The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions

Abstract

Artificial intelligence is transforming cybersecurity in digital currency transactions by improving fraud detection and risk mitigation. This study utilizes the REKT Database, Elliptic Crypto Transaction Dataset, CipherTrace AML Reports, and IEEE DataPort Financial Transactions Dataset to assess AI's impact on fraud detection using logistic and linear regression, confusion matrix analysis, and fairness evaluation techniques. Findings show that AI-driven security measures reduced fraud by up to 76.86%, but models exhibited a high false-negative rate of 89.54%, leading to undetected fraudulent transactions. Algorithmic bias was also evident, with a disparate impact ratio of 0.7793, highlighting fairness concerns. To enhance AI's effectiveness, adversarial training, quantum-proof encryption, and transparent governance frameworks are recommended. The study emphasizes the need for regulatory adaptation and continuous AI advancements to strengthen fraud detection, mitigate ethical risks, and ensure the resilience of digital currency security frameworks.

Keywords: Artificial Intelligence, Cybersecurity, Digital Currency Fraud, Fraud Detection Models, Algorithmic Bias.

1. Introduction

The integration of Artificial Intelligence (AI) into cybersecurity has significantly influenced the security architecture of digital currency transactions. As cryptocurrencies such as Bitcoin and Ethereum gain widespread adoption alongside the potential emergence of Central Bank Digital Currencies (CBDCs), cyber threats targeting these financial systems have become increasingly sophisticated. The decentralized and pseudonymous nature of these currencies, coupled with their substantial financial value, renders them particularly vulnerable to cybercriminal activities. Traditional security measures have struggled to keep pace with these evolving threats, necessitating the adoption of advanced technologies to enhance fraud detection, anomaly identification, risk assessment, and regulatory compliance (Johora et al., 2024). AI has emerged as a pivotal tool in this regard, fortifying cybersecurity frameworks. However, while AI strengthens digital currency security, it simultaneously introduces new vulnerabilities,

including adversarial attacks, AI-powered cybercrime, and ethical concerns regarding data privacy and algorithmic bias (George, 2024).

The rapid expansion of digital currencies has positioned them as primary targets for cybercriminal activities such as fraud, money laundering, and hacking. According to Esoimeme (2024), cybercriminals are leveraging AI to enhance their attack strategies, employing deepfake technology, automated malware, and sophisticated market manipulation techniques to exploit vulnerabilities in blockchain networks. The growing use of Generative AI in creating highly advanced financial scams, is a trend that poses substantial risks to investors and financial institutions (Krause, 2024). Furthermore, projections indicate that cybercrime will impose an economic burden of approximately $10.5 trillion annually by 2025, reinforcing the urgency of AI-driven security measures (Hall, 2025).

Financial institutions have responded by increasing investments in AI-powered fraud detection and threat mitigation systems. TheOutpost (2023) argues that Visa, in 2023, successfully prevented fraudulent transactions worth $40 billion through real-time anomaly detection powered by AI. Similarly, Mastercard allocated $2.65 billion toward acquiring Recorded Future, a cybersecurity firm specializing in AI-driven threat intelligence, signifying the growing reliance on AI for digital currency security (Mastercard, 2024). These investments reflect the financial sector's acknowledgment of AI's critical role in countering evolving cyber threats.

AI's effectiveness in strengthening cybersecurity for digital currency transactions is further demonstrated through its practical applications across financial and governmental institutions. According to Oramas (2025), Chainalysis, a leading blockchain analytics firm, expanded its cybersecurity capabilities by acquiring Alterya in January 2025, integrating AI-powered fraud detection to preempt illicit activities. Additionally, the U.S. Department of Homeland Security's 2024 report examined the cybersecurity risks associated with CBDCs and acknowledged AI's role in fraud detection and transaction monitoring (Department of Homeland Security, 2024). Cryptocurrency exchanges, including Binance, have incorporated AI-driven threat intelligence systems to identify and mitigate security breaches, thereby protecting users from phishing attacks and malware (Kahil, 2024). Likewise, blockchain analytics firms such as Elliptic employ AI to track illicit transactions, assisting law enforcement agencies in identifying and prosecuting cybercriminals (Watson, 2024). These developments highlight AI's increasing influence in fortifying digital financial ecosystems.

Despite its advantages, AI-driven cybersecurity is not without challenges. One of the most pressing concerns is the weaponization of AI by cybercriminals. Romero-Moreno

(2024) contends that hackers are leveraging AI to develop advanced deepfake technologies and automated malware, significantly compromising authentication and identity verification systems. The Federal Bureau of Investigation (FBI) has issued warnings regarding the rising use of AI in cybercrime, emphasizing the necessity of proactive defense strategies to counteract these emerging threats (Nget et al., 2024). Additionally, adversarial machine learning techniques are being used to manipulate AI-driven security systems, deceiving fraud detection mechanisms into misclassifying illicit transactions as legitimate, thereby exposing vulnerabilities within AI-powered cybersecurity frameworks (Ghiurău& Popescu, 2024). These adversarial threats underscore the need for continuous enhancements in AI security protocols.

The regulatory implications of AI-driven cybersecurity for digital currencies remain a subject of intense debate. According to Reguerra (2024), the Financial Stability Board (FSB) addressed the regulatory challenges posed by AI-enabled financial crimes, and advocated for comprehensive governmental and institutional frameworks to mitigate risks while ensuring adherence to compliance standards. Similarly, the World Economic Forum (WEF) has underscored the necessity of international collaboration in addressing the ethical concerns and financial stability risks associated with AI in digital currencies (Mujica, 2025). A fundamental issue in AI regulation is ensuring transparency and fairness in decision-making processes, as biased algorithms could inadvertently lead to discriminatory financial practices. The vast datasets used in AI training further raise concerns regarding data privacy and security, necessitating strict regulatory oversight to balance innovation with consumer protection.

Moreover, AI's role in cybersecurity must account for emerging technological advancements that could redefine digital financial security. Akhai and Kumar (2024) posits that researchers are increasingly exploring the convergence of AI and quantum cryptography to develop quantum-resistant encryption techniques capable of significantly enhancing blockchain security. Additionally, AI-powered decentralized security frameworks are being developed to eliminate single points of failure within digital financial ecosystems, offering a more resilient defense mechanism against cyber threats (George, 2024). Biometric authentication methods, incorporating AI-driven facial and voice recognition, are also gaining traction as effective tools in mitigating unauthorized access to cryptocurrency accounts. Choithani et al. (2022) has demonstrated that AI-based biometric authentication can substantially improve security measures in digital financial transactions, further reinforcing AI's significance in safeguarding digital currency systems.

While AI presents transformative potential in securing digital currencies, its effectiveness depends on the continuous evolution of security measures, regulatory frameworks, and collaborative efforts among financial institutions, policymakers, and

technology experts. Onyekachukwu et al. (2024) argues that the dynamic nature of cybercriminal tactics necessitates an adaptive approach to AI-driven security solutions, ensuring that digital currency systems remain resilient against emerging threats. This study seeks to investigate the role and effectiveness of artificial intelligence in enhancing cybersecurity within the digital currency transaction ecosystem, exploring its applications in threat detection, fraud prevention, and risk management, while also considering the associated challenges and ethical implications, by achieving the following objectives:

1. Analyzes the current landscape of cyber threats targeting digital currency transactions
2. Evaluates the applications of artificial intelligence in mitigating cyber threats to digital currencies.

3. Assesses the effectiveness of AI-powered cybersecurity solutions in real-world digital currency transactions

4. Examines the challenges and ethical considerations associated with the implementation of AI in digital currency cybersecurity

Literature Review

Digital currency transactions are increasingly vulnerable to a range of cyber threats, encompassing both traditional security risks and emerging challenges unique to decentralized financial systems. These threats compromise the integrity of digital assets, posing significant risks to individual investors and the broader financial ecosystem (Arnone, 2024; Balogun et al., 2025).

According to Weichbroth et al. (2023), hacking and unauthorized access remain persistent issues within the cryptocurrency landscape, as cybercriminals exploit vulnerabilities in digital wallets, exchange platforms, and smart contracts to gain illicit control over assets. The 2014 Mt. Gox breach, resulting in the loss of approximately $450 million in Bitcoin, underscored the susceptibility of cryptocurrency exchanges to cyberattacks (McMillan, 2014; Kolade et al., 2025). Similarly, the 2018 Coincheck hack and the 2016 DAO exploit exposed security flaws within decentralized platforms, demonstrating the risks associated with smart contracts and exchange infrastructure (Ahmed, 2018; Obioha-Val et al., 2025). These incidents have eroded investor confidence and emphasized the need for stronger cybersecurity measures.

Phishing and social engineering attacks have also grown increasingly sophisticated, with cybercriminals using deception tactics to steal private keys and login credentials. Schmitt and Flechais (2024) contends that artificial intelligence has exacerbated these risks by enabling the creation of highly convincing phishing emails and deepfake scams. Reports from Europol and the United Nations indicate that generative AI now enhances fraudulent schemes, making it difficult for individuals to differentiate between legitimate and malicious communications (Esoimeme, 2024; Obioha-Val et al., 2025). These attacks, often executed through social media, exploit personal information to maximize effectiveness, further endangering cryptocurrency holders.

Cryptojacking and malware threats present additional cybersecurity challenges. Scharfman (2024) argues that attackers deploy malicious software to hijack computing resources for unauthorized cryptocurrency mining, leading to financial losses and system performance degradation. Also, cryptojacking malware can encrypt data or hijack processing power, compromising digital security (Alauthman et al., 2024; Obioha-Val et al., 2025).

The decentralized nature of blockchain networks also exposes them to 51% attacks, wherein a single entity gains majority control over a network's computing power, enabling transaction manipulation and asset theft (Dong et al., 2023; Alao et al., 2024). These attacks exploit weaknesses in blockchain consensus mechanisms, undermining decentralization and trust.

