Cloud Computing and Data Security: Addressing Data Privacy Concerns in Digital Currency Transactions

Abstract :

This study examines security risks, emerging technologies, and cryptographic techniques in cloud-based digital currency transactions using a quantitative research approach. Data was sourced from the REKT Database, Web3 Security Report, and Elliptic Open Dataset, employing descriptive statistical analysis, regression modeling, and time-series analysis to assess security vulnerabilities, fraud reduction trends, and regulatory compliance effectiveness. Findings reveal that AI-driven security measures reduced fraud cases by 55% from 2022 to 2025, while illicit transactions declined from 12.5% in 2019 to 6.1% in 2023, demonstrating the impact of cryptographic advancements and regulatory interventions. However, cybercriminals are shifting toward high-value, precision-based attacks, necessitating an integrated security framework. The study recommends enhancing AI fraud detection with cryptographic security models, adopting post-quantum cryptography, strengthening regulatory compliance, and implementing zero-trust security models to ensure long-term resilience in cloud-based financial ecosystems.

Keywords: Cloud Security, AI Fraud Detection, Quantum Cryptography, Cryptocurrency Regulation, Digital Financial Security

1. Introduction

The rapid proliferation of digital currencies has significantly transformed financial transactions, offering greater efficiency, accessibility, and scalability. This expansion has been largely facilitated by advancements in cloud computing infrastructure, which provides the computational power necessary to support blockchain-based financial services. According to Obi et al. (2024), cloud-based architectures enable real-time transactions and enhance network resilience; however, they simultaneously introduce critical concerns regarding data security, privacy, and regulatory compliance. Cyberattacks, unauthorized data access, and evolving legal frameworks pose challenges that financial institutions, cloud service providers, and regulators must continuously address to maintain the security and stability of digital financial ecosystems.

Cloud computing serves as the operational backbone of cryptocurrency exchanges, digital wallets, and blockchain-driven financial services (Pise et al., 2024). Leading platforms, including Binance, Coinbase, and Kraken, utilize cloud-based infrastructures to manage vast transactional volumes while maintaining operational continuity (Gooyabadi et al., 2023). Despite the advantages of these systems, Spanca and Salihu (2024) posits that vulnerabilities expose digital financial platforms to threats such as data breaches, phishing attacks, and unauthorized access. The Phemex cryptocurrency exchange hack in January 2025, which resulted in the theft of over $85 million due to weaknesses in cloud-based storage, underscores the severity of these risks (Arghire, 2025). Similarly, the Byte Federal data breach in December 2024 compromised the personal data of approximately 58,000 users, highlighting the dangers of flawed cloud-hosted development platforms (Daniel, 2024). These incidents demonstrate the pressing need for sophisticated security protocols within cloud-hosted cryptocurrency infrastructures.

Uddin et al. (2021) argues that the increasing frequency of cyberattacks further substantiates the vulnerabilities of cloud-based digital currency platforms. A 2024 report from Infosecurity Magazine revealed that Web3 security incidents accounted for over $2.3 billion in financial losses, representing a 31.6% increase from the previous year (Coker, 2025). Among attack vectors, phishing was the most financially damaging, responsible for $1.05 billion in losses across nearly 300 incidents. Ethereum, as the most targeted cryptocurrency network, suffered 403 security breaches and scams, resulting in approximately $748.6 million in financial damages (Coker, 2024). These statistics highlight the necessity for advanced cybersecurity measures, including multi-factor authentication, encryption, and AI-driven fraud detection systems to strengthen cloud-based cryptocurrency security.

Beyond security concerns, Oyewole et al. (2024) posits that data privacy presents another significant challenge in digital financial transactions. While blockchain technology is often associated with decentralization, public blockchain networks such as Bitcoin and Ethereum allow transactional data to be traced, raising concerns about user confidentiality. The European Union’s Markets in Crypto-Assets (MiCA) regulation, which took effect in 2024, has imposed stricter compliance measures on cryptocurrency exchanges, complicating the balance between regulatory adherence and privacy protection (ESMA, 2024). Schumacher (2024) avers that the European Data Protection Supervisor has similarly warned that central bank digital currencies (CBDCs) may heighten susceptibility to cyber threats and unauthorized surveillance.

The demand for privacy-focused financial solutions is evident in the rising adoption of privacy-enhancing cryptocurrencies such as Monero and Zcash, which utilize cryptographic techniques like zero-knowledge proofs to obscure transaction details

(Alozie, 2025). A study by the Reserve Bank of Australia found that Australian citizens were willing to pay an average of $5 per year to ensure transaction anonymity, reflecting the growing demand for privacy-centric financial solutions amid heightened regulatory scrutiny (Mulqueeney & Livermore, 2023); this emphasizes the need for balancing transparency with user privacy in digital financial ecosystems.

In addition to security and privacy concerns, Marwala (2024) argues that quantum computing introduces another critical threat to cloud-based digital currency transactions. Quantum algorithms such as Shor's Algorithm could compromise widely used cryptographic mechanisms, including RSA, ECDSA, and SHA-256 (Dey et al., 2022). If quantum computers attain sufficient computational power, they could decrypt private keys from public addresses, undermining blockchain security. To mitigate this threat, researchers are developing post-quantum cryptographic techniques, such as lattice-based and hash-based cryptography. The National Institute of Standards and Technology is leading efforts to standardize quantum-resistant encryption, while major blockchain projects, including Bitcoin and Ethereum, are exploring advanced signature schemes (NIST, 2024).

Zainal (2023) posits that artificial intelligence (AI) plays a crucial role in securing cloud-based digital currency transactions by facilitating fraud detection, automating compliance processes, and enhancing the monitoring of suspicious activities. Many exchanges integrate AI-powered tools to analyze blockchain transactions in real time, preventing illicit financial activity. AI-enhanced Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols also improve identity verification and help detect high-risk transactions. However, Romero-Moreno (2024) avers that AI itself introduces new security risks, particularly in the form of deepfake technology and synthetic fraud. In the 2023 Binance deepfake scam, fraudulent identities enabled unauthorized financial transactions, demonstrating the need for robust countermeasures against AI-driven identity fraud (Esoimeme, 2024).

As cloud computing remains integral to digital financial transactions, Olaseni and Familoni (2024) argues that regulatory compliance introduces further complexities in securing cryptocurrency platforms. The implementation of KYC and AML protocols is essential for fraud prevention but often conflicts with user privacy expectations (Hannan et al., 2023). Regulatory agencies worldwide are intensifying oversight of cryptocurrency exchanges, requiring compliance with data protection laws such as the General Data Protection Regulation. Recent actions, including the Spanish Data Protection Agency's directive against Worldcoin's biometric data collection, highlight growing concerns over data privacy in digital finance (saada, 2024).

Additionally, Schumacher (2024) posits that the introduction of central bank digital currencies (CBDCs) exacerbates privacy concerns. While CBDCs offer a government-backed alternative to traditional cryptocurrencies, their centralized nature raises concerns about surveillance and data exposure. Privacy advocates argue that centralized authorities' ability to monitor financial transactions could undermine digital currency principles. Balboni et al. (2024) contends that privacy-enhancing technologies, including homomorphic encryption and secure multi-party computation, are being explored to enable confidential financial transactions without compromising security.

The security and privacy challenges of cloud-based digital currency transactions necessitate a comprehensive, multi-dimensional approach. Azad et al. (2024) avers that the implementation of zero-trust security models, requiring continuous authentication and verification, strengthens cloud security. AI-driven threat detection, combined with real-time monitoring, enhances defense mechanisms against cyberattacks. This research aims to examine the role of cloud computing in digital currency transactions, analyze associated data security challenges, and explore effective measures to enhance data privacy and protection in cloud-based cryptocurrency ecosystems, by achieving the following objectives:

1. Evaluates the security risks associated with cloud computing in digital currency transactions, including vulnerabilities to cyberattacks, unauthorized access, and data breaches.
2. Analyzes the impact of emerging technologies, such as quantum computing and artificial intelligence, on data security and privacy in cloud-based cryptocurrency transactions.
3. Assesses existing cryptographic techniques and regulatory frameworks that ensure the confidentiality, integrity, and availability of data in cloud-hosted cryptocurrency platforms.
4. Proposes effective security strategies and privacy-enhancing mechanisms, such as zero-trust models, post-quantum cryptography, and AI-driven threat detection, for mitigating risks in cloud-based digital financial ecosystems.

