Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and Its Applicability to Decentralized Finance (DeFi)

Abstract

This study evaluates the effectiveness of cybersecurity frameworks in mitigating cyber threats in traditional banking while assessing their applicability to Decentralized Finance (DeFi). Using financial sector reports, cybersecurity incident databases, and DeFi security audits, we analyze compliance with NIST CSF, ISO/IEC 27001, and PCI-DSS alongside factors such as bank size, IT security investments, and regulatory fines to determine their impact on cyber resilience. Logistic regression results indicate that compliance with cybersecurity frameworks reduces cyberattack likelihood ($p = 0.0689$, marginally significant), while larger institutions face fewer threats ($p = 0.0256$, statistically significant). However, increased IT security budgets paradoxically correlate with higher attack frequencies ($p = 0.0385$, statistically significant), suggesting larger attack surfaces may offset security investments.In contrast, DeFi faces disproportionately higher smart contract exploits, flash loan attacks, and oracle manipulation, leading to significantly greater financial losses ($F = 216.92$, $p < 0.001$, highly significant) than traditional banking cyber incidents. Regulatory compliance and industry collaboration show promise in reducing attack occurrences, with cyber incidents projected to decline by over 40% by 2029 under stricter enforcement. However, traditional frameworks are insufficient for DeFi's decentralized structure, necessitating AI-driven threat detection, mandatory smart contract audits, secure oracle mechanisms, and adaptive regulatory frameworks.This study highlights the urgent need for tailored DeFi cybersecurity strategies while reinforcing the effectiveness of compliance-driven models in banking. It provides actionable insights for financial institutions, regulators, and cybersecurity professionals seeking to enhance resilience across centralized and decentralized financial systems.

Keywords: Cybersecurity frameworks, financial sector resilience, Decentralized Finance, cyber risk mitigation, regulatory compliance.

1. Introduction

The financial sector has experienced a paradigm shift due to rapid digital transformation, introducing both unprecedented opportunities and significant cybersecurity risks. Traditional banking institutions have long been prime targets for cyberattacks due to their vast repositories of financial and personal data. Similarly, Decentralized Finance (DeFi), an emerging and rapidly evolving financial ecosystem built on blockchain technology, has become a major target for cybercriminals due to its decentralized nature, smart contract vulnerabilities, and regulatory ambiguities (Kaur et al., 2023).

Cyberattacks on financial institutions have surged in recent years, with the International Monetary Fund (IMF) reporting over 20,000 cyberattacks on the financial sector, resulting in losses exceeding $12 billion

in the last two decades (IMF, 2024). The increasing sophistication of cyber threats has led to the adoption of cybersecurity frameworks aimed at safeguarding financial assets and maintaining consumer trust. For traditional banking, frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO/IEC 27001, and the Payment Card Industry Data Security Standard (PCI-DSS) have been instrumental in mitigating risks (Dawodu et al., 2023). However, DeFi, which lacks centralized governance and oversight, has been disproportionately affected by cyber threats, including liquidity pool exploits, oracle manipulation, and smart contract vulnerabilities, leading to significant financial losses (Werner et al., 2023).

Cyberattacks on financial institutions vary in scale and sophistication. The most common threats include phishing, ransomware, Distributed Denial-of-Service (DDoS) attacks, and social engineering tactics (Srinivas et al., 2023). A notable case was the 2021 DDoS attack on a German IT provider, which disrupted 800 cooperative banks, highlighting the vulnerabilities in traditional banking infrastructure. Despite the adoption of robust cybersecurity frameworks, traditional banks remain vulnerable due to the evolving nature of cyber threats and compliance-driven security models that prioritize audits over real-time threat detection (Adegbite et al., 2023).

In contrast, DeFi operates in an unregulated, permissionless environment, making it attractive to malicious actors. Research highlights that the five largest DeFi cyberattacks have resulted in cumulative losses exceeding $2 billion, including the $610 million Poly Network hack in 2021 and the $540 million Ronin Network exploit in 2022 (Liu et al., 2023). The lack of centralized security oversight, reliance on smart contracts, and dependence on oraclesforpricefeeds have significantly increased security risks within the DeFi ecosystem (Piehani, 2023). Additionally, DeFi's susceptibility to market manipulation and fraudulent schemes has raised concerns about its long-term viability without regulatory intervention (Didenko, 2023).

Traditional banking institutions have invested heavily in regulatory compliance, risk management, and incident response strategies. Frameworks like NIST CSF, PCI-DSS, and ISO 27001 have been crucial in standardizing cybersecurity practices across financial institutions (Sulistyowati et al., 2023). However, there are ongoing concerns about whether compliance-based security models are truly effective in preventing sophisticated cyberattacks or merely serve as a regulatory obligation (Goodwin, 2023).

On the other hand, DeFi's regulatory scope remains fragmented. While some jurisdictions have begun exploring regulatory sandboxes and self-regulatory frameworks, there is no global consensus on how DeFi security should be governed (AlBenJasim et al., 2023). The absence of mandatory compliance standards has contributed to DeFi's increased vulnerability to fraud and cyber threats, leading to calls for the adaptation of traditional banking security frameworks to the DeFi ecosystem (Zhou et al., 2023).