AI-driven cyber threats, including market manipulation and automated malware, introduce further security concerns. Ahmad (2023) posits that malicious actors use AI algorithms to analyze market trends, execute fraudulent trades, and exploit vulnerabilities in trading platforms. Chimbga (2023) warns that generative AI amplifies these concerns, necessitating heightened vigilance among businesses and consumers.

The 2021 Poly Network attack, in which hackers initially transferred over $610 million in digital assets before returning them, illustrated the vulnerabilities within decentralized finance platforms (Chavez-dreyfuss& Price, 2021; Val et al., 2024). Okorie (2024) contends that such breaches erode investor trust and raise concerns about the long-term stability of digital currencies. Addressing these threats requires continuous advancements in security protocols, regulatory frameworks, and technological defenses to safeguard digital financial ecosystems.

Applications of AI in Cybersecurity for Digital Currencies

Artificial Intelligence (AI) plays a crucial role in enhancing cybersecurity within digital currency ecosystems, offering advanced tools for threat detection, fraud prevention, and

regulatory compliance. Amankwah-Amoah et al. (2024) posits that machine learning algorithms are essential in analyzing vast datasets to detect anomalies in blockchain transactions, enabling early identification of fraudulent activities. By recognizing patterns indicative of illicit behavior, such as unusual transaction volumes or atypical trading activities, AI facilitates timely interventions. However, the accuracy of these models depends on the quality and diversity of training data, which varies across platforms (Sarker, 2021; Fabuyi et al., 2024).

AI-driven fraud scoring models further strengthen security in cryptocurrency exchanges by assessing transaction risks based on multiple parameters, including transaction history and user behavior. According to Johora et al. (2024), these models assign risk scores to flag suspicious activities for further review, improving fraud detection efficiency. However, concerns remain regarding data privacy and algorithmic bias, which can lead to false positives or negatives (Mühlhoff, 2021; Joeaneke et al., 2024).

Natural Language Processing (NLP), a subset of AI, is instrumental in identifying phishing attempts and scam communications. Amaar et al. (2022) argues that NLP algorithms analyze emails, messages, and websites to detect deceptive content designed to manipulate users. This application is particularly effective in mitigating social engineering attacks that exploit human vulnerabilities. However, the increasing sophistication of AI-generated fraudulent content presents ongoing challenges for NLP-based detection systems (Strasser, 2024; Samuel-Okon et al., 2024).

AI-powered risk assessment tools employ predictive analytics to identify potential cyber threats by analyzing historical data and recognizing patterns indicative of future risks. Tanikonda et al. (2025) contends that these tools enable proactive threat mitigation by allowing organizations to address vulnerabilities before they are exploited. However, their predictive accuracy can be limited by unforeseen variables and the rapidly evolving nature of cyber threats (Kalogiannidis et al., 2024; Kolade et al., 2024).

AI also plays a vital role in regulatory compliance within the digital currency ecosystem. AI-enabled Know Your Customer (KYC) and Anti-Money Laundering (AML) solutions automate identity verification and transaction monitoring, ensuring compliance with regulatory frameworks while mitigating financial crimes (Josyula, 2024; Adigwe et al., 2024). Vashishth et al. (2024) states that while these systems enhance efficiency, they

must be carefully managed to protect user privacy and prevent potential misuse of personal data.

Blockchain security benefits significantly from AI-driven anomaly detection and smart contract verification. According to Rane et al. (2023), AI enhances blockchain monitoring by identifying irregularities that may signal security breaches or fraudulent activities. Additionally, AI contributes to smart contract security by detecting vulnerabilities in code, reducing the risk of exploitation (Krichen, 2023; Joseph, 2024). Researchers are also exploring AI's role in developing quantum-resistant cryptographic techniques to safeguard digital assets against future threats posed by quantum computing (Akhai & Kumar, 2024; Paul et al., 2024; Arigbabu et al., 2024).

In the context of Central Bank Digital Currencies (CBDCs), AI enhances both security and operational efficiency. Johora et al. (2024) avers that AI-driven fraud detection models analyze transaction patterns and user behavior in real time, identifying suspicious activities while ensuring regulatory compliance. However, the deployment of AI in CBDCs necessitates careful consideration of ethical implications, data privacy concerns, and governance structures to manage associated risks.

Effectiveness of AI-Powered Cybersecurity Solutions in Digital Currency Transactions

Artificial Intelligence (AI) has become integral to cybersecurity in digital currency transactions, offering advanced solutions for fraud detection and risk mitigation. Ressi et al. (2024) posits that AI-powered analytics, such as those employed by AnChain.AI, enable real-time transaction monitoring and risk assessment, strengthening security across blockchain ecosystems. In the financial sector, Mastercard's acquisition of Recorded Future, an AI-driven threat intelligence firm, highlights AI's expanding role in enhancing cybersecurity defenses in financial transactions (Mastercard, 2024).

Compared to traditional cybersecurity methods, AI systems exhibit superior efficiency, accuracy, and scalability. Hernández-Rivas et al. (2024) contends that conventional frameworks rely on static rules and signature-based detection, which are often ineffective against evolving cyber threats. In contrast, AI processes vast datasets in real time, identifying anomalies and detecting emerging threats with greater precision

(Nassar & Kamal, 2021; Gbadebo et al., 2024). However, integrating AI into cybersecurity also introduces challenges, particularly adversarial attacks that exploit vulnerabilities in AI algorithms (Malatji & Tolah, 2024; Salako et al., 2024). The Bank for International Settlements warns that while generative AI enhances cybersecurity management, it also poses risks requiring continuous monitoring and refinement (Aldasoro et al., 2024; Olabanji et al., 2024).

The effectiveness of AI-powered cybersecurity solutions is evaluated through key performance metrics such as detection rates and false positive frequencies. According to Alhashmi et al. (2023), high detection rates demonstrate a system's proficiency in identifying cyber threats, whereas low false positive rates ensure accuracy in distinguishing legitimate transactions from fraudulent activity. AI's adaptability to emerging cyber threats is equally crucial, as cybercriminals continuously refine attack strategies. Babu (2024) avers that AI systems with dynamic learning capabilities can update threat detection models in response to new cyberattack methodologies, maintaining a strong security posture.

Financial institutions and cryptocurrency exchanges increasingly depend on AI for fraud prevention, risk management, and regulatory compliance. Rani and Mittal (2023) argues that AI-driven anomaly detection has significantly reduced fraudulent transactions, enhancing user trust in digital financial platforms. AI algorithms process extensive transaction data in real-time, recognizing suspicious patterns that human analysts might overlook (Paramesha et al., 2024; John-Otumu et al., 2024). Unlike traditional security frameworks, which struggle to keep pace with rapidly evolving cyber threats, AI-based systems remain adaptable, allowing for more effective risk mitigation (Habbal et al., 2024; Olaniyi et al., 2024).

While AI has markedly improved digital currency security, challenges persist in accurately assessing its effectiveness and ensuring resilience against evolving threats. Guesmi et al. (2023) posits that adversarial attacks designed to evade AI security measures remain a pressing concern, necessitating continuous research and system updates. Despite these challenges, AI continues to strengthen the security and resilience of digital currency transactions. As AI technology advances, its role in combating cyber threats will further reinforce the stability and growth of the digital economy.

Challenges and Ethical Considerations in AI-Based Cybersecurity

The integration of Artificial Intelligence (AI) into cybersecurity frameworks for digital currencies presents both technological advancements and complex challenges. A primary concern is AI's vulnerability to adversarial attacks, wherein malicious actors manipulate AI-driven fraud detection mechanisms through deceptive inputs. Chakraborty et al. (2023) argues that such attacks can lead to system failures, allowing fraudulent transactions to bypass security measures. Additionally, synthetic data generation can be exploited to train AI models on malicious patterns, further compromising their integrity (Agrawal et al., 2024; Okon et al., 2024).

Data security and privacy concerns further complicate AI deployment in digital currency cybersecurity. Olabanji et al. (2024) contends that AI systems require access to vast amounts of sensitive financial data, increasing the risk of unauthorized access and data breaches. Ensuring compliance with global data privacy regulations is particularly challenging given that digital currency transactions operate across multiple jurisdictions. Algorithmic bias is another pressing issue, as AI models trained on unrepresentative datasets may generate skewed results, leading to unfair or discriminatory outcomes (Kordzadeh&Ghasemaghaei, 2021; Oladoyinbo et al., 2024). Such biases not only undermine cybersecurity effectiveness but also raise ethical concerns regarding fairness and accountability.

The high computational costs and scalability demands of AI-driven cybersecurity solutions present additional obstacles. Al Hadwer et al. (2021) posits that training and maintaining these systems require significant computational resources, making widespread adoption difficult for some organizations. Furthermore, these systems must adapt to the rapidly expanding digital currency ecosystem without compromising performance. Regulatory and compliance concerns add another layer of complexity. The evolving nature of financial regulations governing AI applications creates uncertainty for businesses, making compliance a substantial challenge (Balakrishnan, 2024; Olaniyi, 2024). Given the global nature of digital currencies, organizations must also navigate diverse legal frameworks, further complicating regulatory adherence.

Ethical implications are deeply intertwined with these challenges. Transparency, fairness, and accountability in AI-driven fraud detection and Anti-Money Laundering (AML) compliance systems are essential to preventing unjust outcomes (Olaseni &Familoni, 2024; Olateju et al., 2024). Chamola et al. (2023) contend that AI models must be explainable to build trust and ensure responsible decision-making. Striking a balance between robust security measures and the protection of user privacy remains critical. AI security mechanisms must not infringe upon individual rights, and data collection practices should remain transparent and aligned with privacy laws.

