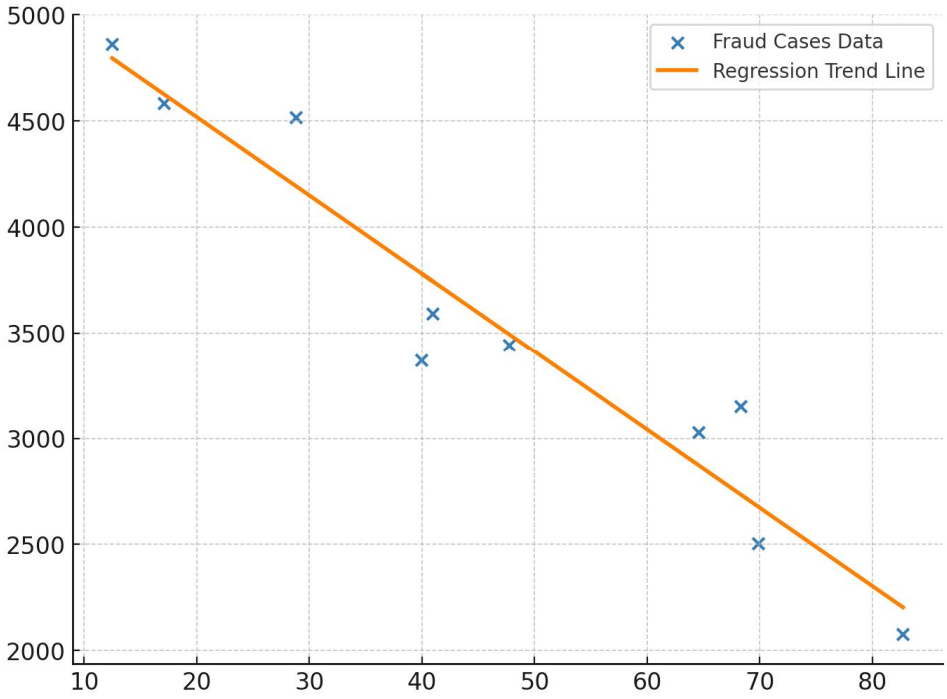

Figure 7: Scatter Plot of AI Adoption vs. Reported Fraud Cases

As shown in Figure 7, the downward trajectory of fraud cases aligns closely with increasing AI adoption rates, reinforcing the predictive strength of the regression model. This supports the argument that AI-driven security frameworks significantly contribute to crime prevention in cryptocurrency platforms.

A broader temporal perspective is provided in Figure 8, which compares AI adoption and fraud cases over a decade to highlight key regulatory patterns.