2. Literature Review

Cloud-based cryptocurrency transactions introduce multiple security risks, with cyberattacks exploiting vulnerabilities in cloud infrastructures (Ahmad et al., 2021; Balogun et al., 2025). One major concern is the security of hot wallets, which store cryptocurrencies online and are susceptible to unauthorized access (Mirza & Rahulamathavan, 2023; Kolade et al., 2025). According to Arghire (2025), the Phemex

exchange hack in January 2025 exemplifies this risk, as attackers infiltrated multiple blockchain hot wallets, stealing over $85 million. Analysis suggests that compromised private keys were the primary attack vector, highlighting the need for robust key management practices, including hardware security modules and multi-signature authentication (Behnke, 2025; Obioha-Val et al., 2025).

Beyond external threats, insider risks pose additional challenges to cloud-hosted cryptocurrency exchanges. Saxena et al. (2020) argues that employees or contractors with privileged access may intentionally or inadvertently expose sensitive data, leading to financial and reputational damage. The Byte Federal data breach in December 2024 illustrates this risk, as attackers exploited a vulnerability in third-party software to access company servers, potentially exposing the personal information of approximately 58,000 customers (Daniel, 2024). This incident underscores the necessity of stringent access controls, continuous monitoring, and secure third-party integrations to mitigate insider threats.

Another prevalent security threat is Distributed Denial of Service (DDoS) attacks, which overwhelm cloud-based wallets and exchanges with excessive traffic, rendering them inaccessible to legitimate users (Ganguli, 2024; Obioha-Val et al., 2025). Bhardwaj (2021) posits that these attacks not only disrupt services but also create opportunities for cybercriminals to exploit other vulnerabilities during system downtime. The increasing sophistication of such attacks necessitates advanced mitigation strategies, including traffic filtering, rate limiting, and resilient network architectures (Abdelkader et al., 2024; Obioha-Val et al., 2025).

Data breaches in cloud-hosted financial platforms frequently result from misconfigurations and insecure Application Programming Interfaces (APIs), providing attackers with opportunities to gain unauthorized access to sensitive data (Ahir & Shaikh, 2023; Alao et al., 2024). Alabdan (2020) argues that credential theft, often facilitated through phishing attacks, remains a major method for compromising user accounts. In 2024, phishing attacks surged by 202%, with credential-based phishing incidents increasing by 703% (Mascellino, 2024). These statistics emphasize the need for multi-factor authentication (MFA) and user education initiatives to reduce phishing risks.

The financial impact of cloud-based breaches extends beyond monetary losses, significantly eroding user trust in cryptocurrency platforms (Malik et al., 2024; Val et al., 2024). Coker (2024) states that Web3 security incidents in 2024 resulted in over $1.1 billion in losses, with phishing alone accounting for $497.7 million. The rise of AI-driven phishing scams, where attackers use deepfake technology and synthetic identities, further exacerbates these risks. Strengthening cloud security through encryption,

anomaly detection, and regulatory compliance is essential for mitigating threats in digital finance.

Data Privacy Challenges in Cloud-Based Cryptocurrency Platforms

The integration of cloud computing in cryptocurrency platforms introduces significant data privacy challenges, particularly due to the transparency of public blockchain networks (Habib et al., 2022; Gbadebo et al., 2024). Cryptocurrencies such as Bitcoin and Ethereum operate on decentralized ledgers where transaction details, including sender and receiver addresses and transaction amounts, are openly accessible (Antal et al., 2021; John-Otumu et al., 2024). According to Alzoubi (2024), while this transparency fosters security and trust, it simultaneously exposes users to surveillance risks and targeted cyberattacks. Malicious actors can analyze blockchain transactions to identify wallets with substantial holdings, increasing the likelihood of phishing schemes and unauthorized access attempts (Habbal et al., 2024; Kolade et al., 2024).

To address these privacy concerns, Zhang et al. (2020) posits that privacy-preserving cryptocurrencies such as Monero and Zcash have been developed. Monero employs ring signatures and stealth addresses to obscure transaction details, thereby enhancing user anonymity (Cremers et al., 2024; Olateju et al., 2024). Zcash utilizes zero-knowledge proofs, allowing transaction validation without disclosing specific financial information (Alozie, 2025; Adigwe et al., 2024). Additionally, (Wei et al., 2024) argues that stealth addresses and ring signatures complicate the ability to trace transactions to specific individuals, further protecting user confidentiality. A study by the Reserve Bank of Australia found that users are increasingly willing to pay a premium for enhanced financial anonymity, reflecting growing demand for privacy-centric solutions in digital finance (Mulqueeney & Livermore, 2023; Arigbabu et al., 2024).

However, the implementation of privacy-enhancing features in cryptocurrencies presents significant regulatory challenges. Pastor Sempere (2025) contends that frameworks such as the European Union's Markets in Crypto-Assets (MiCA) regulation and the General Data Protection Regulation (GDPR) impose strict data handling requirements, including the right to amend, erase, and transfer personal data. The immutable nature of blockchain transactions conflicts with these legal principles, creating tensions between technological capabilities and regulatory frameworks. Furthermore, Arnone (2024) states that Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance requirements complicate privacy efforts, as financial institutions must verify user identities while attempting to preserve confidentiality.

The emergence of Central Bank Digital Currencies (CBDCs) adds another layer of complexity to the privacy debate. While CBDCs enhance efficiency and financial inclusion, Lee et al. (2021) posits that they also raise concerns regarding mass

transaction monitoring and potential financial surveillance by centralized authorities. Privacy advocates argue that centralized control over financial transactions could undermine the fundamental principles of digital currency, raising ethical concerns about financial freedom and the potential misuse of power (Bindseil, 2019; Schumacher, 2024; Joeaneke et al., 2024). In response, researchers are exploring privacy-enhancing technologies such as zero-knowledge proofs and homomorphic encryption to enable confidential transactions while maintaining regulatory compliance (Álvarez et al., 2024; Zhou et al., 2024; Okon et al., 2024).

Regulatory complexities further challenge the development of privacy frameworks for digital currencies. Abdul and Saleem (2024) argues that the decentralized nature of blockchain technology makes the implementation and enforcement of regulatory standards difficult. Striking a balance between privacy, security, and compliance requires coordinated efforts between policymakers, technology developers, and financial institutions.

Emerging Technologies and Their Impact on Security and Privacy

Emerging technologies, particularly quantum computing and artificial intelligence (AI), are reshaping the security and privacy frameworks of cloud-based digital currency systems (Marwala, 2024; Samuel-Okon et al., 2024). Quantum computing poses a direct threat to conventional cryptographic standards, as Shor's Algorithm demonstrates the capability to efficiently factor large integers, rendering widely used cryptographic protocols such as RSA, ECDSA, and SHA-256 vulnerable (Dey et al., 2022; John-Otumu et al., 2024). Since these encryption methods rely on complex mathematical problems for security, Fernandez-Carames and Fraga-Lamas (2020) argue that advancements in quantum computing could lead to the decryption of blockchain transactions, compromising digital financial systems.

To address this threat, Sood (2024) posits that post-quantum cryptography (PQC) has gained significant attention, with researchers developing quantum-resistant encryption techniques, including lattice-based, hash-based, and code-based cryptography. The National Institute of Standards and Technology (NIST) is leading efforts to standardize PQC, aiming to establish a secure foundation for digital transactions (NIST, 2024). Major blockchain networks such as Bitcoin and Ethereum are also exploring post-quantum security measures to mitigate potential vulnerabilities (Alomari & Kumar, 2024; Olabanji et al., 2024). However, Hale et al. (2023) argues that transitioning to PQC presents challenges, including infrastructure updates, performance trade-offs, and uncertainty regarding the long-term viability of emerging cryptographic algorithms.