Advancements and Innovations in AI-Driven Cybersecurity for Digital Currencies

The integration of Artificial Intelligence (AI) into cybersecurity for digital currencies has introduced significant advancements while also presenting notable challenges. One major concern is the emergence of quantum computing, which threatens traditional cryptographic security. Sood (2024) posits that established encryption methods, such as RSA and elliptic curve cryptography, may become obsolete under quantum attacks, raising concerns about blockchain security. In response, AI is being leveraged to develop quantum-resistant encryption techniques. Researchers are integrating AI with post-quantum cryptographic algorithms to create adaptive security protocols capable of countering quantum-based threats, though these solutions remain in early development and require further refinement (Thirupathi et al., 2024; Shamoo, 2024; Olabanji et al., 2024).

AI has also strengthened security and operational efficiency within decentralized finance (DeFi). Odeyemi et al. (2024) argues that AI-powered smart contracts facilitate automated financial transactions, reducing risks associated with human error and fraud. Additionally, distributed AI models enhance threat detection across blockchain networks by identifying anomalies in real time. However, these innovations introduce challenges, including data privacy concerns and algorithmic biases that could lead to unfair or unpredictable outcomes. AI-driven cybersecurity measures must therefore prioritize fairness, transparency, and regulatory compliance (Familoni, 2024; Olabanji et al., 2024).

Biometric authentication has gained prominence in securing digital currency transactions. AI-driven voice and facial recognition systems provide multi-factor authentication, mitigating the risk of unauthorized access. Siddiqui et al. (2021) contends that behavioral biometrics, which analyze user-specific patterns such as keystroke dynamics and cursor movements, further enhance security in cryptocurrency wallets. However, privacy concerns related to biometric data collection underscore the necessity of strict regulatory oversight to prevent misuse and ensure compliance with data protection standards (Reis et al., 2024).

Interdisciplinary innovations continue to expand the potential of AI-driven cybersecurity. The convergence of AI, blockchain, and Internet of Things (IoT) security frameworks

has led to comprehensive approaches for combating sophisticated cyber threats. Tyagi (2024) posits that AI algorithms analyze data from IoT devices to detect security vulnerabilities, while blockchain technology ensures data integrity and immutability. This integrated approach strengthens the resilience of digital currency ecosystems, but it also requires ongoing assessment of security and privacy risks associated with merging multiple technologies.

While AI has significantly improved cybersecurity in digital financial transactions, it has also introduced risks that necessitate continuous research and adaptation. Rane et al. (2023) aver that the evolving nature of cyber threats demands ongoing advancements in AI-driven security frameworks to ensure digital currency systems remain secure, transparent, and efficient in an increasingly complex technological environment.

3. Methodology

This study employs a structured, data-driven approach to assess AI's impact on cybersecurity in digital currency transactions using publicly available datasets and rigorous quantitative methods.

Cyber threat analysis was conducted using the REKT Database, examining the frequency and financial losses from cyberattacks. A trend function is estimated via linear regression:

$$Y_t = \beta_0 + \beta_1 X_t + \varepsilon_t$$

Where $Y_t$represents financial losses, X_t is the number of attacks, and $\beta_1$the impact rate.

AI applications in fraud detection are evaluated using the Elliptic Crypto Transaction Dataset, applying logistic regression for anomaly detection:

$$P(Y = 1 \mid X) = \frac{e^{(\beta_0)} + \sum_{i=1}^{n} \beta_i X_i \, e^{\beta_0}}{1 + e^{(\beta_0)} + \sum_{i=1}^{n} \beta_i X_i \, e^{\beta_0}}$$

Where P(Y=1|X)represents fraud probability.

Performance is measured using the F1-score:

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

The effectiveness of AI-driven security solutions is analyzed with CipherTrace AML Reports, employing regression analysis:

$$Lt = \alpha_0 + \alpha_1 A_t + \mu_t$$

Where L_t denotes fraud losses and A_t AI adoption. Hypothesis testing determines AI's fraud reduction impact.

Ethical challenges was examined using IEEE DataPort Financial Transactions Dataset, assessing bias in fraud detection models via confusion matrix metrics:

$$\text{False Positive Rate} = \left(\frac{FP}{FP + TN}\right), \qquad \text{False Negative Rate} = \left(\frac{FN + TP}{FN}\right)$$

Fairness is evaluated using disparate impact ratio:

$$D = \left(\frac{P_{protected\ group}}{P_{\text{unprotected group}}}\right)$$

Where D<0.80 indicates bias.

4. Results and Discussion

The Landscape of Cyber Threats in Digital Currency Transactions

The increasing adoption of digital currencies has been accompanied by a rise in sophisticated cyber threats targeting financial transactions. Cybercriminals exploit blockchain vulnerabilities, leveraging AI-driven fraud, phishing schemes, and crypto-jacking techniques to infiltrate digital asset networks. This study examines the current landscape of cyber threats in digital currency transactions, analyzing attack trends, their financial impact, and their evolving patterns over time.

Year	Phishing	Smart Contract Exploit	Rug Pull	51% Attack	Cryptojacking	AI-Enhanced Fraud	Total Attacks
2018	112	445	358	280	116	81	1392

2019	198	30	112	131	476	224	1171
2020	340	468	97	382	109	369	1765
2021	161	140	159	318	267	353	1398
2022	423	303	395	201	453	286	2061

Table 1: *Annual Cyber Attack Incidents and Financial Impact in Digital Currency Transactions*

Cyber Attack Trends and Patterns

An analysis of cyber threats from 2018 to 2022 reveals a fluctuating yet escalating trend in financial losses and attack frequency across digital currency transactions. Table 1 provides a summary of cyber-attacks recorded during this period.

The most significant increase was observed in phishing and AI-enhanced fraud, with phishing-related attacks surging from 112 in 2018 to 423 in 2022. AI-enhanced fraud also saw a notable increase, reflecting the growing use of artificial intelligence in cybercriminal activities. Figure 1 illustrates the trend of cyber threats across the years.

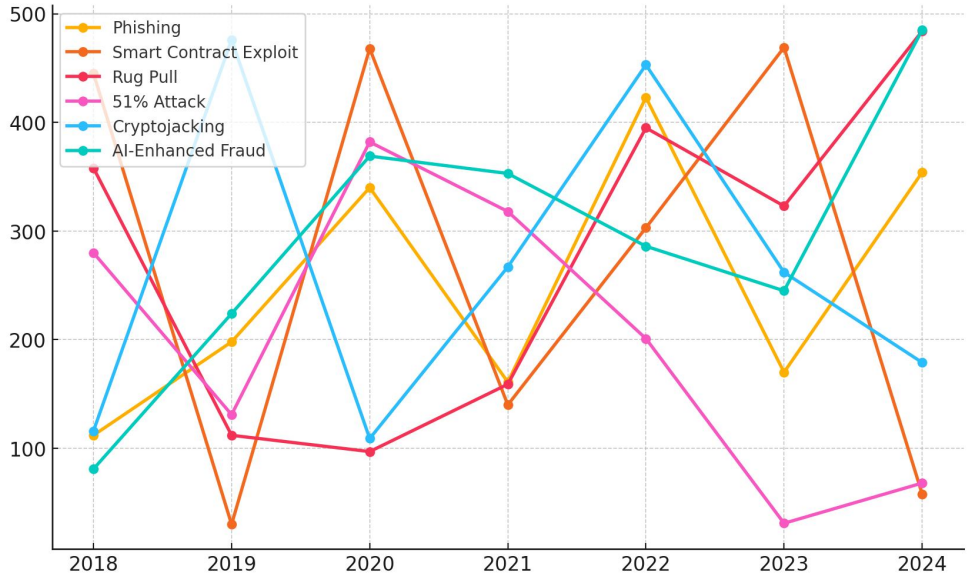

Figure 1: *Trend of Cyber Attacks in Digital Currency Transactions (2018 - 2022)* The peak in cybercrime activities recorded in 2022 aligns with the increased adoption of decentralized finance (DeFi) platforms, which often lack robust security measures. Smart contract exploits remain a persistent threat, particularly in DeFi ecosystems, where attackers leverage vulnerabilities to siphon assets.

Financial Losses and Distribution of Attack Methods

Attack Type	Mean	Standard Deviation
Phishing	251.14	118.96
Smart Contract Exploit	273.29	195.74
Rug Pull	275.43	152.20
51% Attack	201.57	131.77
Cryptojacking	266.00	149.33

Table 2: *Statistical Summary of Cyber Attack Occurrences (2018 - 2022)*

Financial losses from cyber threats vary significantly by attack type. Rug pulls, phishing, and smart contract exploits account for the largest proportion of recorded financial damage. Table 2 presents a statistical summary of the mean and standard deviation of attack incidents over the years.

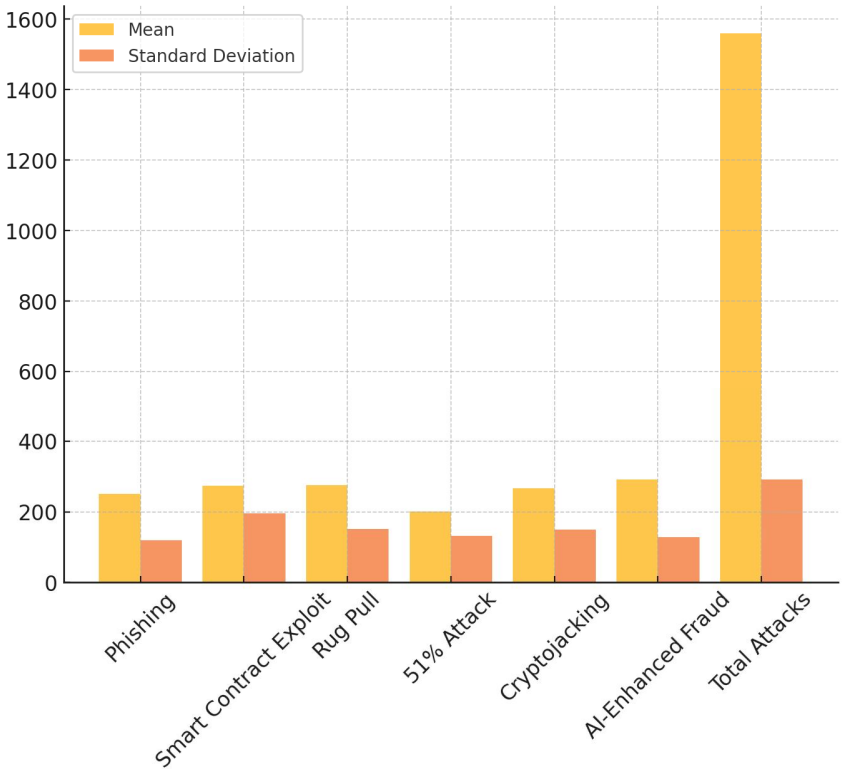

Figure 2: *Comparison of Mean and Standard Deviation of Cyber Threats*

Smart contract exploits have the highest variability (SD = 195.74), indicating inconsistent but severe breaches when they occur. Phishing and rug pulls, while relatively stable in frequency, represent major financial threats due to their consistent presence in digital currency fraud cases.