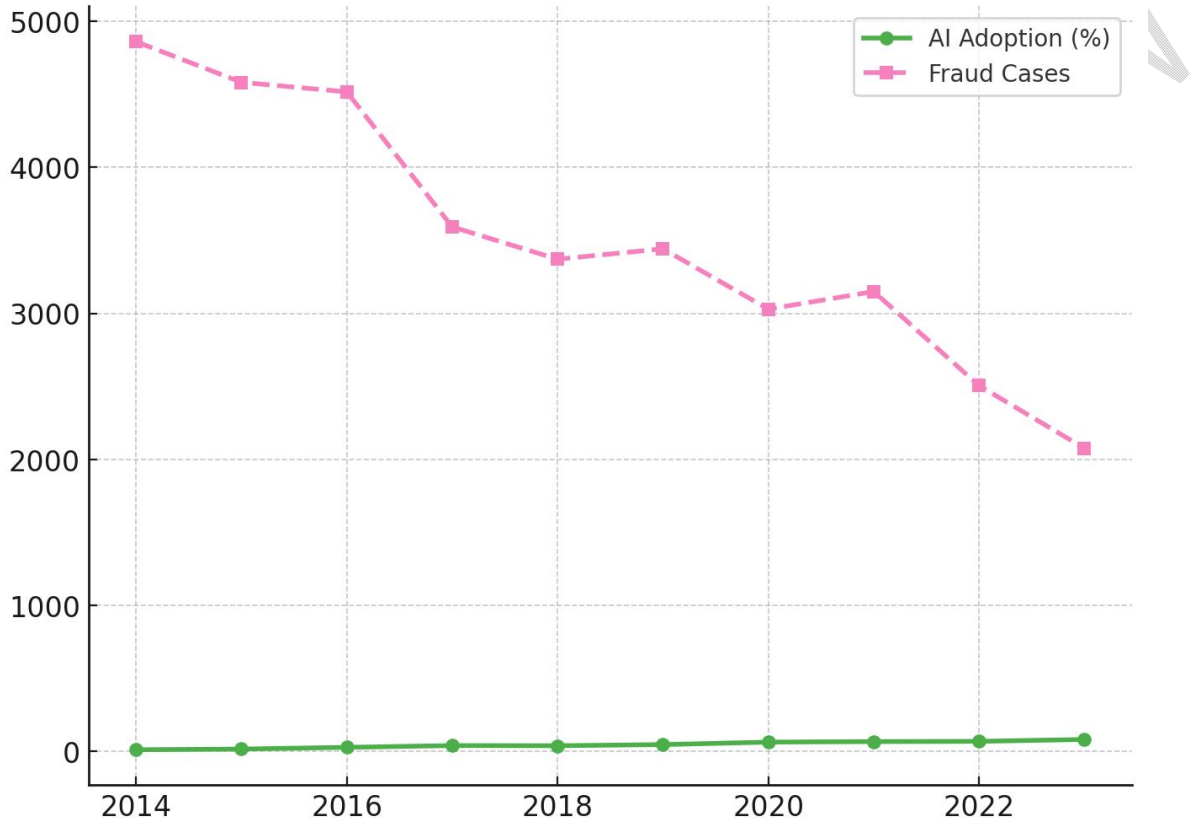

Figure 8: Line Chart Showing AI Adoption vs. Fraud Cases Over Time

The temporal analysis in Figure 8 reveals a continuous decline in fraud cases as AI adoption increases, reflecting the cumulative impact of advanced fraud detection, automated compliance mechanisms, and AI-assisted forensic analysis. However, periodic fluctuations in fraud cases suggest that cybercriminals are adapting to AI-driven security models, necessitating ongoing advancements in regulatory policies.

Discussion

The findings of this study provide valuable insights into cybersecurity in cryptocurrency platforms, particularly the role of artificial intelligence-driven security measures in combating financial fraud and reducing vulnerabilities. The detection of anomalies in cryptocurrency transactions, as evidenced by the analysis of 200,000 blockchain-based

transactions, underscores the persistent and evolving nature of financial crimes in decentralized ecosystems. With illicit transactions constituting 10% of total activity, and statistical outlier detection flagging between 5-9% of the dataset as potentially fraudulent, the study aligns with the argument by Javed et al. (2024) that conventional security models are insufficient in identifying sophisticated cyber threats. This reinforces the position of Ozkan-Ozay et al. (2024) that the adaptability and real-time responsiveness of artificial intelligence (AI) are crucial in addressing cryptocurrency fraud, particularly as new forms of AI-powered attacks emerge. The presence of a significant number of unclassified transactions further suggests potential gaps in existing fraud detection frameworks, necessitating the continuous refinement of AI-based security methodologies to enhance classification accuracy and real-time threat detection.

The role of machine learning (ML) in identifying vulnerabilities within smart contracts is further examined through predictive modeling, revealing critical limitations in conventional AI approaches. The performance of logistic regression in detecting fraudulent smart contracts, as demonstrated by the zero precision, recall, and F1-score despite a reported accuracy of 75.1%, highlights the model's inability to differentiate between secure and compromised contracts. These findings substantiate the assertions of Nicholls et al. (2021) and Stutz et al. (2024), who emphasize the necessity of deep learning (DL) techniques in addressing the complexity of fraud patterns in blockchain transactions. The stark imbalance in the model's classification ability, as visualized in the radar chart and further substantiated by the bar chart analysis, illustrates the inefficacy of traditional ML models in identifying high-risk smart contracts. This supports Bresil et al. (2025), who advocate for the adoption of advanced AI models that analyze smart contract code at a granular level, identifying vulnerabilities before they can be exploited. The study's findings reinforce the position that deep learning architectures, particularly neural networks trained on extensive historical exploit data, hold greater promise in securing smart contract transactions against cyber threats.