However, research suggests that existing banking cybersecurity frameworks cannot be directly applied to DeFi without significant modifications (Wronka, 2023).

Given these concerns, this study aims to critically assess the effectiveness of cybersecurity frameworks in traditional banking and examine their applicability to the DeFi sector. The key research objectives include:

1. Evaluating the extent to which existing cybersecurity frameworks, such as NIST CSF and PCI-DSS, have enhanced cyber resilience in traditional banking institutions.
2. Analyzing the primary cybersecurity threats facing the DeFi ecosystem and comparing them with traditional banking threats.
3. Investigating whether traditional banking cybersecurity strategies can be adapted to DeFi or if novel security measures are required.
4. Assessing the role of regulatory compliance and industry collaboration in mitigating cyber risks across both sectors.

Addressing these objectives is imperative, as financial institutions must proactively enhance their cybersecurity posture to mitigate the growing threats posed by cybercriminals. While traditional banking institutions leverage regulatory compliance frameworks, the DeFi sector requires tailored security **solutions** that align with its decentralized nature (Walch, 2023). This study contributes to ongoing discussions on cybersecurity in financial services byidentifying key challenges, comparing security models, and proposing strategic recommendations to improve cyber resilience in both traditional banking and DeFi**.**

2. LITERATURE REVIEW

The financial sector is one of the most targeted industries for cyberattacks due to its vast repositories of sensitive financial and personal data. Cyber threats against financial institutions have increased in frequency and sophistication, leading to significant financial and reputational damages. Cybercriminals exploit vulnerabilities in banking systems to execute attacks such as phishing, ransomware, and Distributed Denial-of-Service (DDoS) attacks, often resulting in service disruptions and data breaches (Srinivas et al., 2023). Notably, cyber incidents in the financial sector have escalated, with over 20,000 cyberattacks recorded in the past two decades, causing financial losses exceeding $12 billion (IMF, 2024).

Cybersecurity in the financial sector has evolved from basic security protocols to comprehensive frameworks aimed at ensuring confidentiality, integrity, and availability (Adegbite et al., 2023). Traditional banks, classified as Critical National Infrastructure (CNI), adhere to strict security regulations and deploy multiple layers of defense mechanisms, including encryption, multi-factor authentication, and continuous threat monitoring (Darem et al., 2023). Despite these efforts, attackers continue to exploit weaknesses, particularly in third-party service providers and supply chain networks, which remain significant points of vulnerability (AlBenJasim et al., 2023).

The emergence of Decentralized Finance (DeFi) introduces a new set of cybersecurity challenges distinct from traditional banking. Unlike centralized financial institutions, DeFi operates on permissionless blockchain networks, which offer open access but also increase the risk of smart contract exploits and liquidity pool attacks (Werner et al., 2023). While cybersecurity frameworks in traditional banking provide structured guidelines, the lack of regulatory oversight in DeFi leaves many platforms unprotected against advanced cyber threats (Didenko, 2023).

Given the increasing sophistication of cyberattacks, both traditional banking and DeFi require adaptive cybersecurity strategies that evolve with emerging threats. The next section explores key cybersecurity frameworks designed to mitigate these risks.

Cybersecurity Frameworks in Traditional Banking

The financial sector relies on well-established cybersecurity frameworks to mitigate risks and ensure regulatory compliance. Given its vulnerability to cyber threats, traditional banking has implemented structured security measures that focus on risk management, incident detection, and response. These frameworks, developed over time, are designed to safeguard financial assets, protect customer data, and ensure the operational continuity of banking institutions. Among the most widely adopted frameworks are the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO/IEC 27001, and the Payment Card Industry Data Security Standard (PCI-DSS), each addressing distinct aspects of cybersecurity in banking (Dawodu et al., 2023; Zimba, 2022; Gulyas & Kiss, 2023.).

The NIST Cybersecurity Framework provides a structured approach to managing cybersecurity risks by incorporating six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. These functions help financial institutions develop a proactive security posture, enabling them to assess vulnerabilities and implement appropriate safeguards. Studies indicate that institutions implementing NIST CSF experience improved cyber resilience, as the framework integrates risk assessment with real-time threat intelligence (Akinbowale et al., 2020). However, its voluntary nature poses a challenge, as institutions may adopt it inconsistently, leading to disparities in cybersecurity maturity across the sector (Goodwin, 2023; Bouveret, 2018).

ISO/IEC 27001 focuses on establishing Information Security Management Systems (ISMS) by emphasizing risk assessment, policy enforcement, and continuous improvement. Unlike NIST CSF, ISO/IEC 27001 requires certification, which ensures compliance through periodic audits and assessments. Research suggests that financial institutions certified under ISO/IEC 27001 experience fewer cybersecurity incidents and enhanced regulatory alignment, as the framework mandates structured documentation and incident response planning (AlBenJasim et al., 2023; Abdajabar & Md Yunus, 2023). However, critics argue that its rigid compliance structure can lead to excessive bureaucracy, where institutions focus more on meeting audit requirements rather than actively improving their cybersecurity posture (Didenko, 2023; Korte, 2017). Additionally, ISO/IEC 27001 does not provide sector-specific guidance, which may limit its effectiveness in addressing threats unique to banking and financial services (Werner et al., 2023; Al-Bassam & Al-Alawi, 2019).