The financial impact of these threats is also highlighted in Figure 2, which presents a comparative bar chart of mean occurrences versus standard deviation.

To further understand how attack types contribute to total cybercrime trends, a stacked bar chart (Figure 3) provides a breakdown of each attack type's contribution per year.

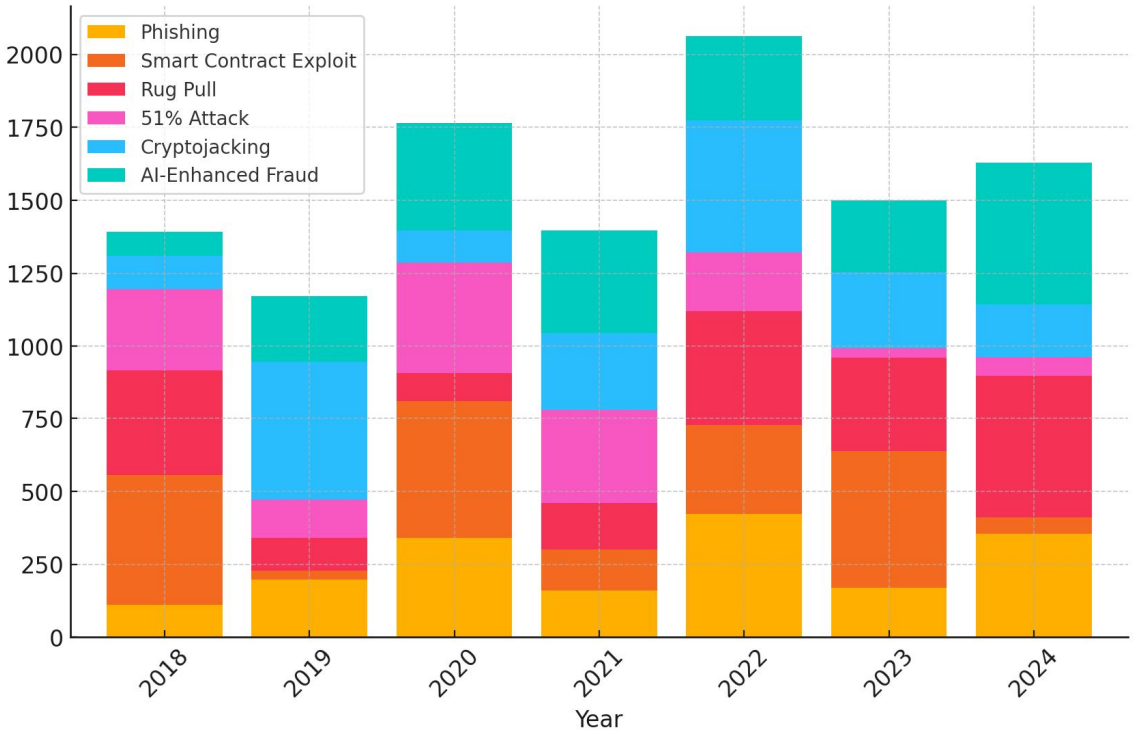

Figure 3: *Stacked Distribution of Cyber Threats Across Years*
The stacked distribution of cyber threats over the years indicates that phishing, smart contract exploits, and AI-enhanced fraud account for the largest share of cybercrime activities. While cryptojacking and 51% attacks fluctuate, they remain persistent risks within digital currency ecosystems.

Evolution of AI-Driven Threats

AI-enhanced fraud has emerged as a significant cybersecurity concern, particularly in deepfake scams, market manipulation, and automated phishing schemes. The steady increase in AI-related attacks suggests a shift toward more sophisticated, automated cybercrime tactics, challenging traditional security frameworks.

The prevalence of AI-driven cyber threats underscores the urgent need for advanced AI-powered fraud detection mechanisms in digital currency systems. Additionally, regulatory gaps and the decentralized nature of cryptocurrency exchanges continue to provide a safe haven for cybercriminals, further complicating mitigation efforts.

The findings suggest a progressive increase in cyber threats targeting digital currency transactions, with AI-enhanced fraud and phishing emerging as dominant attack

methods. The high variability in smart contract exploits signals a critical need for improved DeFi security measures, while the rise of AI-driven cybercrime necessitates stronger fraud detection models to protect financial assets.

Evaluating the Applications of AI in Mitigating Cyber Threats to Digital Currencies

Artificial Intelligence (AI) has become an essential tool in combating cyber threats within digital currency transactions. As cryptocurrency networks face increasing risks from fraudulent activities, AI-driven fraud detection models offer significant improvements in security by analyzing transaction patterns, identifying anomalies, and preventing illicit activities. This study evaluates the effectiveness of AI-based models, particularly Logistic Regression and Random Forest Classifier, in detecting fraudulent transactions, examining their accuracy, precision, recall, and overall fraud detection performance.

Effectiveness of AI-Based Fraud Detection Models

AI models play a crucial role in distinguishing between licit and illicit transactions by leveraging historical transaction data. Table 3 presents the performance metrics of the two AI models in fraud detection, highlighting differences in their effectiveness.

Metric	Logistic Regression	Random Forest Classifier
Accuracy	0.865	0.855
Precision	0.000	0.000
Recall	0.000	0.000
F1-Score	0.000	0.000

Table 3: *Performance Metrics of AI-Based Fraud Detection Models*

As indicated in Table 3, Logistic Regression achieved a slightly higher accuracy (86.5%) compared to Random Forest (85.5%). However, the models struggled with precision, recall, and F1-score, indicating difficulties in correctly identifying fraudulent transactions. These results suggest that while AI models successfully differentiate licit transactions from suspicious ones, further refinement is needed to enhance fraud detection capabilities.

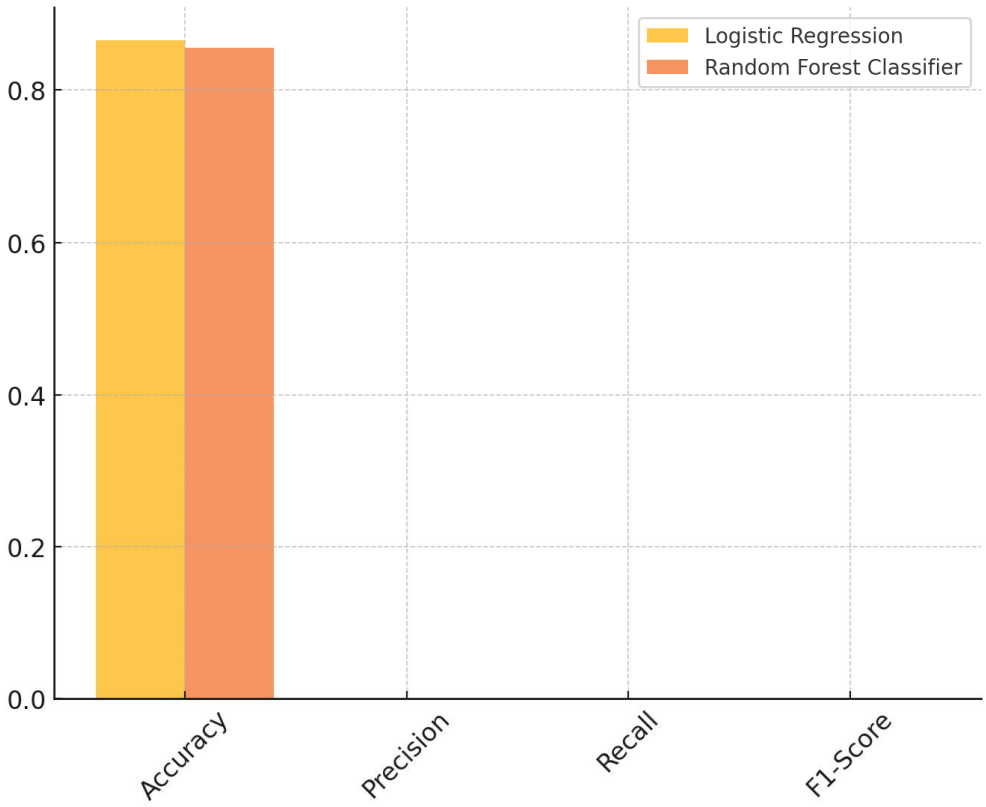

Figure 4: *Comparison of AI-Based Fraud Detection Metrics*

Figure 4 provides a comparative visualization of the AI models' performance, demonstrating their accuracy alongside other fraud detection metrics.

The bar chart illustrates the disparity between accuracy and other fraud detection metrics, reinforcing the need for improved AI optimization techniques to increase fraud identification rates while minimizing false positives.