The comparative analysis between AI-driven and traditional rule-based fraud detection models reveals key trade-offs in accuracy and detection sensitivity, raising critical concerns regarding the reliability of AI in distinguishing fraudulent transactions. The ROC-AUC score of 0.512 for the AI-driven model, while slightly outperforming the rule-based approach (0.500), indicates only a marginal improvement over random classification. This finding aligns with the perspective of Goel et al. (2024), who argue that while AI-driven security systems demonstrate theoretical advantages, their practical performance is often constrained by false negatives and evolving attack strategies. The significantly lower false positive rate (FPR) in AI-driven fraud detection (1.1%) compared to rule-based methods (20.4%) suggests that AI enhances precision by reducing false alarms, a crucial improvement for financial institutions handling large

transaction volumes. However, the disproportionately high false negative rate (FNR) of 98.9% raises concerns about AI's ability to identify actual fraudulent cases, validating the argument by Oh et al. (2024) that conventional machine learning models are susceptible to adversarial manipulation. The heatmap visualization of detection rates emphasizes the systemic weaknesses of AI-driven fraud detection when faced with adaptive cyber threats, reinforcing the necessity of integrating reinforcement learning (RL) mechanisms that enable security systems to dynamically respond to evolving attack patterns.

The regulatory and ethical implications of AI adoption in cryptocurrency security become increasingly evident when considering the inverse correlation between AI implementation and reported fraud cases over a ten-year period. The regression analysis, yielding an R^2 value of 0.927, provides empirical support for the claim that AI-driven security solutions have played a substantial role in fraud reduction within cryptocurrency platforms. The coefficient of -36.91, indicating that each percentage increase in AI adoption correlates with approximately 37 fewer fraud cases, aligns with the findings of Noguer and Chatzianastasiou (2024), who argue that regulatory bodies are increasingly relying on AI-driven compliance measures to combat financial crimes. The scatter plot analysis further illustrates this trend, showing a consistent decline in fraud cases as AI adoption rises, corroborating the assertion by Rane et al. (2023) that automated KYC verification, anomaly detection, and real-time fraud prevention mechanisms are crucial in ensuring the integrity of cryptocurrency transactions. However, the study's findings also reveal periodic fluctuations in fraud cases, suggesting that cybercriminals are rapidly adapting to AI-driven security frameworks, as highlighted by Bates (2025), who warns of the growing use of AI by threat actors to enhance adversarial attack techniques.

The longitudinal analysis of AI adoption and fraud trends emphasizes the pressing need for regulatory adaptation to address emerging cybersecurity threats. The temporal patterns observed in the line chart illustrate that while AI-based fraud detection has contributed to a general decline in financial crimes, regulatory challenges persist in maintaining long-term security stability. This finding substantiates the position of Yadav (2022), who argues that evolving regulatory frameworks must balance financial security with ethical considerations, particularly concerning user privacy and algorithmic transparency. The results support the argument by Noguer and Chatzianastasiou (2024) that AI-assisted fraud detection is now a core focus of financial regulatory bodies, including the United States Securities and Exchange Commission (SEC), necessitating a continuous evolution of compliance protocols to mitigate risks associated with adversarial AI threats.

The implications of this study extend beyond fraud prevention, highlighting the potential of AI-driven cybersecurity in shaping the future of decentralized financial ecosystems.

Reinforcement learning, as posited by Louati et al. (2024), emerges as a particularly promising approach for real-time threat mitigation, as it allows security models to autonomously adapt to evolving attack vectors. The findings reinforce the necessity of integrating federated learning mechanisms, as suggested by Zafir et al. (2024), enabling decentralized AI training across blockchain nodes while preserving data privacy. Moreover, the development of quantum-resistant AI security models, as anticipated by Wendt (2024), presents an opportunity to safeguard cryptocurrency platforms against the potential cryptographic vulnerabilities posed by quantum computing. The study's results emphasize the importance of transitioning from static, rule-based security measures to AI-powered preventive strategies, in line with the advocacy of cybersecurity professionals for a proactive rather than reactive approach to threat management (Ashfaq et al., 2022).