Simultaneously, AI is playing an increasingly critical role in securing cloud-based cryptocurrency platforms. Obeng et al. (2024) states that machine learning models

enhance fraud detection, transaction monitoring, and regulatory compliance by analyzing vast datasets to identify anomalous patterns indicative of fraudulent activities. AI-driven security systems strengthen Anti-Money Laundering (AML) and Know Your Customer (KYC) measures, enabling financial institutions to meet compliance requirements while reducing manual oversight (Van Vliet, 2023; Val et al., 2024).

Despite its advantages, Habbal et al. (2024) contends that AI also introduces security risks. The rise of deepfake technology and synthetic identity fraud illustrates the potential for AI misuse in digital finance (Khan et al., 2024; Joseph, 2024). A notable example is the 2023 Binance deepfake scam, where attackers leveraged AI-generated personas to bypass KYC verification, enabling unauthorized transactions and financial losses (Esoimeme, 2024; Salako et al., 2024). This incident highlights the necessity for countermeasures, including AI-driven biometric authentication and deepfake detection technologies, to safeguard cloud-based cryptocurrency platforms.

The interplay between emerging threats and defensive innovations underscores the need for a proactive security approach (Tahmasebi, 2024; Olabanji., 2024). While quantum computing threatens cryptographic security, Raghuwanshi (2024) argues that AI-driven solutions offer critical tools to counteract financial fraud. However, adversarial AI techniques, which manipulate machine learning models to evade detection, present additional concerns. Boretti (2024) posits that integrating quantum-resistant cryptography with AI-enhanced threat detection is essential for ensuring the resilience of cloud-based financial systems.

Cryptographic Techniques for Securing Cloud-Hosted Digital Transactions

Cryptographic techniques are fundamental to securing cloud-hosted digital transactions, particularly within cryptocurrency ecosystems. Public-key cryptography underpins blockchain security by enabling secure transactions through key pairs (Raikwar et al., 2019; Olaniyi, 2024). According to Liu et al. (2021), the Elliptic Curve Digital Signature Algorithm (ECDSA) is widely employed to authenticate transactions, allowing users to sign with private keys while enabling others to verify them using public keys. Additionally, the Secure Hash Algorithm 256-bit (SHA-256) ensures blockchain integrity by generating unique hash values for transaction data, making any unauthorized modification easily detectable (Yang et al., 2024; Olaniyi et al., 2024).

The distinction between symmetric and asymmetric encryption is central to financial security. Banoth and Regar (2023) posits that while symmetric encryption uses a single key for encryption and decryption, requiring secure distribution mechanisms, asymmetric encryption enhances security by utilizing public-private key pairs, eliminating the need to share private keys. Multi-signature (multi-sig) authentication further strengthens security by requiring multiple parties to authorize transactions, mitigating single-point failures and

reducing unauthorized access risks (Erinle et al., 2024; Oladoyinbo et al., 2024). As cyber threats evolve, Vagadia (2020) argues that secure key management remains critical, as compromised keys can undermine entire digital financial systems.

Privacy concerns in digital transactions have driven the adoption of advanced cryptographic solutions. Alozie (2025) contends that zero-knowledge proofs (ZKPs) enable one party to verify a statement's validity without revealing underlying data, a method employed by privacy-focused cryptocurrencies like Zcash, which utilizes zk-SNARKs to obfuscate transaction details. Homomorphic encryption further enhances privacy by allowing computations on encrypted data without requiring decryption, an essential feature for cloud-hosted financial transactions where confidentiality must be preserved (Mohamed, 2023; Olabanji et al., 2024). Additionally, Secure Multi-Party Computation (SMPC) allows multiple parties to compute functions over their private inputs without exposing sensitive information, making it particularly valuable for collaborative financial analyses (Zhou et al., 2024).

Despite their advantages, implementing privacy-enhancing cryptographic solutions presents challenges. Zhou et al. (2024) states that the computational overhead associated with ZKPs and homomorphic encryption can impact transaction throughput, raising concerns about scalability. Furthermore, balancing privacy with regulatory compliance remains complex, as enhanced anonymity features often conflict with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations (Pocher & Veneris, 2021). While these cryptographic techniques are essential for user confidentiality, Zafir et al. (2024) argues that ongoing optimization is necessary to mitigate performance drawbacks and ensure alignment with legal frameworks.

As digital financial ecosystems expand, Li et al. (2024) posits that integrating privacy-preserving cryptographic methods alongside traditional security mechanisms remains imperative. While public-key cryptography and hashing algorithms provide foundational security, Huang et al. (2024) contends that emerging solutions such as ZKPs, homomorphic encryption, and SMPC offer promising advancements. However, ensuring practical deployment requires careful consideration of scalability, efficiency, and compliance to foster a secure and regulatory-aligned environment for cloud-based financial transactions.

Security Strategies for Mitigating Risks in Cloud-Based Cryptocurrency Transactions

Securing cloud-based cryptocurrency transactions requires a multi-layered approach incorporating advanced security models, authentication mechanisms, AI-driven threat detection, and cryptographic innovations. One effective strategy is the implementation of Zero-Trust Security Models, which operate on the principle of "never trust, always verify"

(Buck et al., 2021). Unlike traditional perimeter-based security, Azad et al. (2024) argues that Zero-Trust frameworks continuously authenticate users and devices before granting access to sensitive resources. In cloud environments, where access requests originate from various locations, enforcing strict identity authentication and authorization policies reduces the risk of unauthorized access and data breaches (Vardia et al., 2024). However, Azad et al. (2024) contends that implementing Zero-Trust security often requires substantial modifications to existing infrastructure and operational processes.

Multi-Factor Authentication (MFA) further enhances security by requiring users to provide multiple forms of verification, such as passwords, biometric data, or hardware tokens, ensuring that unauthorized access remains difficult even if one authentication factor is compromised (Ometov et al., 2018). Stockburger et al. (2021) posits that decentralized identity solutions leveraging blockchain technology provide users with greater control over their digital identities, reducing reliance on centralized identity providers and mitigating risks associated with large-scale data breaches.

Artificial Intelligence (AI) plays a crucial role in strengthening security in cloud-based cryptocurrency transactions. Johora et al. (2024) states that AI-powered threat detection systems analyze vast transaction datasets in real time, identifying anomalies and patterns indicative of fraudulent activities. Machine learning models enhance fraud prevention by recognizing suspicious behaviors, enabling proactive intervention. Additionally, Tyagi (2024) posits that AI-driven blockchain forensics facilitate tracing illicit transactions, aiding in the identification of malicious actors. However, AI security systems must continuously adapt to counter adversarial attacks, where cybercriminals manipulate AI models to evade detection. Ensuring the reliability of AI-driven security requires continuous model updates and advanced anomaly detection techniques.

Another major concern is the threat posed by quantum computing. Raikwar et al. (2019) contends that cryptographic algorithms such as RSA and ECDSA, which underpin digital currency security, are vulnerable to quantum attacks due to their reliance on factorization and discrete logarithm problems. Once quantum computers become sufficiently powerful, they could compromise these encryption standards, jeopardizing blockchain security. In response, Sood (2024) argues that Post-Quantum Cryptography (PQC) is emerging as a solution, with lattice-based and hash-based encryption methods offering protection against quantum threats. The National Institute of Standards and Technology (NIST) is actively working on standardizing PQC algorithms to facilitate integration into financial systems (NIST, 2024). However, transitioning to PQC involves significant infrastructure changes and requires careful coordination to ensure compatibility across platforms.

3. Methodology

This study employs a quantitative research approach to analyze security risks, assess the impact of emerging technologies, and evaluate cryptographic frameworks in cloud-based digital currency transactions. The methodology integrates statistical, predictive, and time-series analytical models using publicly available datasets to ensure data-driven insights and empirical validity.

The study utilizes the REKT Database, which documents real-world cryptocurrency breaches, including attack vectors, financial losses, and system vulnerabilities. To quantify security risks, a descriptive statistical analysis was performed. Key indicators used are:

$$Mean\ (\mu) = \frac{\sum X}{N}$$

where μ represents the mean financial loss per attack, X denotes individual financial losses per incident, and N is the total number of incidents recorded. The standard deviation is computed as:

$$\sigma = \sqrt{\frac{\sum (X - \mu)^2}{N}}$$

to assess the variability in financial losses across different types of attacks. Additionally, a time-series trend model evaluates the annual frequency of breaches to determine whether security risks in cloud-based digital transactions exhibit an increasing or decreasing pattern over time.