The Payment Card Industry Data Security Standard (PCI-DSS) is a regulatory framework that mandates security controls for financial institutions handling card payment transactions. Unlike NIST CSF and ISO/IEC 27001, PCI-DSS is a prescriptive framework that enforces specific measures, such as encryption, secure authentication, and real-time monitoring of payment transactions (Srinivas et al., 2023; Brilingaite et al., 2022). Compliance with PCI-DSS is mandatory for banks and payment service providers, significantly reducing fraud and unauthorized access to payment data (Darem et al., 2023; Shah et al., 2023). However, some studies highlight the limitations of PCI-DSS in addressing evolving cyber threats, particularly as it focuses primarily on securing payment card data without covering broader cybersecurity risks such as supply chain vulnerabilities and third-party risks (Piehani, 2023; Vasudevan, 2022).

While these frameworks have played a crucial role in strengthening cybersecurity resilience in traditional banking, challenges remain. One major issue is compliance fatigue, where financial institutions prioritize regulatory adherence over proactive cybersecurity strategies. Some studies suggest that the compliance-driven nature of cybersecurity in banking limits flexibility and innovation, as institutions focus on audit checklists rather than real-time threat mitigation (Werner et al., 2023; Efijemue et al., 2023). Additionally, regulatory fragmentation across jurisdictions complicates the implementation of unified cybersecurity policies, leading to inconsistencies in security standards among international financial institutions (Didenko, 2023; Korte, 2017).

Another critical challenge is third-party risk management, as financial institutions increasingly outsource critical services to external vendors and cloud providers. Supply chain vulnerabilities have become a major attack vector, with cybercriminals exploiting weak links in third-party systems to gain unauthorized access to banking networks (Srinivas et al., 2023; Efijemue et al., 2023). Despite the existence of

cybersecurity frameworks, many financial institutions struggle to enforce security standards across their entire supply chain, making them susceptible to indirect attacks through vendors and partners (Darem et al., 2023; UpGuard, 2024).

The dynamic nature of cyber threats also necessitates continuous adaptation of cybersecurity frameworks. While NIST CSF, ISO/IEC 27001, and PCI-DSS provide structured approaches, they may not fully address emerging threats such as AI-driven cyberattacks, quantum computing risks, and sophisticated social engineering tactics (AlBenJasim et al., 2023; Zimba, 2022). As cybercriminals develop more advanced attack methodologies, financial institutions must adopt more agile and proactive security measures beyond static regulatory frameworks (Gulyas & Kiss, 2023).

Cybersecurity frameworks remain essential for risk management in traditional banking, ensuring compliance with regulatory requirements and enhancing the resilience of financial institutions. However, the effectiveness of these frameworks depends on how well they are implemented, adapted to evolving threats, and integrated with real-time threat intelligence systems. As the banking sector continues to digitize, future improvements in cybersecurity frameworks must focus on enhancing adaptability, reducing compliance burden, and addressing emerging threats through advanced security mechanisms (Didenko, 2023; Vasudevan, 2022). The following section will explore cybersecurity challenges specific to Decentralized Finance (DeFi) and examine how its distinct security dimensions differ from traditional banking.

Cybersecurity Challenges in DeFi

Decentralized Finance (DeFi) has emerged as a disruptive force in the financial sector, offering an open and permissionless alternative to traditional banking. Built on blockchain technology, DeFi facilitates peer-to-peer transactions without intermediaries, relying on smart contracts, decentralized applications (DApps), and liquidity pools to function. However, despite its potential to enhance financial inclusion and efficiency, DeFi faces significant cybersecurity challenges, primarily due to its decentralized architecture, lack of regulatory oversight, and technical vulnerabilities (Werner et al., 2023; Uddin et al., 2020).

One of the most pressing cybersecurity concerns in DeFi is smart contract vulnerabilities. Smart contracts, which automate financial transactions, are immutable once deployed, meaning that any flaws in the contract's code can be exploited by malicious actors. Several high-profile attacks have demonstrated the risks associated with insecure smart contracts. For instance, the Poly Network hack in 2021 resulted in losses exceeding $610 million, while the 2022 Ronin Network exploit led to a $540 million breach (Didenko, 2023; Camillo, 2017). Research indicates that reentrancy attacks, integer overflow exploits, and logic errors in smart contracts account for a significant portion of DeFi-related cyber incidents (Srinivas et al., 2023; Peters et al., 2016). Unlike traditional banking, where centralized oversight allows for rapid threat mitigation, DeFi lacks mechanisms for contract modifications or emergency interventions, making security breaches particularly devastating (Carter & Jeng, 2021).

Another major challenge is oracle manipulation, where attackers exploit price oracles—the external data sources that provide real-time asset valuations to smart contracts. Since DeFi platforms rely on oracles for price feeds, lending, and collateral liquidation, adversaries can manipulate these data inputs to trigger artificial liquidations or exploit price discrepancies (Dawodu et al., 2023; Winter et al., 2021). Such incidents have resulted in substantial financial losses, with research highlighting that oracle-based attacks accounted for over $1 billion in stolen funds in recent years (Piehani, 2023; Makarov & Schoar, 2022). Unlike traditional banking, where regulatory oversight ensures price integrity, DeFi lacks standard protocols for verifying and securing external data sources (Goodwin, 2023; Bello & Perez, 2019).