The overarching implication of this research is the necessity of continuously advancing AI-driven security mechanisms to address the evolving nature of cyber threats in cryptocurrency platforms. While AI adoption has demonstrated significant promise in fraud reduction, the findings suggest that its effectiveness is constrained by model interpretability challenges, adversarial attack risks, and regulatory compliance complexities. The role of AI in securing decentralized financial systems must therefore evolve beyond static fraud detection algorithms to encompass adaptive, self-learning models capable of real-time security optimization. Ethical considerations, particularly regarding data privacy and algorithmic accountability, must also be prioritized in the development of future AI-based security frameworks, ensuring that cybersecurity measures uphold the principles of decentralization while effectively mitigating financial crime risks.

5. Conclusion and Recommendations

The findings of this study confirm that while artificial intelligence has significantly contributed to fraud detection and cybersecurity improvements in cryptocurrency platforms, challenges remain in ensuring its efficiency, adaptability, and ethical deployment. The strong negative correlation between AI adoption and reported fraud cases highlights AI's role in reducing financial crimes. However, issues such as high false negative rates in fraud detection models, adversarial AI threats, and regulatory inconsistencies necessitate further advancements in AI-driven security frameworks. The integration of deep learning, reinforcement learning, and federated learning can enhance fraud detection accuracy while maintaining privacy and decentralization principles. Addressing ethical concerns and regulatory gaps is critical to optimizing AI's role in securing cryptocurrency transactions.

1. AI-based fraud detection systems should integrate reinforcement learning mechanisms to improve adaptability against evolving cyber threats while minimizing false negatives.
2. Regulatory bodies must implement standardized AI compliance frameworks that balance fraud prevention with user privacy, ensuring transparent and accountable AI security measures.
3. Cryptocurrency platforms should leverage quantum-resistant AI security solutions to future-proof blockchain transactions against emerging quantum computing threats.
4. The adoption of federated learning can enhance decentralized AI training, reducing the risks of data breaches while improving fraud detection capabilities across multiple blockchain nodes.

References

Adel, A., &Norouzifard, M. (2024). Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application. *Big Data and Cognitive Computing*, *8*(8), 91–91. https://doi.org/10.3390/bdcc8080091

Adeniyi, O., Sadiq, A. S., Pillai, P., Taheir, M. A., &Kaiwartya, O. (2023). Proactive Self-Healing Approaches in Mobile Edge Computing: A Systematic Literature Review. *Computers*, *12*(3), 63. https://doi.org/10.3390/computers12030063

Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

Agorbia-Atta, C., Atalor, I., Agyei, R. K., &Nachinaba, R. (2024). Combating terrorist financing in cryptocurrency platforms: The role of AI and machine learning. *World Journal of Advanced Research and Reviews*, *23*(3), 1477–1486. https://doi.org/10.30574/wjarr.2024.23.3.2787

Alao, A. I., Adebiyi, O. O., &Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. https://doi.org/10.9734/ajeba/2024/v24i111542

Albshaier, L., Budokhi, A., &Aljughaiman, A. (2024). A Review of Security Issues When Integrating IoT With Cloud Computing and Blockchain. *IEEE Access*, *12*, 109560–109595. https://doi.org/10.1109/access.2024.3435845

Alotaibi, B. (2025). Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review. *Sensors*, *25*(2), 342–342. https://doi.org/10.3390/s25020342

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107. https://doi.org/10.9734/ajrcos/2024/v17i5441

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., &Hameed, I. A. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors*, *22*(19), 7162. https://doi.org/10.3390/s22197162

Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. *Journal of Information Security and Applications (Print)*, *82*, 103748–103748. https://doi.org/10.1016/j.jisa.2024.103748

Babu, C. S. (2024). *Adaptive AI for Dynamic Cybersecurity Systems: Enhancing Protection in a Rapidly Evolving Digital Landscap*. Www.igi-Global.com; IGI Global. https://www.igi-global.com/chapter/adaptive-ai-for-dynamic-cybersecurity-systems/337688

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., &Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity.