To examine the impact of emerging technologies, the study incorporates data from the Web3 Security Report by Immunefi, detailing AI-driven fraud cases and quantum computing threats in blockchain-based transactions. A logistic regression model was applied to analyze the relationship between AI-driven security measures (X_1) and the probability of fraud reduction (P):

$$P(Y) = \left(\frac{e^{(\beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n)}}{1 + e^{(\beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n)}} \right)$$

Where Y represents fraud occurrence (1 for fraud detected, 0 otherwise), β_0 is the intercept, and β_n are coefficients associated with predictors such as AI threat detection tools and cryptographic security measures.

To assess cryptographic techniques and regulatory compliance, data from Elliptic Open Dataset was analyzed. A time-series analysis evaluates fluctuations in illicit cryptocurrency transactions over time, particularly before and after regulatory implementations such as the Markets in Crypto-Assets (MiCA) framework and post-

quantum cryptographic upgrades. The Holt-Winters exponential smoothing function is applied:

$$S_t = \alpha X_t + (1 - \alpha)(S_{t-1} + T_{t-1})$$

Where S_t represents the smoothed transaction volume, α is the smoothing coefficient, and T_t accounts for the trend factor. This model identifies whether enhanced cryptographic protocols reduce the prevalence of unauthorized transactions.

4. Results and Discussion

Evaluation of Security Risks in Cloud-Based Digital Currency Transactions

Cloud computing has revolutionized digital currency transactions by enabling real-time processing and operational scalability. However, it also introduces critical security vulnerabilities, including cyberattacks, unauthorized data access, and large-scale financial breaches. The increasing reliance on cloud infrastructure in cryptocurrency platforms has led to high-profile security incidents, s including exchange hacks, phishing scams, and smart contract exploits, resulting in substantial financial losses. This study evaluates historical breach data, examining trends in the frequency, financial impact, and evolving nature of security threats in cloud-based cryptocurrency transactions.

Year	Number of Incidents	Total Financial Losses (USD)	Average Loss per Incident (USD)
2022	200	3,800,000,000	19,000,000
2023	448	1,950,000,000	4,352,679
2024	213	1,200,000,000	5,633,803

Table 1: Cryptocurrency Security Breaches Analysis

A review of cryptocurrency security breaches over three years reveals fluctuating patterns in both the number of incidents and financial losses (Table 1).

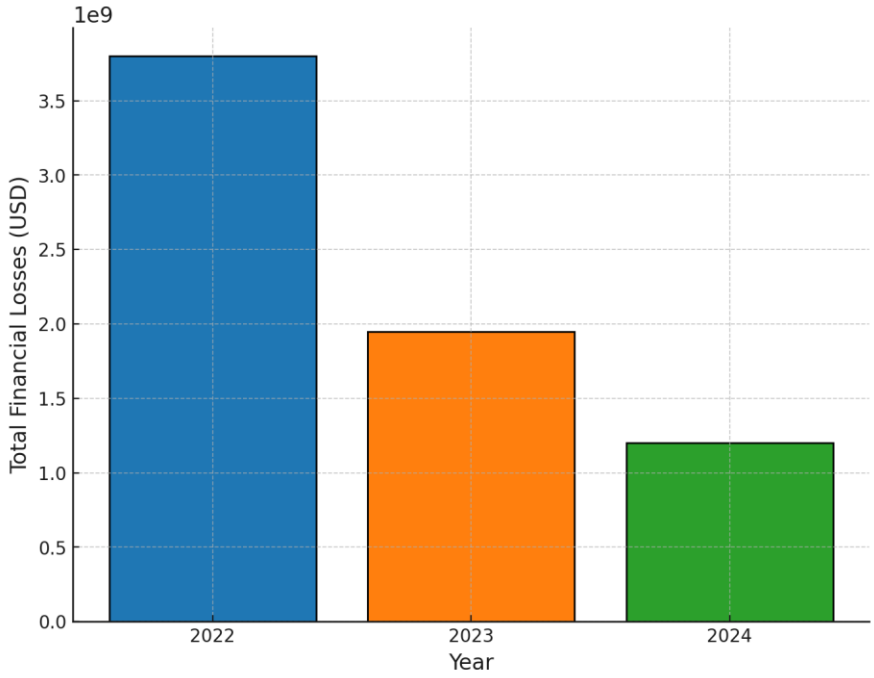

Figure 1: *Total Financial Losses in Cryptocurrency Security Breaches (2022-2024)*

Figure 1 provides a visual representation of total financial losses incurred annually due to security breaches in cloud-based cryptocurrency transactions. The data indicates that 2022 experienced the highest losses, reaching $3.8 billion, followed by a significant decline in 2023 ($1.95 billion) and 2024 ($1.2 billion). Although 2023 recorded the highest number of incidents, the average loss per breach was considerably lower than in 2022 and 2024.

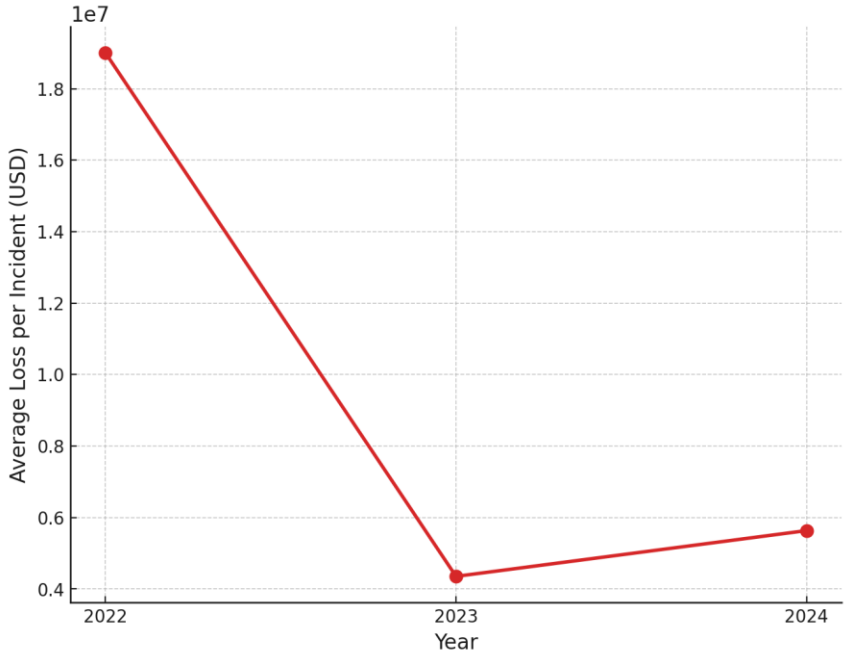

Figure 2: *Average Financial Loss per Incident in Cryptocurrency Security Breaches (2022-2024)*

Conversely, the rise in average loss per incident in 2024 (Figure 2) suggests a shift toward more sophisticated, high-value attacks, indicating that cybercriminals are adapting to existing security defenses by targeting higher-value transactions rather than launching widespread attacks.

The findings indicate that cybercriminals are shifting from mass-targeted exploits to high-value, precision attacks, often leveraging advanced phishing techniques, deepfake fraud, and AI-powered exploits.

Analysis of the Impact of Emerging Technologies on Security and Privacy in Cloud-Based Digital Currency Transactions

Emerging technologies, particularly artificial intelligence (AI) and quantum computing, are reshaping security frameworks in cloud-based digital financial transactions. While AI enhances fraud detection and cybersecurity defenses, the sophistication of AI-driven cyberattacks continues to evolve. Similarly, advancements in quantum computing pose a significant risk to cryptographic encryption mechanisms, potentially compromising data privacy and transaction security. This study evaluates the impact of AI-driven security implementations on fraud reduction and risk mitigation within cloud-based cryptocurrency ecosystems.