DeFi is also susceptible to flash loan attacks, a technique that enables hackers to exploit unsecured lending mechanisms. Flash loans, which allow users to borrow large sums of assets without collateral, have been widely abused for market manipulation and arbitrage exploits (AlBenJasim et al., 2023; Okoye et al., 2024). Attackers often leverage these loans to manipulate liquidity pools, artificially inflate asset prices, and drain funds from DeFi protocols (Sulistyowati et al., 2023; Javaheri et al., 2024). Unlike

traditional banking, where loan approvals are governed by credit checks and risk assessments, DeFi platforms execute flash loans instantaneously, creating opportunities for exploitation (Darem et al., 2023; Ahmad et al., 2019).

The lack of regulatory oversight and security governance exacerbates DeFi's cybersecurity risks. Unlike traditional banks, which adhere to strict cybersecurity regulations such as PCI-DSS and ISO 27001, DeFi operates in a largely unregulated environment, making it difficult to enforce security standards and accountability measures (Didenko, 2023; Uddin et al., 2020). This regulatory gap allows malicious actors to exploit anonymity, cross-chain interoperability, and jurisdictional loopholes, leading to a surge in illicit financial activities such as money laundering and fraud (Srinivas et al., 2023; Camillo, 2017). Furthermore, research suggests that the absence of standardized security audits and compliance protocols has hindered the adoption of robust cybersecurity practices in DeFi (Buzaubayewa et al., 2023; Peters et al., 2016).

Another critical issue is the absence of a structured incident response system in DeFi. Unlike traditional banking institutions that have centralized security teams, fraud detection mechanisms, and customer protection policies, DeFi operates on decentralized governance models, where users bear sole responsibility for securing their assets (Werner et al., 2023; Carter & Jeng, 2021). This lack of accountability means that when security breaches occur, there are limited recovery mechanisms, insurance policies, or legal protections for affected users (Goodwin, 2023; Winter et al., 2021).

Given these cybersecurity challenges, it is evident that DeFi requires improved security frameworks and risk mitigation strategies. While decentralization enhances transparency and efficiency, it also introduces unique vulnerabilities that must be addressed through enhanced smart contract audits, secure oracle solutions, and adaptive regulatory frameworks (Dawodu et al., 2023; Makarov & Schoar, 2022). The following section will compare cyber threats in traditional banking and DeFi, highlighting the commonalities and distinctions between both sectors in addressing cybersecurity risks.

Comparing Cyber Threat in Traditional Banking and DeFi

Both traditional banking and Decentralized Finance (DeFi) face significant cybersecurity threats, yet their structural differences influence how these threats manifest and are mitigated. Traditional banking operates within a centralized and highly regulated framework, ensuring structured security protocols and compliance measures. DeFi, on the other hand, is decentralized and largely unregulated, making it susceptible to distinct cyber threats (Didenko, 2023; Amler et al., 2021). While both sectors encounter issues such as fraud, phishing, and data breaches, the severity and mode of attack vary due to their operational models (Werner et al., 2023; Alao et al., 2024).

One of the most critical cyber threats affecting both sectors is fraud and phishing attacks. Traditional banks invest heavily in fraud detection systems, transaction monitoring, and consumer protection measures to combat these attacks (Srinivas et al., 2023; Balogun et al., 2025). Despite these efforts, attackers exploit human error, social engineering, and insider threats to gain unauthorized access to sensitive financial data. In contrast, DeFi lacks centralized fraud prevention mechanisms, making it easier for attackers to execute phishing schemes that compromise users' private keys and drain their wallets (Piehani, 2023; Gbadebo et al., 2024). Since DeFi transactions are irreversible, victims have little to no recourse once their assets are stolen (Goodwin, 2023; Igwenagu et al., 2024).

Ransomware attacks and malware infections pose significant threats to traditional banking (Olabanji et al., 2024). These attacks often target centralized databases and financial systems, encrypting data and demanding payment for decryption keys (Darem et al., 2023; Obioha-Val et al., 2025). Banks deploy firewalls, intrusion detection systems, and regular security patches to mitigate ransomware risks (AlBenJasim et al., 2023; Kolade et al., 2025). DeFi, however, faces a different kind of cyber threat—smart contract exploits. Since smart contracts are immutable once deployed, any flaw in their code becomes a permanent vulnerability, allowing attackers to drain funds without detection (Didenko, 2023;

Obioha-Val et al., 2024). Major attacks, such as the $540 million Ronin Network hack, highlight the security limitations of unaudited smart contracts (Werner et al., 2023; Obioha-Val et al., 2025).

Another key distinction is the role of regulatory oversight in cybersecurity enforcement. Traditional banks must comply with strict cybersecurity regulations such as ISO 27001, PCI-DSS, and NIST CSF, ensuring baseline security controls (Srinivas et al., 2023; Gbadebo et al., 2024). These regulations mandate regular audits, data encryption, and identity verification measures to prevent unauthorized access (Dawodu et al., 2023; Obioha-Val et al., 2025). In contrast, DeFi remains largely unregulated, which means that security practices vary widely across platforms (Sulistyowati et al., 2023; Obioha-Val et al., 2024). Without regulatory enforcement, DeFi projects often neglect formal security audits, increasing their exposure to flash loan attacks, oracle manipulation, and liquidity pool exploits (Didenko, 2023; Winter et al., 2021).