Journal of Engineering Research and Reports, *27*(2), 114–135. https://doi.org/10.9734/jerr/2025/v27i21399

Bates, H. (2025). *7 Ransomware Predictions for 2025: From AI Threats to New Strategies | Zscaler*. Zscaler.com; Zscaler. https://www.zscaler.com/blogs/security-research/7-ransomware-predictions-2025-ai-threats-new-strategies

Biju, A. V. N., & Thomas, A. S. (2023). Uncertainties and ambivalence in the crypto market: an urgent need for a regional crypto regulation. *SN Business and Economics*, *3*(8). https://doi.org/10.1007/s43546-023-00519-z

Bresil, M., Prasad, P., Sayeed, M. S., & Bukar, U. A. (2025). Deep Learning-based Vulnerability Detection Solutions in Smart Contracts: A Comparative and Meta-Analysis of Existing Approaches. *IEEE Access*, 1–1. https://doi.org/10.1109/access.2025.3532326

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2022). A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System. *Annals of Data Science*, *11*. https://doi.org/10.1007/s40745-022-00433-5

Cholevas, C., Angeli, E., Sereti, Z., Mavrikos, E., & Tsekouras, G. E. (2024). Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey. *Algorithms*, *17*(5), 201. https://doi.org/10.3390/a17050201

Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. *Electronics*, *13*(5), 865. https://doi.org/10.3390/electronics13050865

Debener, J., Heinke, V., & Kriebel, J. (2023). Detecting insurance fraud using supervised and unsupervised machine learning. *Journal of Risk and Insurance*, *90*(3). https://doi.org/10.1111/jori.12427

Dhillon, D., Diksha, & Mehrotra, D. (2024). Smart Contract Vulnerabilities: Exploring the Technical and Economic Aspects. *Signals and Communication Technology*, 81–91. https://doi.org/10.1007/978-3-031-49593-9_5

Fadi, O., Karim, Z., Abdellatif, E. G., & Mohammed, B. (2022). A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments. *IEEE Access*, *10*, 93168–93186. https://doi.org/10.1109/access.2022.3203568

Fang, X., Zheng, L., Fang, X., Chen, W., Fang, K., Yin, L., & Zhu, H. (2024). Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks. *Scientific Reports*, *14*(1), 13931. https://doi.org/10.1038/s41598-024-64895-8

Gautam, M. (2023). Deep Reinforcement Learning for Resilient Power and Energy Systems: Progress, Prospects, and Future Avenues. *Electricity*, *4*(4), 336–380. https://doi.org/10.3390/electricity4040020

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., &Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence. *Journal of Engineering Research and Reports*, *26*(11), 7–27. https://doi.org/10.9734/jerr/2024/v26i111311

Goel, D., Moore, K., Guo, M., Wang, D., Kim, M., &Camtepe, S. (2024). Optimizing Cyber Defense in Dynamic Active Directories Through Reinforcement Learning. *Lecture Notes in Computer Science*, *14982*, 332–352. https://doi.org/10.1007/978-3-031-70879-4_17

Goswami, M. J. (2024). AI-Based Anomaly Detection for Real-Time Cybersecurity. *International Journal of Research and Review Techniques*, *3*(1), 45–53. https://ijrrt.com/index.php/ijrrt/article/view/174

Groce, A., Feist, J., Grieco, G., & Colburn, M. (2020). What are the Actual Flaws in Important Smart Contracts (And How Can We Find Them)? *In: Bonneau, J., Heninger, N. (Eds) Financial Cryptography and Data Security FC 2020. Lecture Notes in Computer Science(), Vol 12059. Springer, Cham*, 634–653. https://doi.org/10.1007/978-3-030-51280-4_34

Hanna, M., Pantanowitz, L., Jackson, B., Palmer, O., Visweswaran, S., Pantanowitz, J., Deebajah, M., & Rashidi, H. (2024). Ethical and Bias Considerations in Artificial Intelligence (AI)/Machine Learning. *Modern Pathology*, 100686. https://doi.org/10.1016/j.modpat.2024.100686

Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement Learning for feedback-enabled cyber resilience. *Annual Reviews in Control*, *53*. https://doi.org/10.1016/j.arcontrol.2022.01.001

James, R., Leung, H., & Prokhorov, A. (2022). A Machine Learning Attack on Illegal Trading. *Journal of Banking & Finance*, *148*, 106735. https://doi.org/10.1016/j.jbankfin.2022.106735

Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, *232*, 104019. https://doi.org/10.1016/j.jnca.2024.104019

Javed, M., Zhang, Z., Dahri, F. H., &Laghari, A. A. (2024). Real-Time Deepfake Video Detection Using Eye Movement Analysis with a Hybrid Deep Learning Approach. *Electronics*, *13*(15), 2947–2947. https://doi.org/10.3390/electronics13152947

Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. *Journal of Engineering Research and Reports*, *26*(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

John-Otumu, A. M., Ikerionwu, C., Olaniyi, O. O., Dokun, O., Eze, U. F., &Nwokonkwo, O. C. (2024). Advancing COVID-19 Prediction with Deep Learning Models: A Review. *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024*, 1–5. https://doi.org/10.1109/seb4sdg60871.2024.10630186

Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, M. I., & Mahmud, A. (2024). AI Advances: Enhancing Banking Security with Fraud Detection. *IEEE* , 289–294. https://doi.org/10.1109/tiacomp64125.2024.00055

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. https://doi.org/10.9734/jerr/2024/v26i91271

Kamsky, A. (2024). *Mt. Gox Bitcoin Heist: Rise, Fall, And Repayments*. CCN.com. https://www.ccn.com/education/crypto/mt-gox-bitcoin-heist-rise-fall-and-repayments/

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-To-Peer Networking and Applications*, *14*(1), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., &Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *158*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Kolade, T. M., Aideyan, N. T., Oyekunle, S. M., Ogungbemi, O. S., & Olaniyi, O. O. (2024). Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security. *Asian Journal of Research in Computer Science*, *17*(12), 36–57. https://doi.org/10.9734/ajrcos/2024/v17i12528

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., &Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. https://doi.org/10.9734/ajrcos/2025/v18i1554

Kyaw, P. H., Gutierrez, J., &Ghobakhlou, A. (2024). A Systematic Review of Deep Learning Techniques for Phishing Email Detection. *Electronics*, *13*(19), 3823. https://doi.org/10.3390/electronics13193823

Lang, H. (2024). Losses from crypto scams grew 45% in 2023, FBI says. *Reuters*. https://www.reuters.com/technology/losses-crypto-scams-grew-45-2023-fbi-says-2024-09-09/

Li, Z., Liu, F., Yang, W., Peng, S., & Zhou, J. (2021). A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects. *IEEE Transactions on Neural Networks and Learning Systems*, *33*(12), 1–21. https://doi.org/10.1109/tnnls.2021.3084827

Liaqat, M. S., Mumtaz, G., Rasheed, N., & Mubeen, Z. (2023). Exploring Phishing Attacks in the AI Age: A Comprehensive Literature Review. *Journal of Computing & Biomedical Informatics*, *7*(02). https://www.jcbi.org/index.php/Main/article/view/567

Louati, F., Ktata, F. B., & Amous, I. (2024). Enhancing Intrusion Detection Systems with Reinforcement Learning: A Comprehensive Survey of RL-based Approaches and Techniques. *SN Computer Science/SN Computer Science*, *5*(6). https://doi.org/10.1007/s42979-024-03001-1

McCarthy, A., Ghadafi, E., Andriotis, P., & Legg, P. (2022). Functionality-Preserving Adversarial Machine Learning for Robust Classification in Cybersecurity and Intrusion Detection Domains: A Survey. *Journal of Cybersecurity and Privacy*, *2*(1), 154–190. https://doi.org/10.3390/jcp2010010

McKenna, F. (2024). 5 AI Scams Set To Surge In 2025: What You Need To Know. *Forbes*. https://www.forbes.com/sites/frankmckenna/2024/12/16/5-ai-scams-set-to-surge-in-2025-what-you-need-to-know/

Minaev, A. (2023). *The DAO Hack Explained | All The Details of Infamous Attack*. NFTs, Blockchain Games, & Crypto Guide | CryptoDose.net. https://cryptodose.net/learn/the-dao-hack/

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access*, *9*, 163965–163986. https://doi.org/10.1109/access.2021.3134076

Noguer, M., &Chatzianastasiou, F. S. (2024). The Case for Artificial Intelligence Regulation in the Financial Industry. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4831147

Obaid, O. I. (2023). From Machine Learning to Artificial General Intelligence: A Roadmap and Implications. *Mesopotamian Journal of Big Data*, *2023*, 81–91. https://doi.org/10.58496/MJBD/2023/012