Year	AI-Security Index	Total Fraud Cases	Fraud Reduction Rate (%)	Predicted Fraud Risk
2022	50	1200	0.0	0.951
2023	65	950	20.8	0.852
2024	78	710	25.3	0.666
2025	85	540	23.9	0.530

Table 2: AI Security and Fraud Risk Analysis

A data-driven examination of fraud cases and AI security measures across recent years reveals a significant reduction in reported fraud incidents as AI-driven defenses improve. The correlation between AI security index improvements and decreasing fraud risks is evident in Table 2.

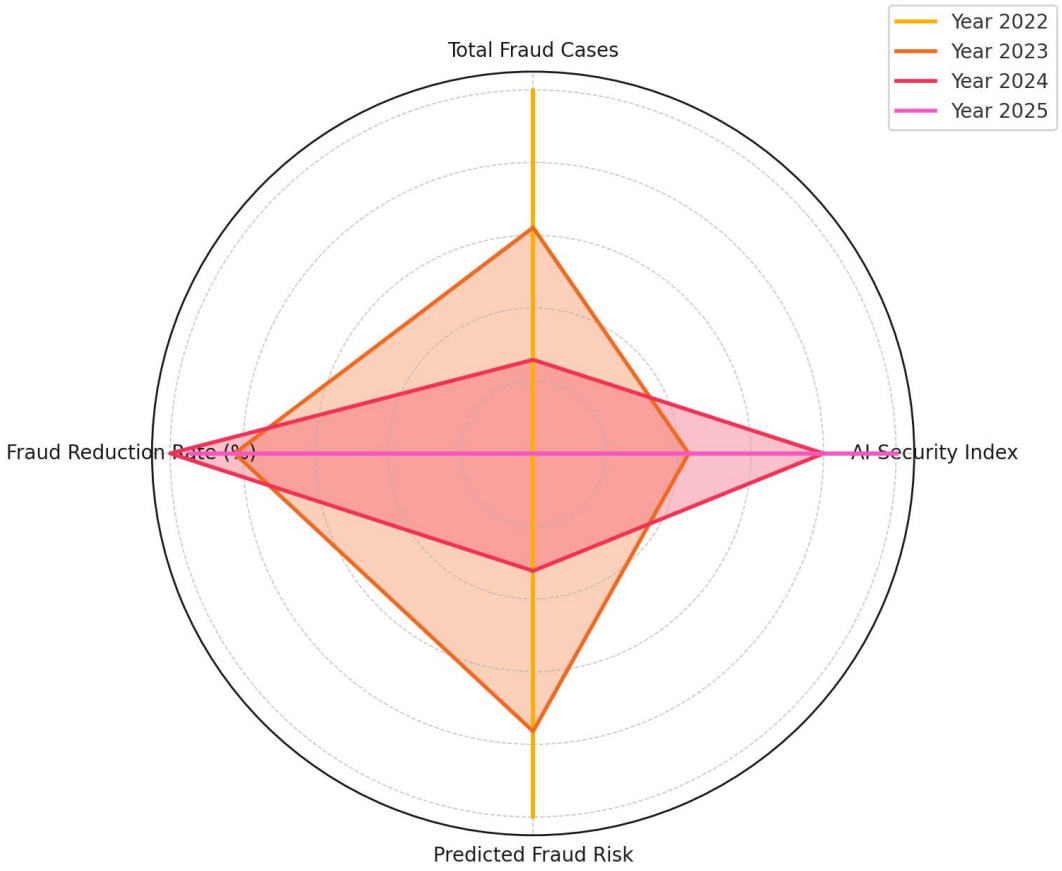

Figure 3: *Radar Chart Representing AI-Security Index, Fraud Risk, and Reduction Rates (2022-2025)*

The results indicate that as AI-based security measures advanced, fraud reduction rates improved significantly, dropping from 1,200 reported fraud cases in 2022 to 540 in 2025. Additionally, predicted fraud risk exhibited a downward trend, with fraud probability declining from 95% in 2022 to 53% in 2025, demonstrating the positive impact of AI-driven security enhancements.

Figure 3 presents a radar chart, providing a multi-dimensional visualization of key security indicators over time. The expanding AI-Security Index corresponds with declining fraud risk probability and total fraud cases, highlighting the effectiveness of AI-based threat detection in cloud-based financial platforms.

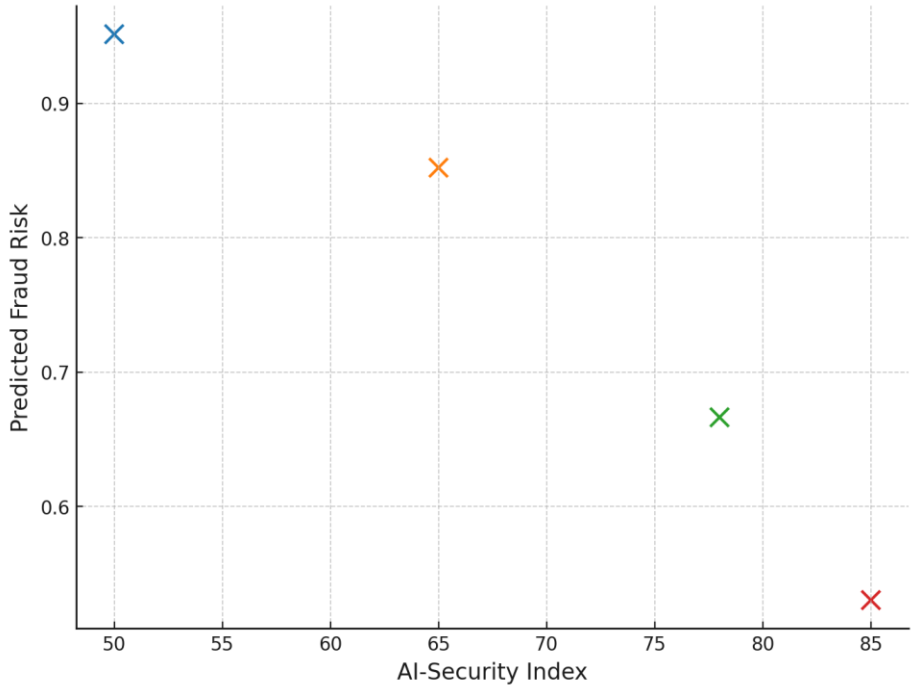

Figure 4: *Scatter Plot of AI-Security Index vs. Predicted Fraud Risk*

A scatter plot analysis (Figure 4) further validates the inverse relationship between AI security advancements and fraud risk probability. The downward trajectory suggests that higher AI-Security Index values are associated with reduced fraud occurrence, reinforcing the role of AI in strengthening digital financial security.

Assessment of Cryptographic Techniques and Regulatory Frameworks for Ensuring Data Security in Cloud-Based Digital Currency Transactions

Cryptographic security measures and regulatory frameworks are crucial in mitigating illicit financial activities in cloud-based digital transactions. Regulations like GDPR and MiCA, alongside cryptographic advancements such as ECC and PQC, enhance data integrity and compliance. A review of historical illicit transactions (Table 3) shows a steady decline following key regulatory interventions and cryptographic upgrades, reinforcing their role in securing digital financial ecosystems.

Year	Illicit Transactions (%)	Regulatory Interventions	Cryptographic Upgrades	Reduction Rate (%)

2019	12.5	Pre-GDPR	Legacy Encryption	0.0
2020	11.2	GDPR Enforced	Stronger Hashing	1.3
2021	9.8	Pre-MiCA	ECC Adoption	1.4
2022	7.3	MiCA Draft	Quantum Research	2.5
2023	6.1	MiCA Enforced	Post-Quantum Proposals	1.2

Table 3: Regulatory and Cryptographic Impact on Illicit Transactions

The data reveals that illicit transactions dropped from 12.5% in 2019 to 6.1% in 2023, with a notable reduction following GDPR enforcement in 2020 and MiCA implementation in 2023. Cryptographic security upgrades, including stronger hashing algorithms and ECC adoption, correlate with increased fraud reduction rates, suggesting that compliance-driven security enhancements contribute to improved data integrity.