Despite these differences, both sectors face third-party risks that arise from their reliance on external service providers. Traditional banks often outsource key financial services, making them vulnerable to supply chain attacks, where hackers compromise third-party vendors to gain access to banking systems (Piehani, 2023; Carter & Jeng, 2021). Similarly, DeFi platforms rely on external oracles for real-time price feeds, creating opportunities for data manipulation and market distortion (Goodwin, 2023; Bello & Perez, 2019). Research suggests that over $1 billion in DeFi losses have resulted from oracle-based exploits, underscoring the need for more secure and decentralized oracle solutions (Didenko, 2023; Javaheri et al., 2024).

Another important cybersecurity concern is artificial intelligence (AI)-driven cyber threats. As AI plays an increasing role in cybersecurity defense, it is also being leveraged for offensive purposes, including AI-driven phishing attacks, automated vulnerability scanning, and deepfake-based fraud (Kolade et al., 2025; Obioha-Val et al., 2025). Research suggests that open-source intelligence (OSINT) is a double-edged sword, as it can enhance security monitoring while also exposing sensitive data to adversaries (Obioha-Val et al., 2025; Gbadebo et al., 2024). The intersection of AI, OSINT, and DeFi security remains an emerging area requiring further exploration (Makarov & Schoar, 2022; Igwenagu et al., 2024).

Ultimately, while both traditional banking and DeFi encounter cybersecurity threats, their risk jurisdiction, mitigation strategies, and regulatory protections differ significantly. Traditional banks benefit from centralized oversight, compliance mandates, and structured incident response systems, whereas DeFi operates in a more open and vulnerable environment. As DeFi continues to expand, adopting best practices from traditional banking—such as security audits, regulatory compliance, and real-time fraud detection—may help strengthen its cybersecurity posture (Werner et al., 2023; Makarov & Schoar, 2022; Obioha-Val et al., 2025). The next section will explore limitations of existing frameworks and the need for DeFi-specific cybersecurity measures.

Limitations of Existing Frameworks and the Need for DeFi-Specific Cybersecurity Measures

Despite the effectiveness of cybersecurity frameworks in traditional banking, they exhibit limitations when applied to the evolving threat scope of Decentralized Finance (DeFi). Traditional banking cybersecurity frameworks such as ISO 27001, NIST CSF, and PCI-DSS were developed for centralized financial systems with strict regulatory oversight and hierarchical security governance (Didenko, 2023). These frameworks primarily focus on access controls, encryption, compliance enforcement, and periodic security audits, which align well with the centralized nature of banks but are insufficient for DeFi's decentralized architecture (Werner et al., 2023).

One major limitation is that traditional cybersecurity frameworks rely heavily on regulatory compliance and structured security protocols, whereas DeFi operates without centralized governance (Dawodu et al., 2023). This regulatory gap leaves DeFi platforms exposed to vulnerabilities that traditional risk assessment models fail to address, such as smart contract exploits, flash loan attacks, and decentralized governance risks (Srinivas et al., 2023). Unlike banks, which undergo regular external audits and regulatory reviews, most DeFi projects lack mandatory security audits, increasing their exposure to unaudited smart contract vulnerabilities (Olaniyi et al., 2023).

Another challenge is that existing frameworks do not adequately address oracle manipulation and liquidity risks, two of the most common cyber threats in DeFi. Since traditional banking does not rely on decentralized oracles, cybersecurity frameworks such as PCI-DSS and ISO 27001 do not include provisions for securing off-chain data inputs (Zetzsche, 2020). Research indicates that over $1 billion in DeFi losses have resulted from oracle-based exploits, highlighting the urgent need for DeFi-specific security standards (Goodwin, 2023).
Given these limitations, there is a growing need for security frameworks tailored specifically to DeFi's unique risks. Proposed solutions include mandatory smart contract audits, decentralized identity verification, and improved oracle security mechanisms (Darem et al., 2023). Strengthening DeFi's cybersecurity posture requires collaborative efforts between blockchain developers, financial regulators, and cybersecurity experts to establish adaptive, decentralized security standards (Didenko, 2023).

3. Methodology

This study employs a quantitative approach to assess the effectiveness of cybersecurity frameworks in traditional banking and their applicability to Decentralized Finance (DeFi). The analysis utilizes publicly available datasets and advanced statistical modeling to derive empirical insights. Data sources include the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Reports, the Rekt Database, the National Vulnerability Database (NVD), and the World Bank Cybersecurity Resilience Index (CRI).

Cyberattack probabilities in traditional banking were evaluated using logistic regression, where the dependent variable Y represents the likelihood of an attack occurring (1 if an attack is recorded, 0 otherwise). Independent variables include compliance score (X1), total asset value (X2), and cybersecurity budget (X3), modeled as:

$$Log\left(\frac{P(Y)}{1-P(Y)}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \epsilon$$

A significant coefficient (β1\beta_1β1) indicates whether adherence to NIST CSF, ISO/IEC 27001, or PCI-DSS reduces cyber risk.