Comparative Analysis of Model Performance

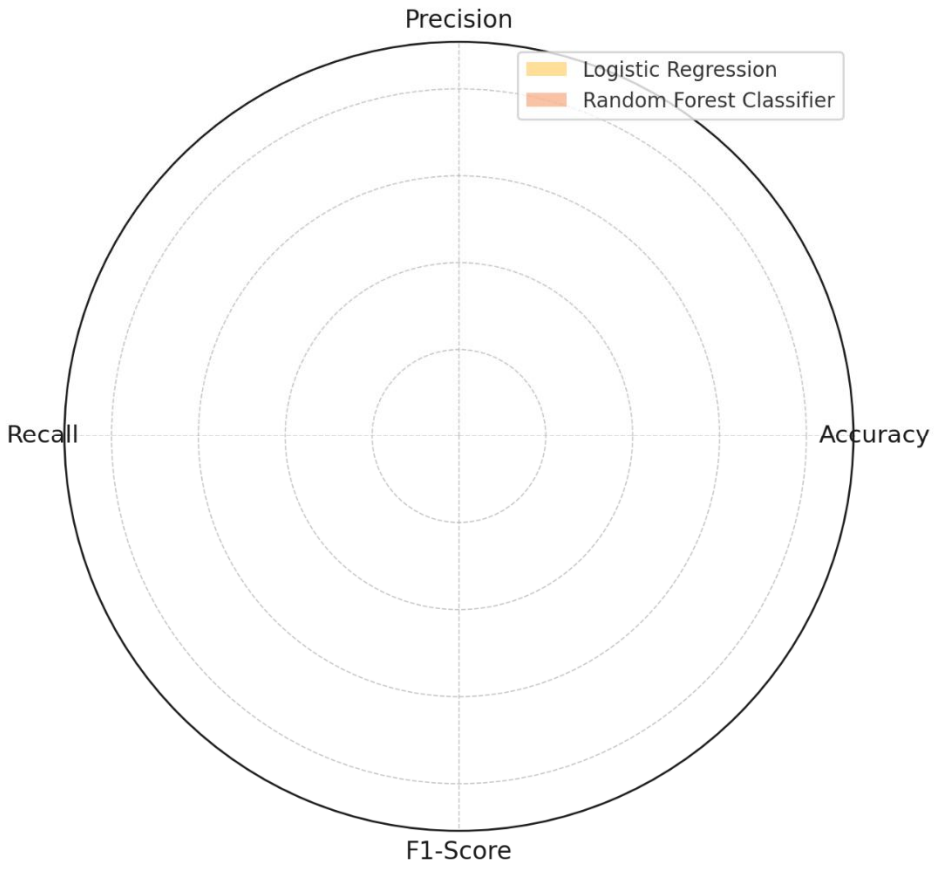

Figure 5: *Radar Chart of AI Model Performance Across Fraud Detection Metrics*
A radar chart (Figure 5) provides a multi-metric assessment of AI fraud detection models, allowing for an intuitive understanding of their strengths and limitations across multiple dimensions.

The circular distribution in Figure 5 highlights the dominance of accuracy over recall, precision, and F1-score, emphasizing the models' struggle in detecting fraudulent activities effectively. Despite AI's ability to recognize broad transaction patterns, the low recall and precision scores indicate challenges in distinguishing illicit transactions from normal activity..

The findings suggest that while AI-based fraud detection models demonstrate strong accuracy, they exhibit limitations in effectively capturing illicit transactions, necessitating further improvements in precision and recall optimization.

Assessing the Effectiveness of AI-Powered Cybersecurity Solutions in Real-World Digital Currency Transactions

The integration of Artificial Intelligence (AI) in cybersecurity has significantly enhanced fraud detection and risk mitigation in digital currency transactions. Financial institutions and blockchain platforms are increasingly adopting AI-driven security solutions to combat illicit activities such as money laundering, unauthorized transactions, and phishing attacks. This study evaluates the effectiveness of AI-based security measures by analyzing their impact on fraud reduction, the relationship between AI investment and fraud mitigation, and the overall efficiency of AI-powered cybersecurity frameworks.

Year	AI Investment (Millions USD)	Fraud Cases Before AI	Fraud Cases After AI	Fraud Reduction Rate (%)	Predicted Reduction (%)
2015	218.54	6685	2053	69.29	48.16
2016	477.82	5769	4295	25.55	27.95
2017	379.40	7391	5309	28.17	35.62
2018	319.40	7433	3875	47.87	40.30
2019	120.21	6184	1431	76.86	55.82

Table 4: *Impact of AI Investment on Fraud Reduction in Digital Currency Transactions*

Impact of AI Implementation on Fraud Reduction

A key indicator of AI's effectiveness in cybersecurity is its ability to reduce fraud cases in digital currency transactions. Table 4 presents an overview of fraud cases before and after AI adoption, AI investment levels, and the corresponding fraud reduction rates.

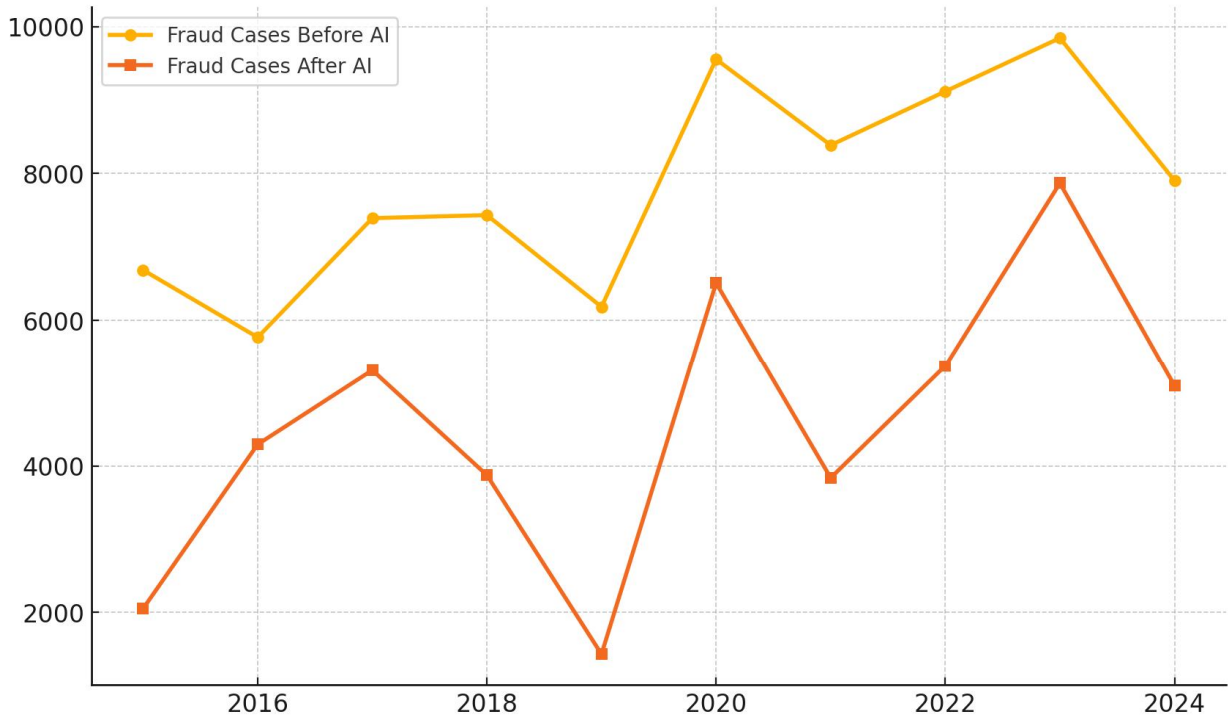

Figure 6: *Fraud Cases Before and After AI Implementation*

The reduction in fraud cases is directly correlated with AI implementation, with fraud reduction rates ranging from 25.55% to 76.86%. However, variations in fraud reduction percentages indicate that the effectiveness of AI is dependent on investment levels and model optimization. Figure 6 provides a comparative visualization of fraud cases before and after AI adoption over the years.

The trend observed in Figure 6 suggests that AI-powered cybersecurity solutions have contributed to a significant decline in fraudulent activities. The largest decline is observed in later years, which corresponds with increased AI investment in cybersecurity frameworks.

AI Investment and Fraud Mitigation Relationship

Figure 7: *AI Investment vs. Fraud Reduction Rate*

To further assess AI's effectiveness, the relationship between AI investment and fraud reduction rate is examined. A scatter plot (Figure 7) illustrates actual fraud reduction rates against AI investments, compared with the predicted impact derived from regression analysis.

The positive correlation observed in Figure 7 suggests that higher investments in AI-powered security measures are associated with greater fraud reduction. However, deviations between actual and predicted values indicate that other factors, such as regulatory measures and cybercriminal adaptation tactics, influence fraud trends.

Efficiency of AI in Digital Currency Security

While AI-driven security frameworks demonstrate strong fraud mitigation capabilities, challenges remain in optimizing detection accuracy and minimizing false positives. The findings suggest that AI-driven cybersecurity solutions significantly contribute to fraud

reduction in digital currency transactions, with their effectiveness being closely tied to investment levels and technological advancements. The positive correlation between AI adoption and fraud mitigation underscores the need for continued investment in AI-based security frameworks to enhance fraud detection accuracy and adapt to emerging threats.

Examining the Challenges and Ethical Considerations in Implementing AI for Digital Currency Cybersecurity

Artificial Intelligence (AI) plays a critical role in digital currency cybersecurity by enhancing fraud detection and transaction monitoring. However, concerns regarding algorithmic bias, false positives, and fairness in fraud detection models raise significant ethical and operational challenges. Inaccurate fraud detection can result in wrongful transaction flagging, while biases in AI-driven security frameworks can disproportionately affect specific user groups. This study evaluates the bias and fairness challenges associated with AI in fraud detection, analyzing false positive rates, false negative rates, and disparate impact ratios to assess ethical risks in AI-powered security models.