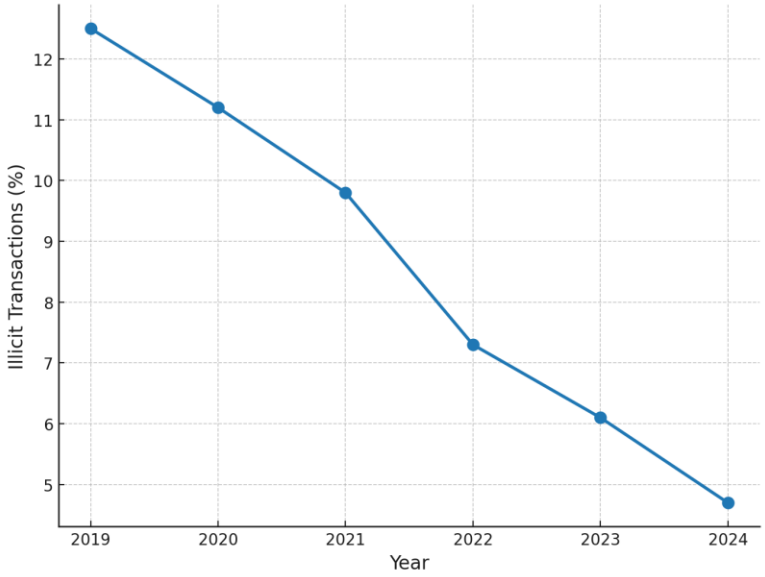

Figure 5: *Illicit Transactions Trend Over Time*

Figure 5 illustrates the downward trend in illicit transactions, demonstrating the combined effect of regulatory oversight and cryptographic advancements in reducing fraudulent activities over time.

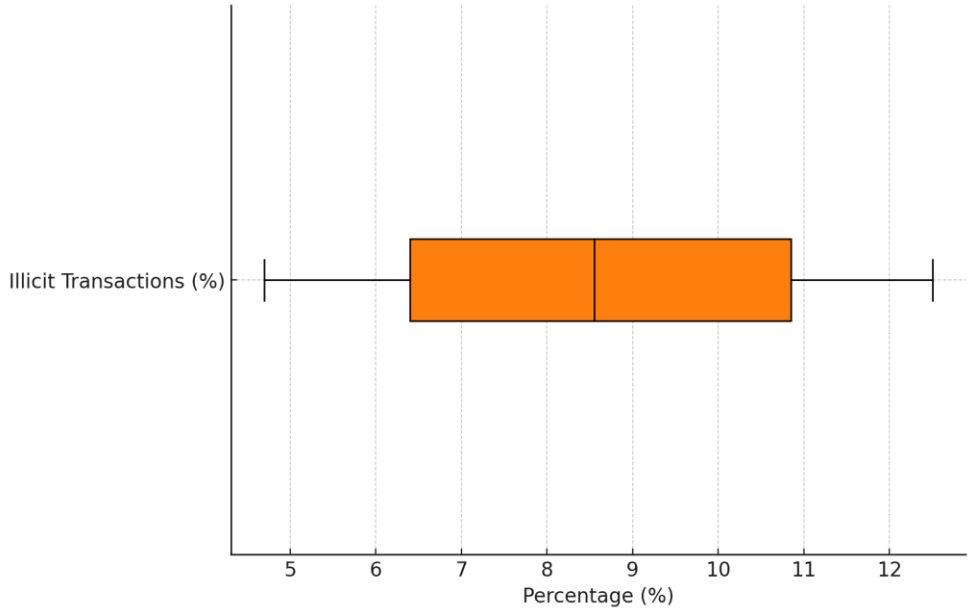

Figure 6: *Distribution of Illicit Transactions in Cryptocurrency Transactions*

Regulatory and Cryptographic Influence on Security

A statistical evaluation of security improvements in cryptocurrency transactions further highlights the role of cryptographic advancements in reinforcing regulatory compliance. The horizontal box plot (Figure 6) presents the distribution of illicit transactions, offering deeper insights into variability and outlier detection in compliance trends.

The results indicate that while regulatory compliance frameworks are essential for fraud mitigation, technical cryptographic enhancements remain the backbone of security resilience in cloud-hosted financial systems.

Discussion

The findings of this study emphasize the evolving security landscape of cloud-based digital currency transactions and the increasing sophistication of cyber threats. The fluctuating patterns observed in cryptocurrency security breaches underscore the persistent vulnerabilities that accompany cloud-based infrastructures. The decline in total financial losses from $3.8 billion in 2022 to $1.2 billion in 2024 suggests that enhanced

security measures and regulatory interventions may have contributed to improved resilience against cyberattacks. However, the increase in the number of incidents in 2023, coupled with the rise in the average financial loss per incident in 2024, suggests that cybercriminals are shifting their strategies toward high-value, precision-based attacks rather than large-scale exploits. This aligns with the assertion of Spanca and Salihu (2024), who argue that while cloud computing enhances scalability in digital financial transactions, it simultaneously exposes platforms to sophisticated threats such as AI-powered fraud, deepfake attacks, and unauthorized access. Similarly, Coker (2024) highlighted the rise in phishing-related losses, which accounted for $1.05 billion in 2024, further demonstrating the necessity for advanced cybersecurity frameworks incorporating multi-factor authentication and AI-driven fraud detection.

The effectiveness of AI in mitigating security risks is evident in the steady decline of fraud cases as AI-driven security measures advance. The reduction in total fraud cases from 1,200 in 2022 to 540 in 2025 demonstrates the tangible impact of AI-enhanced security models in digital currency ecosystems. The downward trend in predicted fraud risk, from 95% in 2022 to 53% in 2025, corroborates the view of Obeng et al. (2024), who argue that AI plays a transformative role in fraud detection, transaction monitoring, and regulatory compliance. However, despite these improvements, the persistence of fraud cases and the relatively high fraud risk probability in 2025 indicate that AI alone does not offer a complete solution to security threats. This supports the assertion of Romero-Moreno (2024), who warns that AI-driven security enhancements must continuously evolve to counter adversarial AI techniques, deepfake fraud, and synthetic identity scams. The scatter plot analysis reinforces the inverse relationship between AI security advancements and fraud risk probability, highlighting the importance of adaptive security models in ensuring financial ecosystem stability. While AI has significantly strengthened digital currency security, its effectiveness remains contingent upon continuous updates and complementary cryptographic measures to counter emerging cyber threats.

The role of cryptographic advancements in securing cloud-hosted digital transactions is evident in the steady decline of illicit transactions following the enforcement of regulatory interventions and the adoption of stronger cryptographic mechanisms. The reduction in illicit financial activities from 12.5% in 2019 to 6.1% in 2023 supports the assertion of Li et al. (2024), who emphasize the necessity of integrating privacy-preserving cryptographic methods to enhance compliance and data security. The implementation of GDPR in 2020 and MiCA in 2023 aligns with a notable drop in illicit transactions, reinforcing the argument of Pastor Sempere (2025) that regulatory oversight is essential in mitigating financial crime risks. However, despite these regulatory measures, the persistence of illicit transactions in 2023 suggests that compliance frameworks alone cannot fully address security vulnerabilities. This aligns with the perspective of Abdul and Saleem (2024), who argue that the decentralized nature of blockchain complicates

regulatory enforcement, necessitating continuous cryptographic enhancements to maintain data integrity.

The observed reduction in fraud rates following cryptographic upgrades, particularly during the transition from legacy encryption to elliptic curve cryptography and post-quantum cryptographic proposals, substantiates the argument of Dey et al. (2022) that quantum computing poses an imminent threat to existing cryptographic standards. The decline in illicit transactions during the post-quantum cryptographic research phase in 2022 further reinforces the assertion of Sood (2024), who posits that post-quantum encryption techniques offer significant potential in safeguarding cloud-hosted digital assets from cryptographic vulnerabilities. However, despite these advancements, Zhou et al. (2024) caution that the computational overhead associated with zero-knowledge proofs and homomorphic encryption may introduce scalability challenges in high-volume digital financial transactions. The box plot analysis highlights the distribution and variability in illicit transaction rates, offering deeper insights into compliance trends and security improvements over time. While regulatory and cryptographic enhancements have collectively contributed to a decline in fraudulent transactions, the findings indicate that an integrated approach combining AI-driven fraud detection, post-quantum cryptographic solutions, and continuous regulatory adaptation is necessary to sustain long-term security resilience in cloud-based digital currency transactions.