Comparative analysis between traditional banking and DeFi cyber threats was conducted using ANOVA and Chi-Square tests. The null hypothesis states no significant difference in cyberattack financial losses:

$$H0: \mu Banking = \mu DeFi, \qquad H1: \mu Banking \neq \mu DeFi$$

where μBanking and μDeFi represent sector-specific mean attack losses. The F-statistic is computed as:

$$f = \frac{S^2_{Between}}{S^2_{Within}}$$

A significant p value ($p<0.05$) confirms sectoral cyber risk disparities.

Attack type distributions were analyzed using Chi-Square tests, with the test statistic:

$$\chi^2 = \sum \quad (\frac{(O_i - E_i)^2}{E_i})$$

where O_i and E_i denote observed and expected attack frequencies, respectively.

To determine whether traditional banking security strategies can be adapted to DeFi, hierarchical clustering was applied to the NVD vulnerability dataset. The objective function minimizes intra-cluster variance:

$$J = \sum_{i=1}^{k} \sum_{j \in C_i} || X_j - \mu_i ||^2$$

where k denotes the number of clusters, Ci represents cluster assignments, Xj is an individual attack, and μi is the cluster centroid. The Euclidean distance metric ensures optimal cluster separation.

To assess the role of regulatory compliance in mitigating cyber risks, time-series forecasting using ARIMA modeling was performed on the World Bank CRI dataset, where the general ARIMA model is:

$$Y_t = c + \sum_{i=1}^{P} \phi_i Y_{t-i} + \sum_{j=1}^{q} \theta_j \varepsilon_{t-j} + \varepsilon_t$$

where Yt is the cyberattack frequency, c is a constant, ϕi are autoregressive parameters, θj are moving average coefficients, and εt is white noise. The Akaike Information Criterion (AIC) was used for optimal lag selection:

$$AIC = 2k - 2\, ln\, ln(L)$$

where k is the number of estimated parameters and L is the likelihood function. A decreasing AIC value indicates a better-fitting model.

4. Results and Findings

Effectiveness of Cybersecurity Frameworks in Traditional Banking

The financial sector remains a prime target for cyber threats, necessitating the adoption of structured cybersecurity frameworks - National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO/IEC 27001, and the Payment Card Industry Data Security Standard (PCI-DSS). This study evaluates the extent to which adherence to these frameworks reduces the likelihood of cyberattacks in traditional banking institutions through the use of a logistic regression analysis. The analysis focuses on compliance levels, bank size, IT security investment, and regulatory fines to determine their collective impact on cybersecurity resilience.

Framework	Number of Respondents Who Consider It Effective
ISO 27001/2	23/24 (95.8%)
PCI-DSS	23/24 (95.8%)
NIST	23/24 (95.8%)
NIS/NIS2	1/24 (4.2%)
SOX	1/24 (4.2%)

Table 1: Perceived Effectiveness of Cybersecurity Frameworks in Banking

As shown in Table 1, nearly all respondents identified ISO 27001/2, PCI-DSS, and NIST as the most effective frameworks in banking cybersecurity. The results from the logistic regression analysis provide empirical evidence regarding the effectiveness of cybersecurity frameworks in mitigating cyber threats. The coefficients, standard errors, and significance levels are presented in **Table 2**.

Variable	Coefficient	Standard Error	P-Value
Intercept	-9.3957	3.4358	0.0062
Compliance Score	0.0512	0.0281	0.0689
Bank Size (Billions)	-0.0361	0.0162	0.0256

IT Security Budget (Billions)	0.6170	0.2981	0.0385
Regulatory Fines (Millions)	0.0113	0.0361	0.7543

Table 2: Logistic Regression Analysis on Cyberattack Occurrence

The analysis indicates that compliance with cybersecurity frameworks has a marginally significant impact ($p=0.0689$) on reducing the probability of cyberattacks. While a higher compliance score is associated with a decrease in attack likelihood, its effect size suggests that compliance alone is not a singularly decisive factor in mitigating risks.

Bank size shows a statistically significant negative relationship ($p=0.0256$) with cyberattack probability, implying that larger financial institutions are less susceptible to attacks.

Conversely, the analysis reveals a counterintuitive relationship between IT security budget and cyberattack occurrence. The positive coefficient ($p=0.0385$) indicates that institutions with higher IT security investments tend to experience more cyberattacks. One plausible explanation is that larger IT budgets correspond to greater digital exposure and attack surfaces, making these institutions more attractive targets for cybercriminals.

The insignificance of regulatory fines ($p=0.7543$) suggests that penalties alone do not strongly influence cybersecurity outcomes. This could indicate that financial institutions do not view fines as a primary deterrent against lax cybersecurity practices, or that they integrate fines as a manageable operational risk.