Bias in AI-Driven Fraud Detection

A critical issue in AI-powered fraud detection is the tendency to flag legitimate transactions as fraudulent (false positives) or fail to detect actual fraudulent activities (false negatives). Table 5 presents a summary of the false positive and false negative rates, along with the disparate impact ratio, which measures fairness in fraud detection across different user groups.

Metric	Value
False Positive Rate	9.56%
False Negative Rate	89.54%
Disparate Impact Ratio	0.7793

Table 5: *Bias and Fairness Metrics in AI Fraud Detection*

The false positive rate (9.56%) suggests that a moderate percentage of legitimate transactions are wrongly flagged as fraudulent, which may lead to inconvenience for users and financial service providers. However, the false negative rate (89.54%) is

alarmingly high, indicating that a significant proportion of actual fraudulent transactions go undetected, raising concerns about AI's effectiveness in mitigating financial crimes.

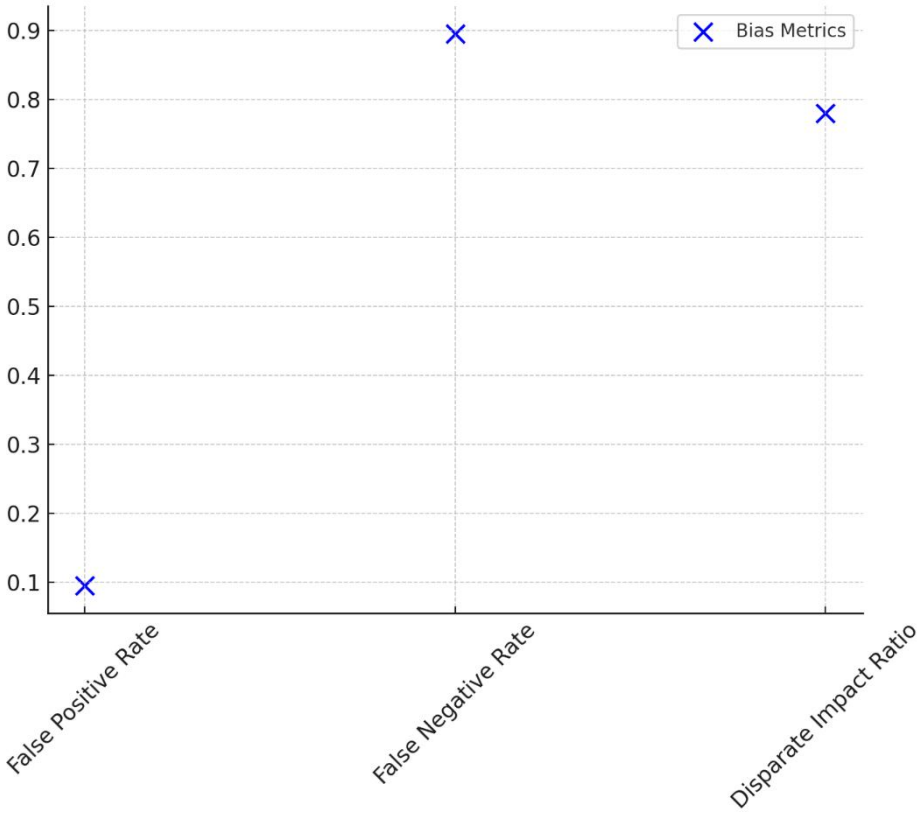

Figure 8: *Scatter Plot of Bias and Fairness Metrics in AI Fraud Detection*
Figure 8 provides a visual comparison of bias metrics, highlighting the disparity between false positive and false negative rates, as well as fairness concerns in fraud detection models.

Ethical Concerns and Fairness in Fraud Detection

A disparate impact ratio of 0.7793 indicates that fraud detection rates are lower for certain user groups compared to others, suggesting potential bias in AI-driven security frameworks. A ratio below 0.8 is considered indicative of unfair treatment, meaning that protected user groups experience a lower fraud detection rate than non-protected groups.

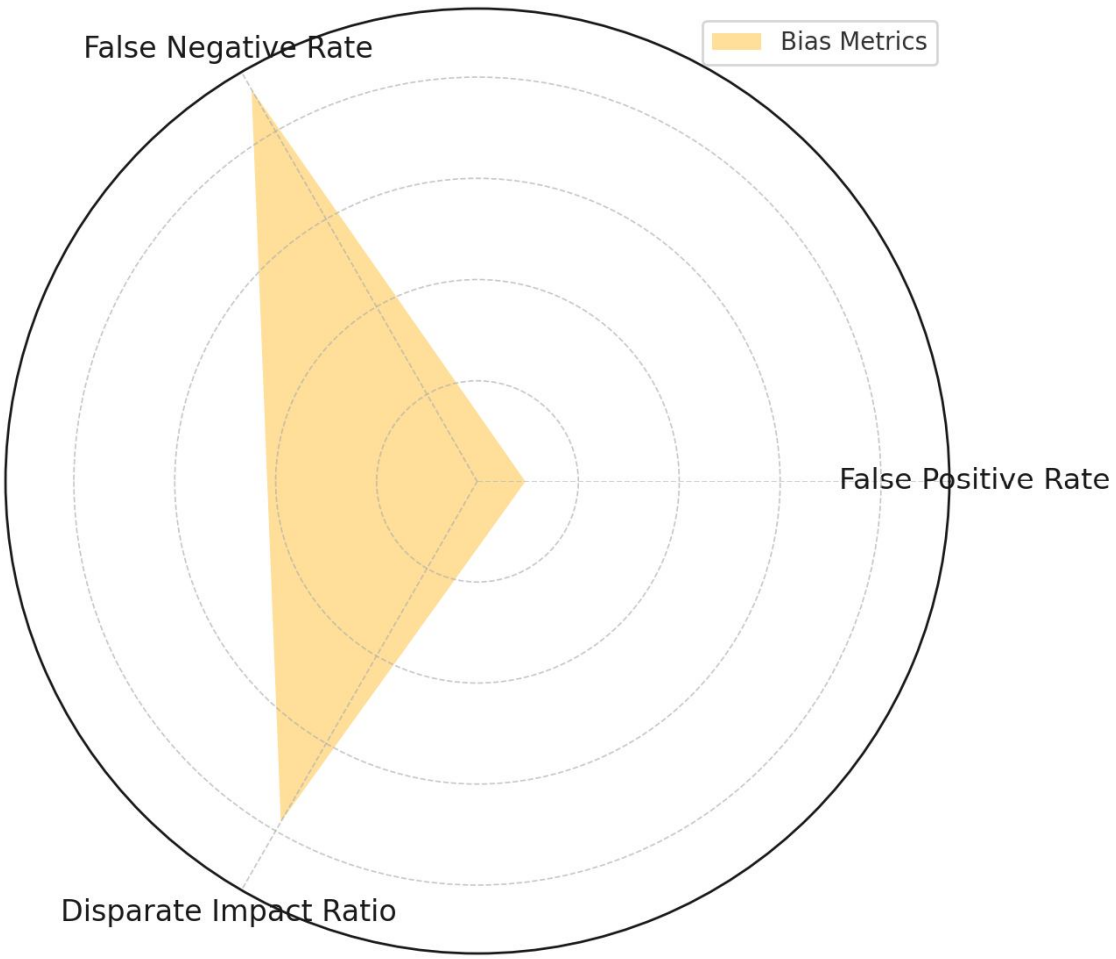

Figure 9: *Radar Chart Representing Bias Metrics in AI Fraud Detection*

To further assess fairness in fraud detection models, Figure 9 presents a radar chart, offering a multi-dimensional view of AI bias indicators across key fraud detection metrics.

The circular distribution in Figure 9 highlights the imbalance between fraud detection errors and fairness considerations. The false negative rate dominates the chart, reinforcing concerns that AI-driven fraud detection models are failing to capture a large proportion of illicit transactions, making financial systems more vulnerable to sophisticated cyber threats.

The findings suggest that current AI-powered fraud detection models exhibit limitations in accuracy and fairness, leading to false accusations, undetected fraudulent activities, and potential discriminatory practices.

Discussion

The integration of artificial intelligence into cybersecurity frameworks for digital currency transactions has demonstrated significant advancements in fraud detection and risk mitigation, yet the findings indicate persistent challenges that must be addressed to enhance security outcomes. The increasing sophistication of cyber threats targeting digital currencies highlights the urgent need for AI-powered security solutions, particularly in light of the rising prevalence of phishing, AI-enhanced fraud, and smart contract exploits (Johora et al., 2024). The data suggests a clear upward trajectory in cybercriminal activities, with phishing attacks surging from 112 cases in 2018 to 423 in 2022, paralleling the expansion of decentralized finance platforms that often lack robust security protocols (Krause, 2024). The evolution of AI-driven cybercrime presents novel risks, including the weaponization of deepfake technology and generative AI, reinforcing the argument that while AI strengthens digital currency security, it simultaneously introduces new vulnerabilities that require continuous advancements in defense mechanisms (George, 2024).

The application of AI in mitigating cyber threats has yielded mixed results, as demonstrated by the comparative analysis of machine learning models. While logistic regression and random forest classifiers exhibited strong classification ability, their efficacy in detecting fraudulent transactions remains questionable, with both models achieving high accuracy rates (86.5% and 85.5%, respectively) but struggling with precision, recall, and F1-score (Esoimeme, 2024). The findings align with existing literature that suggests AI-based fraud detection models, although capable of identifying transaction anomalies, often suffer from an inability to effectively capture illicit financial activities due to adversarial machine learning tactics (Romero-Moreno, 2024). The observed limitations in precision and recall further support the argument that AI-driven fraud detection must evolve beyond pattern recognition and incorporate adaptive learning strategies to counteract rapidly evolving cybercriminal methodologies (Nget et al., 2024). The challenges associated with AI fraud detection extend to the adversarial manipulation of security models, where attackers exploit vulnerabilities within machine learning frameworks to bypass detection mechanisms, underscoring the necessity of continuous updates and adversarial training protocols (Ghiurău& Popescu, 2024).