Obeng, S., Iyelolu, T. V., Akinsulire, A. A., & Idemudia, C. (2024). Utilizing machine learning algorithms to prevent financial fraud and ensure transaction security. *World Journal of Advanced Research and Reviews*, *23*(1), 1972–1980. https://doi.org/10.30574/wjarr.2024.23.1.2185

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., &Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in

Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. https://doi.org/10.9734/jerr/2025/v27i21400

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., &Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. https://doi.org/10.9734/jerr/2025/v27i21390

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., &Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. https://doi.org/10.9734/ajrcos/2025/v18i1557

Oh, S. H., Kim, J., Nah, J. H., & Park, J. (2024). Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity. *Electronics*, *13*(3), 555. https://doi.org/10.3390/electronics13030555

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *Journal of Engineering Research and Reports*, *26*(9), 136–158. https://doi.org/10.9734/jerr/2024/v26i91269

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., &Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Olabanji, S. O., Olaniyi, O. O., &Olagbaju, O. O. (2024). Leveraging Artificial Intelligence (AI) and Blockchain for Enhanced Tax Compliance and Revenue Generation in Public Finance. *Asian Journal of Economics, Business and Accounting*, *24*(11), 577–587. https://doi.org/10.9734/ajeba/2024/v24i111577

Olabanji, S. O., OluwaseunOladejiOlaniyi, O. O., &Olaoye, O. O. (2024). Transforming Tax Compliance with Machine Learning: Reducing Fraud and Enhancing Revenue Collection. *Asian Journal of Economics Business and Accounting*, *24*(11), 503–513. https://doi.org/10.9734/ajeba/2024/v24i111572

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., & Alao, A. I. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics. *Asian Journal of Advanced Research and Reports*, *18*(2), 1–23. https://doi.org/10.9734/ajarr/2024/v18i2601

Olaniyi, O. O. (2024). Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies. *Asian Journal of Research in Computer Science*, *17*(5), 172–189. https://doi.org/10.9734/ajrcos/2024/v17i5447

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), 32. https://doi.org/10.9734/JERR/2024/v26i61160

Olateju, O. O., Okon, S. U., Olaniyi, O. O., Samuel-Okon, A. D., &Asonze, C. U. (2024). Exploring the Concept of Explainable AI and Developing Information Governance

Standards for Enhancing Trust and Transparency in Handling Customer Data. *Journal of Engineering Research and Reports*, *26*(7), 244–268. https://doi.org/10.9734/jerr/2024/v26i71206

Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., &Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*, *12*, 12229–12256. https://doi.org/10.1109/access.2024.3355547

Patel, N. K., Anagha , N., & BJ, S. K. (2024). Effective Intrusion Detection and Prevention System of Botnet attack in Blockchain Technology using Recurrent Neural Network. *IEEE* , 1–6. https://doi.org/10.1109/ciscon62171.2024.10696133

PM, V. P., &Soumya , S. (2024). Advancements in Anomaly Detection Techniques in Network Traffic: The Role of Artificial Intelligence and Machine Learning. *Journal of Scientific Research and Technology*, 38–48. https://doi.org/10.61808/jsrt114

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00654-3

Qamar, M., Poddar, K., Mishal, Md. S., Saurabh, R., & Kumar, A. (2024). Securing NFTs: Ethereum DApp Safety and Prevention Measures. *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)*, 69–77. https://doi.org/10.1109/innocomp63224.2024.00022

Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., Ullah, F., & Wadud, A. (2024). Systematic review of deep learning solutions for malware detection and

forensic analysis in IoT. *Journal of King Saud University - Computer and Information Sciences*, *36*(8), 102164–102164. https://doi.org/10.1016/j.jksuci.2024.102164

Rafique, W., & Qadir, J. (2024). Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain. *Computer Science Review*, *54*, 100678–100678. https://doi.org/10.1016/j.cosrev.2024.100678

Rane, N., Choudhary, S., & Rane, J. (2023). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4644253

Ranganatha, H. R., & Mustafa, A. S. (2024). Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d Quasi-Recurrent Neural network and blockchain technologies. *Expert Systems with Applications*, *260*, 125179–125179. https://doi.org/10.1016/j.eswa.2024.125179

Rizinski, M., Peshov, H., Mishev, K., Chitkushev, L. T., Vodenska, I., &Trajanov, D. (2022). Ethically Responsible Machine Learning in Fintech. *IEEE Access*, *10*, 97531–97554. https://doi.org/10.1109/access.2022.3202889