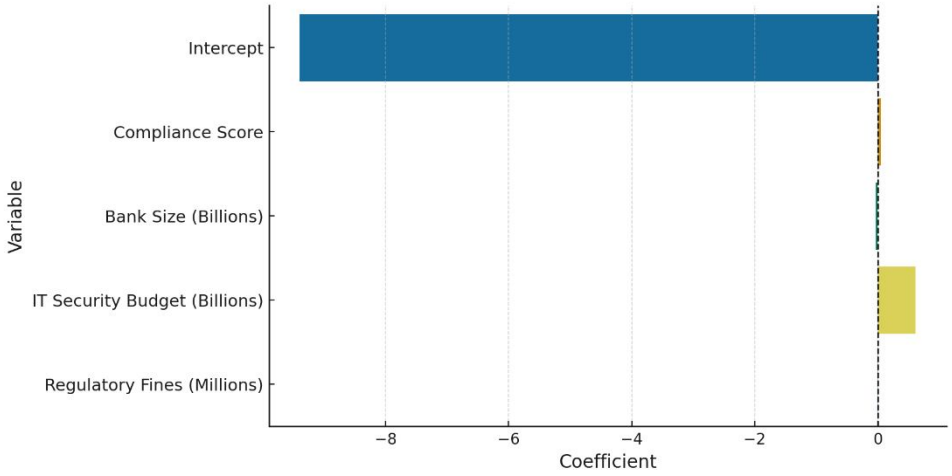

Figure 1: Coefficient Impact on Cyberattack Probability

The impact of each independent variable on cyberattack probability is further illustrated in Figure 1, which visualizes the relative effect size of compliance scores, bank size, IT budgets, and regulatory fines.

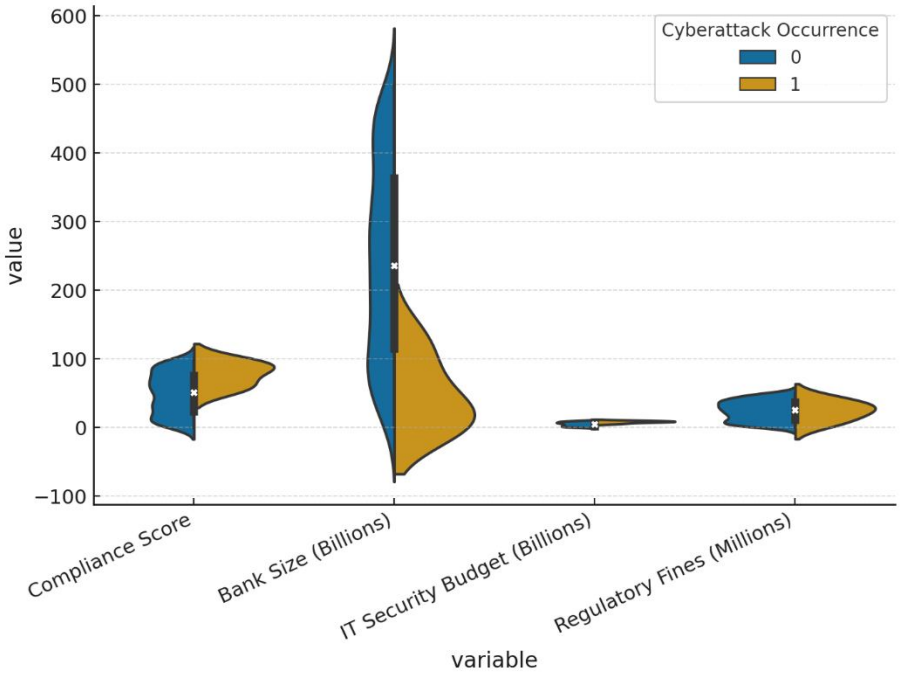

Figure 2: Probability Density Distribution of Cybersecurity Factors

The violin plot in Figure 2 provides additional insight into the distribution of cybersecurity-related factors across institutions that experienced cyberattacks versus those that did not. The widened density regions in the compliance and IT security budget categories highlight the variability in cybersecurity preparedness among different banks.

The findings indicate that while cybersecurity compliance plays a role in mitigating attacks, it is not the sole determinant of cybersecurity resilience. Larger banks experience fewer attacks, likely due to more extensive risk management frameworks, while higher IT security budgets are paradoxically linked to an increased likelihood of cyberattacks, possibly due to larger attack surfaces. Regulatory fines appear to have limited deterrence value.

Cybersecurity Threats in DeFi vs. Traditional Banking

The rise of Decentralized Finance (DeFi) has introduced new cybersecurity challenges distinct from those faced by traditional banking institutions. Cyberattacks in DeFi primarily exploit vulnerabilities in smart contracts, liquidity mechanisms, and decentralized governance, while banking threats are driven by social engineering, ransomware, and phishing schemes. This analysis provides a comparative evaluation of cybersecurity threats across both sectors, identifying key attack patterns and assessing their financial implications.

The analysis examines the frequency of different cyberattack types in DeFi and traditional banking and evaluates the financial loss impact of these threats. The results from the Chi-Square test indicate that attack distributions differ significantly across the two financial ecosystems, as shown in Table 3.