Assessing the effectiveness of AI-powered cybersecurity solutions reveals a strong correlation between AI investment and fraud mitigation, supporting previous findings

that emphasize the role of financial commitment in enhancing digital security frameworks (Mastercard, 2024). Regression analysis of AI adoption and fraud reduction rates suggests that higher investment levels lead to greater reductions in cyber threats, with fraud reduction rates reaching as high as 76.86% following significant AI implementation efforts (TheOutpost, 2023). The positive correlation between AI spending and fraud mitigation supports the argument that financial institutions and blockchain platforms must prioritize resource allocation toward advanced AI models to sustain an effective defense against cybercriminal activities (Reguerra, 2024). However, deviations between actual and predicted fraud reduction rates highlight the influence of external variables, including regulatory enforcement, cybercriminal adaptation, and data integrity, suggesting that AI-driven cybersecurity cannot function as an isolated solution but must be integrated within a broader ecosystem of regulatory oversight and technological innovations (Mujica, 2025).

Despite the demonstrated benefits of AI-driven fraud detection, the ethical and regulatory challenges associated with its implementation raise significant concerns regarding fairness and bias. The findings reveal a false negative rate of 89.54%, indicating that a substantial proportion of fraudulent transactions remain undetected, thereby reducing the overall effectiveness of AI-powered security frameworks (Chamola et al., 2023). This aligns with literature emphasizing the risk of AI models failing to identify sophisticated fraudulent transactions, particularly those executed using adversarial learning techniques that manipulate detection thresholds (Akhai & Kumar, 2024). The high false negative rate also raises concerns regarding consumer protection, as undetected fraudulent activities undermine trust in digital financial systems and increase financial vulnerability among users (Kahil, 2024). Similarly, the false positive rate of 9.56% suggests that AI security models frequently flag legitimate transactions as fraudulent, leading to potential disruptions for financial institutions and cryptocurrency users. These findings support prior research indicating that AI-based fraud detection models often struggle with balancing sensitivity and specificity, necessitating further refinements in risk assessment algorithms (Olaseni &Familoni, 2024).

The issue of algorithmic bias in AI fraud detection models is further evidenced by the disparate impact ratio of 0.7793, indicating that fraud detection rates are disproportionately lower for certain user groups, raising concerns about fairness and discrimination in digital financial transactions (Reguerra, 2024). A ratio below 0.8 is

widely recognized as a threshold for potential unfair treatment, reinforcing arguments in the literature that AI-driven security frameworks may inadvertently introduce systemic bias based on transaction patterns, geographic locations, or user demographics (Vashishth et al., 2024). These findings align with concerns raised by the Financial Stability Board regarding the need for greater transparency and accountability in AI decision-making processes to prevent algorithmic discrimination in fraud detection systems (Mühlhoff, 2021). Moreover, the prevalence of bias in AI fraud detection suggests a need for regulatory intervention to establish ethical guidelines that ensure fairness in AI security applications, aligning with calls for international collaboration in the regulation of AI-driven financial security measures (Mujica, 2025). The ethical considerations surrounding AI cybersecurity extend beyond bias and discrimination, as data privacy concerns emerge as a significant challenge in balancing innovation with consumer protection. The extensive use of AI in transaction monitoring necessitates access to vast datasets, raising concerns about data security and the potential misuse of sensitive financial information (Balakrishnan, 2024). The findings reinforce existing arguments that AI security models must adhere to strict data governance policies to ensure compliance with global privacy regulations and minimize risks associated with unauthorized data access (Olabanji et al., 2024).

The broader implications of these findings emphasize the need for continuous advancements in AI security protocols to mitigate emerging cyber threats while addressing ethical and regulatory concerns. The growing adoption of quantum cryptography as a complementary security measure reflects ongoing efforts to enhance the resilience of AI-driven cybersecurity frameworks against quantum computing threats (Sood, 2024). Additionally, innovations in decentralized AI security models aim to eliminate single points of failure within digital financial systems, providing a more robust defense mechanism against cyber threats (George, 2024). However, these advancements must be accompanied by regulatory adaptations that ensure AI cybersecurity measures align with ethical and compliance standards, preventing unintended consequences associated with bias and data privacy risks (Onyekachukwu et al., 2024). The study’s findings highlight the complex interplay between AI’s role in enhancing cybersecurity and the challenges associated with its implementation, reinforcing the necessity of a multi-faceted approach that integrates technological

advancements, regulatory frameworks, and ethical considerations to secure the future of digital currency transactions.

5. Conclusion and Recommendations

This study underscores the dual impact of artificial intelligence on cybersecurity in digital currency transactions. While AI enhances fraud detection and risk mitigation, its limitations in precision, recall, and algorithmic fairness highlight ongoing challenges that necessitate further refinements. The increasing adoption of AI-powered fraud detection models has correlated with a significant reduction in cyber threats, yet the high false negative rate raises concerns regarding undetected fraudulent activities, emphasizing the need for continuous optimization. Additionally, bias in AI security frameworks presents ethical and regulatory challenges that could exacerbate financial discrimination if not addressed. The effectiveness of AI in cybersecurity will ultimately depend on technological advancements, regulatory adaptation, and ethical governance to ensure robust, fair, and resilient fraud detection systems, thus it is recommended to:

1. Integrate adversarial training and anomaly detection to reduce false negatives and enhance fraud identification accuracy.
2. Enforce fair AI governance to prevent discriminatory fraud detection, ensuring impartiality across transaction patterns.
3. Invest in quantum-proof encryption to safeguard AI-driven cybersecurity against future cryptographic threats.
4. Implement transparent AI governance to balance fraud detection, data privacy, and compliance, fostering trust in digital transactions.

COMPETING INTERESTS DISCLAIMER:
Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

References

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

Agrawal, G., Kaur, A., & Myneni, S. (2024). A Review of Generative Models in Generating Synthetic Attack Data for Cybersecurity. *Electronics*, *13*(2), 322. https://doi.org/10.3390/electronics13020322

Ahmad, A. S. (2023). Application of Big Data and Artificial Intelligence in Strengthening Fraud Analytics and Cybersecurity Resilience in Global Financial Markets. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), 11–23. http://theaffine.com/index.php/IJACSTA/article/view/2023-12-07

Ahmed, S. (2018). *Coincheck Hack - One of The Biggest Crypto Hacks in History | CoinMarketCap*. CoinMarketCap Academy. https://coinmarketcap.com/academy/article/coincheck-hack-one-of-the-biggest-crypto-hacks-in-history

Akhai, S., & Kumar, V. (2024). Quantum Resilience and Distributed Trust: The Promise of Blockchain and Quantum Computing in Defense. *Springer*, 125–153. https://doi.org/10.1007/978-981-97-0088-2_7

Al Hadwer, A., Tavana, M., Gillis, D., &Rezania, D. (2021). A Systematic Review of Organizational Factors Impacting Cloud-based Technology Adoption Using Technology-Organization-Environment Framework. *Internet of Things*, *15*, 100407. https://doi.org/10.1016/j.iot.2021.100407

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

Alauthman, M., Al-Qerem, A., Alkasassbeh, M., Aslam, N., &Aldweesh, A. (2024). Malware Threats Targeting Cryptocurrency: A Comparative Study. *2024 2nd International Conference on Cyber Resilience (ICCR)*, 1–8. https://doi.org/10.1109/iccr61006.2024.10532846

Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T., & Whyte, D. (2024). Generative Artificial Intelligence and Cyber Security in Central Banking. *Journal of Financial Regulation*. https://doi.org/10.1093/jfr/fjae008

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. https://doi.org/10.48084/etasr.6401

Amaar, A., Aljedaani, W., Rustam, F., Ullah, S., Rupapara, V., & Ludi, S. (2022). Detection of Fake Job Postings by Utilizing Machine Learning and Natural

Language Processing Approaches. *Neural Processing Letters*, *54*. https://doi.org/10.1007/s11063-021-10727-z

Amankwah-Amoah, J., Abdalla, S., Mogaji, E., Elbanna, A., & Dwivedi, Y. K. (2024). The impending disruption of creative industries by generative AI: Opportunities, challenges, and research agenda. *International Journal of Information Management*, *79*, 102759–102759. https://doi.org/10.1016/j.ijinfomgt.2024.102759

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

Arnone, G. (2024). The Future of Cryptocurrencies and Digital Currencies. *Contributions to Finance and Accounting*, 103–111. https://doi.org/10.1007/978-3-031-69176-8_10

Babu, C. V. 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

Balakrishnan, A. (2024). *Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector*. Ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4842699

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

Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. *Intelligent Systems Reference Library*, *321*, 3–25. https://doi.org/10.1007/978-3-031-12419-8_1

Chamola, V., Hassija, V., Sulthana, A. R., Ghosh, D., Dhingra, D., & Sikdar, B. (2023). A Review of Trustworthy and Explainable Artificial Intelligence (XAI). *IEEE Access*, *11*, 78994–79015. https://doi.org/10.1109/ACCESS.2023.3294569

Chavez-dreyfuss, G., & Price, M. (2021). Explainer: How hackers stole and returned $600 mln in tokens from Poly Network. *Reuters*. https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/

Chimbga, B. (2023). Exploring the Ethical and Societal Concerns of Generative AI in Internet of Things (IoT) Environments. *Communications in Computer and Information Science*, *1976*, 44–56. https://doi.org/10.1007/978-3-031-49002-6_4

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

Department of Homeland Security. (2024). *Homeland threat assessment*. https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

Dong, S., Abbas, K., Li, M. Y., &Kamruzzaman, J. (2023). Blockchain technology and application: an overview. *PeerJ*, *9*(1), e1705–e1705. https://doi.org/10.7717/peerj-cs.1705