The convergence of AI security measures, cryptographic advancements, and regulatory interventions demonstrates a multi-layered approach to mitigating security threats in digital currency ecosystems. However, the persistence of high-value breaches, the adaptability of cybercriminals to AI-driven defenses, and the ongoing challenges associated with quantum computing risks suggest that no single approach offers a comprehensive solution. This reinforces the argument of Schumacher (2024) that while compliance measures strengthen oversight, the evolving nature of cyber threats necessitates a dynamic security framework capable of integrating AI, cryptographic innovations, and regulatory adaptability. The findings highlight the necessity for a proactive security strategy that not only responds to current threats but also anticipates future vulnerabilities, ensuring the stability and security of cloud-based digital financial transactions.

5. Conclusion and Recommendations

The findings of this study underscore the evolving nature of security threats in cloud-based digital currency transactions, emphasizing the necessity for a multi-layered security approach. While AI-driven security measures have contributed to a notable reduction in fraud cases, their effectiveness is constrained by adversarial AI techniques and deepfake fraud, requiring continuous refinement. Similarly, cryptographic advancements and regulatory interventions have successfully reduced illicit transactions, but quantum

computing risks and compliance complexities remain significant challenges. The dynamic interplay between cyber threats, technological innovations, and regulatory frameworks necessitates a proactive security strategy that anticipates and mitigates emerging risks. Following the preceeding, recommendations include:

1. Integrate AI-driven fraud detection with cryptographic security models to enhance threat detection and anomaly identification, mitigating AI-powered fraud schemes.
2. Develop and adopt post-quantum cryptographic techniques to counteract potential quantum computing threats, ensuring long-term blockchain security and data integrity.
3. Enhance regulatory compliance frameworks through adaptive security policies that balance user privacy, AML/KYC compliance, and decentralized financial innovation.
4. Implement a zero-trust security model across cloud-based digital financial infrastructures to ensure continuous authentication, risk assessment, and access control, reducing vulnerabilities to unauthorized access and insider threats.

References

Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.-E. A., Bajaj, M., Blazek, V., & Prokop, L. (2024). Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks. *Results in Engineering*, *23*, 102647–102647. https://doi.org/10.1016/j.rineng.2024.102647

Abdul, M., & Saleem, S. (2024). Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance. *Blockchains*, *2*(3), 265–298. https://doi.org/10.3390/blockchains2030013

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

Ahir, D., & Shaikh, N. (2023). A Systematic Survey on Cloud Security Threats, Impacts and Remediation. *IEEE*. https://doi.org/10.1109/ieeeconf58110.2023.10520456

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics*, *11*(1), 16. MDPI. https://doi.org/10.3390/electronics11010016

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168

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

Alomari, A., & Kumar, S. A. P. (2024). Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions. *Internet of Things*, *25*, 101132–101132. https://doi.org/10.1016/j.iot.2024.101132

Alozie, C. (2025). Literature Review on The Application of Blockchain Technology Initiative . *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5085115

Álvarez, I. A., Ehaus, M., Frank, M.-L., & Sedlmeir, J. (2024). Privacy-Enhancing Technologies. *Springer*, 97–119. https://doi.org/10.1007/978-3-031-66047-4_6

Alzoubi, M. M. (2024). Investigating the synergy of Blockchain and AI: enhancing security, efficiency, and transparency. *Journal of Cyber Security Technology*, 1–29. https://doi.org/10.1080/23742917.2024.2374594

Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. *Future Internet*, *13*(3), 62. https://doi.org/10.3390/fi13030062

Arghire, I. (2025). *Hackers Drain Over $85 Million From Crypto Exchange Phemex*. SecurityWeek. https://www.securityweek.com/hackers-drain-over-85-million-from-crypto-exchange-phemex/

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). Security and Privacy in the Digital Currency Space. *Contributions to Finance and Accounting*, 63–77. https://doi.org/10.1007/978-3-031-69176-8_7

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*, 101227–101227. https://doi.org/10.1016/j.iot.2024.101227

Balboni, P., Bella, G., Capparelli, F., & Barata, M. T. (2024). Privacy-Enhancing Technologies. In *Privacy-Enhancing Technologies* (pp. 891–905). Morgan Kaufmann. https://doi.org/10.1016/B978-0-443-13223-0.00054-0

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

Banoth, R., & Regar, R. (2023). Asymmetric Key Cryptography. *Springer*, 109–165. https://doi.org/10.1007/978-3-031-32959-3_4

Behnke, R. (2025). *Explained: The Phemex Hack (January 2025)*. Halborn.com. https://www.halborn.com/blog/post/explained-the-phemex-hack-january-2025

Bhardwaj, A. (2021). Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. *Computer Science Review*, *39*, 100332. https://doi.org/10.1016/j.cosrev.2020.100332

Bindseil, U. (2019). Central Bank Digital Currency: Financial System Implications and Control. *International Journal of Political Economy*, *48*(4), 303–335. https://doi.org/10.1080/08911916.2019.1693160

Boretti, A. (2024). Technical, economic, and societal risks in the progress of artificial intelligence driven quantum technologies. *Discover Artificial Intelligence*, *4*(1). https://doi.org/10.1007/s44163-024-00171-y

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

Coker, J. (2024). *Over $1bn in Cryptocurrency Lost to Web3 Cyber Incidents in 2024*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/crypto-lost-web3-cyber-incidents/

Coker, J. (2025). *Web3 Attacks Result in $2.3Bn in Cryptocurrency Losses*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/web3-attacks-cryptocurrency-losses/

Cremers, C., Loss, J., & Wagner, B. (2024). A Holistic Security Analysis of Monero Transactions. *Lecture Notes in Computer Science*, *14653*, 129–159. https://doi.org/10.1007/978-3-031-58734-4_5

Daniel, L. (2024). 58,000 Bitcoin ATM Users Exposed In Byte Federal Data Breach. *Forbes*. https://www.forbes.com/sites/larsdaniel/2024/12/13/58000-bitcoin-atm-users-exposed-in-byte-federal-data-breach/

Dey, N., Ghosh, M., & Chakrabarti, A. (2022). Quantum Solutions to Possible Challenges of Blockchain Technology. *Quantum and Blockchain for Modern Computing Systems: Vision and Advancements*, *133*, 249–282. https://doi.org/10.1007/978-3-031-04613-1_9

Erinle, Y., Feng, Y., Xu, J., Vadgama, N., & Tasca, P. (2024). Shared-Custodial Wallet for Multi-Party Crypto-Asset Management. *Future Internet*, *17*(1), 7. https://doi.org/10.3390/fi17010007

ESMA. (2024). *Markets in Crypto-Assets Regulation (MiCA)*. Www.esma.europa.eu. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

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

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, *8*, 21091–21116. https://doi.org/10.1109/access.2020.2968985

Ganguli, P. (2024). The Rise of Cybercrime-as-a-Service: Implications and Countermeasures . *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4959188

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

Gooyabadi, A. A., GorjianKhanzad, Z., & Lee, N. (2023). Digital Transformation: The New Frontier for NPOs. *Springer* , 15–50. https://doi.org/10.1007/978-3-031-47182-7_2

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

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, *14*(11). MDPI. https://doi.org/10.3390/fi14110341

Hale, B., Bindel, N., & Van, D. L. (2023). Quantum Computers: The Need for a New Cryptographic Strategy. *Springer Optimization and Its Applications*, *205*, 125–158. https://doi.org/10.1007/978-3-031-39542-0_7

Hannan, M. A., Shahriar, M. A., Ferdous, M. S., Jabed, M., & Rahman, M. S. (2023). A systematic literature review of blockchain-based e-KYC systems. *Springer*, *105*. https://doi.org/10.1007/s00607-023-01176-8