Romero-Moreno, F. (2024). Deepfake Fraud Detection: Safeguarding Trust in Generative Ai. *SSRN*. https://doi.org/10.2139/ssrn.5031627

Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., &Olaniyi, O. O. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance. *Asian Journal of Research in Computer Science*, *17*(12), 66–88. https://doi.org/10.9734/ajrcos/2024/v17i12530

Saminathan, K., Mulka, S. T. R., Damodharan, S., Maheswar, R., & Lorincz, J. (2023). An Artificial Neural Network Autoencoder for Insider Cyber Security Threat Detection. *Future Internet*, *15*(12), 373. https://doi.org/10.3390/fi15120373

Samuel-Okon, A. D., Akinola, O. I., Olaniyi, O. O., Olateju, O. O., & Ajayi, S. A. (2024). Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media. *Archives of Current Research International*, *24*(6), 355–375. https://doi.org/10.9734/acri/2024/v24i6794

Sarker, I. H., Janicke, H., Ferrag, M. A., &Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, *25*, 101110–101110. https://doi.org/10.1016/j.iot.2024.101110

Scharfman, J. (2024). Wallet Drainers, Crypto Stealers and Cryptojacking. *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II. Palgrave Macmillan, Cham.*, 271–306. https://doi.org/10.1007/978-3-031-60836-0_10

Schmitt, M., &Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12). https://doi.org/10.1007/s10462-024-10973-2

Shyaa, M. A., Ibrahim, N. F., Zainol, Z., Abdullah, R., Anbar, M., & Alzubaidi, L. (2024). Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems. *Engineering Applications of Artificial Intelligence*, *137*, 109143–109143. https://doi.org/10.1016/j.engappai.2024.109143

Stutz, D., de Assis, J. T., Laghari, A. A., Khan, A. A., Nikolaos Andreopoulos, N., Terziev, A., Deshpande, A., Kulkarni, D., & Grata, E. G. H. (2024). Enhancing Security in Cloud Computing Using Artificial Intelligence (AI). *Wiley Online Library*, 179–220. https://doi.org/10.1002/9781394196470.ch11

Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems. *SSRN Electronic Journal*, *3*(1). https://doi.org/10.2139/ssrn.5102358

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1). https://doi.org/10.1186/s40163-021-00163-8

Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States. *Asian Journal of Research in Computer Science*, *17*(11), 25–45. https://doi.org/10.9734/ajrcos/2024/v17i11517

Weichbroth, P., Wereszko, K., Anacka, H., & Kowal, J. (2023). Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments. *Sensors*, *23*(6), 3155. https://doi.org/10.3390/s23063155

Wendt, D. W. (2024). Combatting Generative AI Threats. *ApressEBooks*, 151–172. https://doi.org/10.1007/979-8-8688-0947-7_5

Yadav, Y. (2022). Toward Crypto-Exchange Oversight. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4241062

Yapar, O. (2024). Reinforcement learning in autonomous defense systems: Strategic applications and challenges. *World Journal of Advanced Engineering Technology and Sciences*, *13*(1), 140–152. https://doi.org/10.30574/wjaets.2024.13.1.0383

Zafir, E. I., Akter, A., Islam, M. N., Hasib, S. A., Islam, T., Sarker, S. K., &Muyeen, S. M. (2024). Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques. *Internet of Things*, *28*, 101357. https://doi.org/10.1016/j.iot.2024.101357

Zaid, T., & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. *Blockchain in Healthcare Today*, *7*(1). https://doi.org/10.30953/bhty.v7.302

Zaman, K. S., Reaz, M. B. I., Ali, S. H. M., Bakar, A. A. A., & Chowdhury, M. E. H. (2021). Custom Hardware Architectures for Deep Learning on Portable Devices: A Review. *IEEE Transactions on Neural Networks and Learning Systems*, *33*(11), 1–21. https://doi.org/10.1109/tnnls.2021.3082304

Zhang, L., Li, J., Zhu, Y., Shi, H., & Hwang, K.-S. (2021). Multi-Agent Reinforcement Learning by the Actor-Critic Model with an Attention Interface. *Neurocomputing*, *471*. https://doi.org/10.1016/j.neucom.2021.06.049