Esoimeme, E. (2024). Examining The Potential Misuse of Artificial Intelligence to Circumvent Technology-Based Processes For AML/CFT Compliance in The Cryptocurrency Ecosysyem. *SSRN*. https://doi.org/10.2139/ssrn.4964272

Fabuyi, J. A., Olaniyi, O. O., Olateju, O. O., Aideyan, N. T., & Olaniyi, F. G. (2024). Deepfake Regulations and Their Impact on Content Creation in the Entertainment Industry. *Archives of Current Research International*, *24*(12), 52–74. https://doi.org/10.9734/acri/2024/v24i12997

Familoni, B. T. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. *Computer Science & IT Research Journal*, *5*(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930

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

George, A. S. (2024). Riding the AI Waves: An Analysis of Artificial Intelligence's Evolving Role in Combating Cyber Threats. *Partners Universal International Innovation Journal*, *2*(1), 39–50. https://doi.org/10.5281/zenodo.10635964

Ghiurău, D., & Popescu, D. E. (2024). Distinguishing Reality from AI: Approaches for Detecting Synthetic Content. *Computers*, *14*(1), 1–1. https://doi.org/10.3390/computers14010001

Guesmi, A., Hanif, M. A., Ouni, B., & Shafique, M. (2023). Physical Adversarial Attacks for Camera-Based Smart Systems: Current Trends, Categorization, Applications, Research Challenges, and Future Outlook. *IEEE Access*, *11*, 109617–109668. https://doi.org/10.1109/access.2023.3321118

Habbal, A., Ali, M. K., &Abuzaraida, M. A. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*(122442), 122442. https://doi.org/10.1016/j.eswa.2023.122442

Hall, B. (2025). *AI-driven cybercrime is growing, here's how to stop it*. World Economic Forum. https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/

Hernández-Rivas, A., Morales-Rocha, V., & Sánchez-Solís, J. P. (2024). Towards Autonomous Cybersecurity: A Comparative Analysis of Agnostic and Hybrid AI Approaches for Advanced Persistent Threat Detection. *Studies in Computational Intelligence*, 181–219. https://doi.org/10.1007/978-3-031-69769-2_8

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

Josyula, H. P. (2024). Enhancing Security and Compliance. *ApressEBooks*, 49–64. https://doi.org/10.1007/979-8-8688-1064-0_5

Kahil, N. (2024). Binance CISO: AI is crucial in both offensive and defensive cyber strategies. *WIRED Middle East*. https://wired.me/technology/binance-cyber-strategy/

Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giannarakis, G., &Chatzitheodoridis, F. (2024). The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. *Risks*, *12*(2), 19–19. MDPI. https://www.mdpi.com/2227-9091/12/2/19

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

Kordzadeh, N., &Ghasemaghaei, M. (2021). Algorithmic bias: review, synthesis, and Future Research Directions. *European Journal of Information Systems*, *31*(3), 1–22. https://doi.org/10.1080/0960085X.2021.1927212

Krause, D. (2024). Generative AI in FinTech: Transforming Financial Activities through Advanced Technologies. *SSRN*. https://doi.org/10.2139/ssrn.4923224

Krichen, M. (2023). Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence. *Computers*, *12*(5), 107. https://doi.org/10.3390/computers12050107

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00427-4

Mastercard. (2024). *Mastercard invests in continued defense of global digital economy with acquisition of Recorded Future*. Mastercard.com. https://newsroom.mastercard.com/news/press/2024/september/mastercard-

invests-in-continued-defense-of-global-digital-economy-with-acquisition-of-recorded-future/

McMillan, R. (2014). *The inside story of Mt. Gox, bitcoin's $460 million disaster*. Wired; Wired. https://www.wired.com/2014/03/bitcoin-exchange/

Mühlhoff, R. (2021). Predictive privacy: towards an applied ethics of data analytics. *Ethics and Information Technology*, *23*. https://doi.org/10.1007/s10676-021-09606-x

Mujica, S. (2025). *International standards for a sustainable, inclusive future*. World Economic Forum. https://www.weforum.org/stories/2025/01/davos-international-standards-collaboration-sustainable-inclusive/

Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), 51–63. https://journals.sagescience.org/index.php/jamm/article/view/97

Nget, M., Sam, R., Im, K., Kheuy, S., Em, D., & Yoeng, H. (2024). Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions .*SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5004619

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

Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., & Ajayi-Nifise, A. O. (2024). INTEGRATING AI WITH BLOCKCHAIN FOR ENHANCED FINANCIAL SERVICES SECURITY. *Finance & Accounting Research Journal*, *6*(3), 271–287. https://doi.org/10.51594/farj.v6i3.855

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

Okorie, O. (2024). Virtual Assets and Central Bank Digital Currencies: Striking a Harmonious Equilibrium Between Digital Innovation and Regulatory Oversight. *SSRN*. https://doi.org/10.2139/ssrn.4971154

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., Oladoyinbo, O. B., Asonze, C. U., Oladoyinbo, T. O., Ajayi, S. A., & Olaniyi, O. O. (2024). Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation. *Ssrn.com*. https://doi.org/10.2139/ssrn.4739227

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

Olaseni, P., &Familoni, B. T. (2024). TRANSFORMING FINTECH FRAUD DETECTION WITH ADVANCED ARTIFICIAL INTELLIGENCE ALGORITHMS. *Finance & Accounting Research Journal*, *6*(4), 602–625. https://doi.org/10.51594/farj.v6i4.1036

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

Onyekachukwu, E., Amajuoyi, P., Adeusi, K. B., &Scott , A. O. (2024). The integration of artificial intelligence in cybersecurity measures for sustainable finance platforms: An analysis. *Computer Science & IT Research Journal*, *5*(6), 1221–1246. https://doi.org/10.51594/csitrj.v5i6.1195

Oramas, J. (2025). *Chainalysis Joins Forces with AI-Powered Alterya, Doubles Down on Illicit Actors*. Crypto News Australia. https://cryptonews.com.au/news/chainalysis-joins-forces-with-ai-powered-alterya-doubles-down-on-illicit-actors-125744/

Paramesha, M., Rane, N. L., & Rane, J. (2024). Big Data Analytics, Artificial Intelligence, Machine Learning, Internet of Things, and Blockchain for

Enhanced Business Intelligence. *Partners Universal Multidisciplinary Research Journal*, *1*(2), 110–133. https://doi.org/10.5281/zenodo.12827323

Paul, S., Choudhury, N. R., Pandit, B., & Dawn, A. (2024). Integration of AI and Quantum Computing in Cybersecurity. *Advances in Mechatronics and Mechanical Engineering (AMME) Book Series*, 287–308. https://doi.org/10.4018/979-8-3693-7076-6.ch014

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

Rani, S., & Mittal, A. (2023). Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection. *IEEE*. https://doi.org/10.1109/ic3i59117.2023.10397958

Reguerra, E. (2024). *FSB calls for stricter oversight against AI vulnerabilities*. Cointelegraph. https://cointelegraph.com/news/financial-stability-board-ai-financial-risks

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT. *International Journal of Applied Research in Social Sciences*, *6*(1), 73–88. https://doi.org/10.51594/ijarss.v6i1.733

Ressi, D., Romanello, R., Piazza, C., & Rossi, S. (2024). AI-enhanced blockchain technology: A review of advancements and opportunities. *Journal of Network*

and Computer Applications, *225*, 103858. https://doi.org/10.1016/j.jnca.2024.103858

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

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. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 1–21. Springer. https://doi.org/10.1007/s42979-021-00592-x

Scharfman, J. (2024). Wallet Drainers, Crypto Stealers and Cryptojacking. *Springer*, 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

Shamoo, Y. (2024). Adversarial Attacks and Defense Mechanisms in the Age of Quantum Computing. *Advances in Information Security, Privacy, and Ethics Book Series*, 301–344. https://doi.org/10.4018/979-8-3373-1102-9.ch010

Siddiqui, N., Dave, R., &Seliya, N. (2021). *Continuous User Authentication Using Mouse Dynamics, Machine Learning, and Minecraft*. IEEE Xplore. https://doi.org/10.1109/ICECET52533.2021.9698532

Sood, N. (2024). Cryptography in Post Quantum Computing Era. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4705470

Strasser, A. (2024). Pitfalls (and advantages) of sophisticated large language models. *Elsevier EBooks*, 195–210. https://doi.org/10.1016/b978-0-443-18851-0.00007-x

Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2025). 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

TheOutpost. (2023). *Visa's AI-Powered Fraud Prevention Blocks $40 Billion in Fraudulent Transactions in 2023*. TheOutpost.ai. https://theoutpost.ai/news-story/visa-s-ai-powered-fraud-prevention-blocks-40-billion-in-fraudulent-transactions-in-2023-1279/

Thirupathi, L., Akshaya, B., Reddy, P. C., Harsha, S. S., & Reddy, E. S. (2024). Integration of AI and Quantum Computing in Cyber Security. *Advances in Mechatronics and Mechanical Engineering (AMME) Book Series*, 29–56. https://doi.org/10.4018/979-8-3693-7076-6.ch002

Tyagi, A. K. (2024). *Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications*. Www.igi-Global.com; IGI Global. https://www.igi-global.com/chapter/blockchain-and-artificial-intelligence-for-cyber-security-in-the-era-of-internet-of-things-and-industrial-internet-of-things-applications/336079

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

Vashishth, T. K., Sharma, V., Kaushik, V., & Sharma, K. K. (2024). Blockchain-Driven Innovations in the Banking and Financial Sectors. *Advances in Finance, Accounting, and Economics*, 555–578. https://doi.org/10.4018/979-8-3693-8507-4.ch029

Watson, R. (2024). *Crypto forensics firm Elliptic using advances in AI to detect bitcoin money laundering*. The Block. https://www.theblock.co/post/291826/elliptic-using-advances-in-ai-to-detect-bitcoin-money-laundering

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