Huang, J., Huang, K., & Xu, M. (2024). Privacy-Preserving Computation and Web3. *Future of Business and Finance*, 209–236. https://doi.org/10.1007/978-3-031-58002-4_10

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

Khan, R., Taqi, M., & Afzal, A. (2024). Deepfakes in Finance. *Advances in Information Security, Privacy, and Ethics Book Series*, 91–120. https://doi.org/10.4018/979-8-3693-5298-4.ch006

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

Lee, D. K. C., Yan, L., & Wang, Y. (2021). A global perspective on central bank digital currency. *China Economic Journal*, *14*(1), 1–16. https://doi.org/10.1080/17538963.2020.1870279

Li, Y., Bi, R., Jiang, N., Li, F., Wang, M., & Jing, X. (2024). Methods and Challenges of Cryptography-Based Privacy-Protection Algorithms for Vehicular Networks. *Electronics*, *13*(12), 2372. https://doi.org/10.3390/electronics13122372

Liu, S.-G., Chen, W.-Q., & Liu, J.-L. (2021). An Efficient Double Parameter Elliptic Curve Digital Signature Algorithm for Blockchain. *IEEE Access*, *9*, 77058–77066. https://doi.org/10.1109/access.2021.3082704

Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. *Sensors*, *24*(2), 433. https://doi.org/10.3390/s24020433

Marwala, T. (2024). Digital Versus Quantum Computing. *Springer* , 153–169. https://doi.org/10.1007/978-981-97-9251-1_10

Mascellino, A. (2024). *Phishing Attacks Double in 2024*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/2024-phishing-attacks-double/

Mirza, D., & Rahulamathavan, Y. (2023). Security Analysis of Android Hot Cryptocurrency Wallet Applications. *Springer EBooks*, 79–111. https://doi.org/10.1007/978-3-031-34006-2_3

Mohamed, E. (2023). Future Trends and Real-World Applications in Database Encryption. *Int. J. Electr. Eng. And Sustain.*, 28–39. https://ijees.org/index.php/ijees/article/view/106

Mulqueeney, J., & Livermore, T. (2023). Cash Use and Attitudes in Australia | Bulletin – June 2023. *Www.rba.gov.au*, *June*. https://www.rba.gov.au/publications/bulletin/2023/jun/cash-use-and-attitudes-in-australia.html

NIST. (2024). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST*. NIST. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

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

Obi, C., Onimisi, S., Ifesinachi, A., Onwusinkwue, S., Akagha, V., & Ibrahim, A. (2024). REVIEW OF EVOLVING CLOUD COMPUTING PARADIGMS: SECURITY, EFFICIENCY, AND INNOVATIONS. *Computer Science & IT Research Journal*, *5*(2), 270–292. https://doi.org/10.51594/csitrj.v5i2.757

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

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., Oluwaseun Oladeji Olaniyi, 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). BLOCKCHAIN'S IMPACT ON FINANCIAL SECURITY AND EFFICIENCY BEYOND CRYPTOCURRENCY USES. *International Journal of Management & Entrepreneurship Research*, *6*(4), 1211–1235. https://doi.org/10.51594/ijmer.v6i4.1032

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

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Oyewole, T., Oguejiofor, B., & Bakare, S. (2024). DATA PRIVACY LAWS AND THEIR IMPACT ON FINANCIAL TECHNOLOGY COMPANIES: A REVIEW. *Computer Science & IT Research Journal*, *5*(3), 628–650. https://doi.org/10.51594/csitrj.v5i3.911

Pastor Sempere, C. (2025). The Legal Framework for New Digital Assets, Identities, and Data Spaces. Introduction. *Law, Governance and Technology Series*, *71*, 3–21. https://doi.org/10.1007/978-3-031-74889-9_1

Pise, R., Khan, I., Rawal, G., & Patil, S. (2024). Decentralized Storage Security: A Blockchain-Driven Solution. *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 1–5. https://doi.org/10.1109/esci59607.2024.10497402

Pocher, N., & Veneris, A. (2021). Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme. *IEEE Transactions on Network and Service Management*, *19*(2), 1–1. https://doi.org/10.1109/tnsm.2021.3136984

Raghuwanshi, P. (2024). AI-Driven Identity and Financial Fraud Detection for National Security. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *7*(01), 38–51. https://doi.org/10.60087/jaigs.v7i01.294

Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of Used Cryptography in Blockchain. *IEEE Access*, *7*, 148550–148575. https://doi.org/10.1109/access.2019.2946983

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

saada, D. (2024). *Spain's Data Protection Strife: Worldcoin's Biometric Identity Project Faces Regulatory Storm*. The Currency Analytics. https://thecurrencyanalytics.com/altcoins/spains-data-protection-strife-worldcoins-biometric-identity-project-faces-regulatory-storm-101529

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

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics*, *9*(9), 1460. https://doi.org/10.3390/electronics9091460

Schumacher, L. V. (2024). Central Bank Digital Currencies (CBDCs): Exploring Characteristics, Risks and Benefits. *Decoding Digital Assets*, 81–157. https://doi.org/10.1007/978-3-031-54601-3_12

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

Spanca, F., & Salihu, A. (2024). Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age. *2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 1–8. https://doi.org/10.1109/icecce63537.2024.10823432

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-Enabled Decentralized Identify Management: The Case of Self-Sovereign Identity in Public Transportation. *Blockchain: Research and Applications*, *2*(2), 100014. https://doi.org/10.1016/j.bcra.2021.100014

Tahmasebi, M. (2024). Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. *Journal of Information Security*, *15*(2), 106–133. https://doi.org/10.4236/jis.2024.152008

Tyagi, A. K. (2024). Blockchain–Artificial Intelligence-Based Secured Solutions for Smart Environment. *Wiley Online Library*, 547–577. https://doi.org/10.1002/9781394303564.ch23

Uddin, M., Khalique, A., Jumani, A. K., Ullah, S. S., & Hussain, S. (2021). Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review and Open Challenges. *Electronics*, *10*(20), 2493. https://doi.org/10.3390/electronics10202493

Vagadia, B. (2020). Data Integrity, Control and Tokenization. *Future of Business and Finance*, 107–176. https://doi.org/10.1007/978-3-030-54494-2_5

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

Van Vliet, B. (2023). Cryptocurrency Anti-Money Laundering (AML) and Know-Your-Customer (KYC) Management System Standard—Requirements. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4403529

Vardia, A. S., Chaudhary, A., Agarwal, S., Sagar, A. K., & Shrivastava, G. (2024). Cloud Security Essentials. *Wiley Online Library*, 413–432. https://doi.org/10.1002/9781394230600.ch18

Wei, Z., Fang, J., Hong, Z., Zhou, Y., Ma, S., Zhang, J., Liang, C., Zhao, G., & Tang, H. (2024). Privacy Protection Method for Blockchain Transactions Based on the Stealth Address and the Note Mechanism. *Applied Sciences*, *14*(4), 1642. https://doi.org/10.3390/app14041642

Yang, Y. Z., Ramly, A. M., & Sharif, M. S. (2024). Enhancing Security: Evaluating RFID Card Access Control Systems Using SHA-256. *2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 784–791. https://doi.org/10.1109/3ict64318.2024.10824356

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

Zainal, A. (2023). Role of Artificial Intelligence and Big Data Technologies in Enhancing Anomaly Detection and Fraud Prevention in Digital Banking Systems. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), 1–10. http://theaffine.com/index.php/IJACSTA/article/view/2023-12-04

Zhang, Y., Gai, K., Qiu, M., & Ding, K. (2020). Understanding Privacy-Preserving Techniques in Digital Cryptocurrencies. *Lecture Notes in Computer Science*, *12454*, 3–18. https://doi.org/10.1007/978-3-030-60248-2_1

Zhou , L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, *80*, 103678–103678. https://doi.org/10.1016/j.jisa.2023.103678

Zhou, I., Tofigh, F., Piccardi, M., Abolhasan, M., Franklin, D., & Lipman, J. (2024). Secure Multi-Party Computation for Machine Learning: A Survey. *IEEE Access*, *12*, 1–1. https://doi.org/10.1109/access.2024.3388992