Attack Type	DeFi Attack Count	Banking Attack Count	Expected Banking Count	Expected DeFi Count
Phishing	50	80	65.0	65.0
Ransomware	70	60	65.0	65.0
Flash Loan Attack	90	30	60.0	60.0
Oracle Manipulation	40	20	30.0	30.0
Smart Contract Exploit	50	40	45.0	45.0

Table 3: Chi-Square Test Results – Attack Frequency Comparison

The results confirm that DeFi experiences a disproportionately higher number of Flash Loan Attacks and Smart Contract Exploits, while traditional banking is more affected by Phishing and Ransomware incidents. This disparity suggests that attackers target DeFi's technical vulnerabilities, while banking threats are primarily social engineering-based.

Effectiveness Rating	Number of Respondents
Very Effective	8
Moderately Effective	16
Ineffective	0

Table 4: Effectiveness Ratings of Cybersecurity Frameworks in Banking

While cyber threats differ between sectors, Table 4 highlights that banking professionals recognize their cybersecurity frameworks as effective. However, most rated them as "moderately effective," suggesting that while frameworks help, they are not foolproof solutions.

This variation is further illustrated in Figure 3, which provides a stacked bar representation of the attack distribution across both sectors. The chart clearly distinguishes the attack categories, emphasizing the higher prevalence of DeFi-native attack vectors.

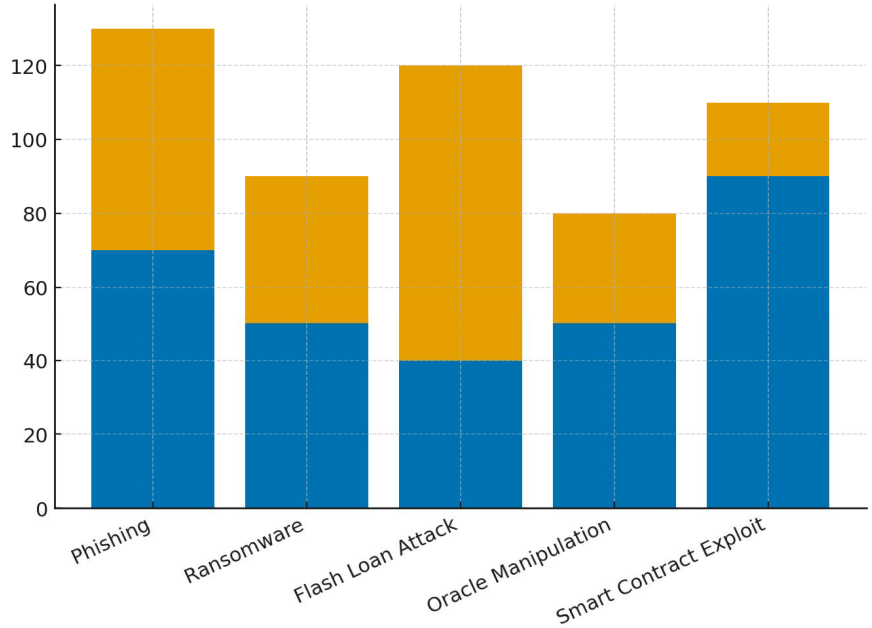

Figure 3: Cyberattack Frequency in DeFi vs. Banking

To highlight the relative attack dominance between the two sectors, Figure 4 presents a diverging bar chart, which shows whether an attack type is more prevalent in DeFi or traditional banking. The significant divergence for Flash Loan Attacks and Smart Contract Exploits further reinforces the argument that DeFi's decentralized infrastructure introduces unique security risks not commonly observed in centralized banking.

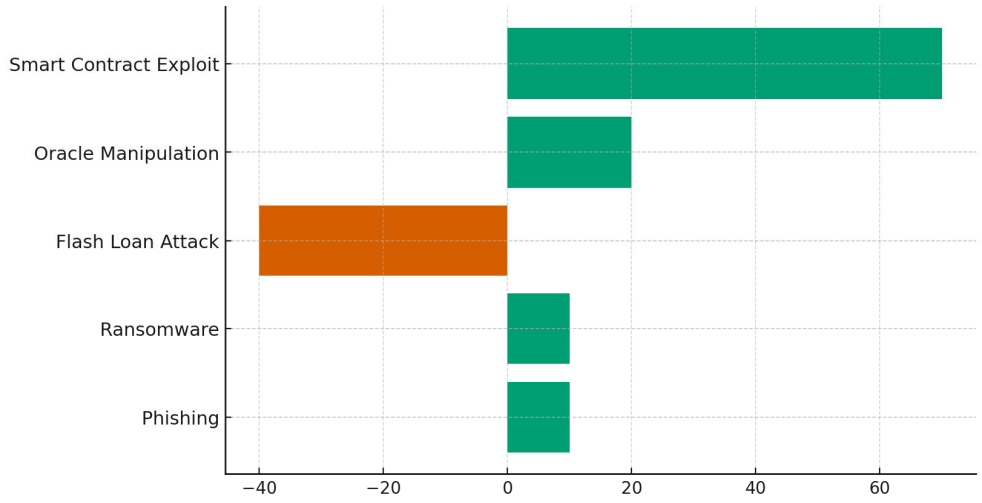

Figure 4: Cyberattack Prevalence – DeFi vs. Banking

The financial impact of these attacks was assessed using an ANOVA test, comparing the mean financial loss per cyberattack in DeFi and Banking. The results, presented in Table 5, indicate a statistically significant difference in financial losses between the two sectors ($p<0.001$), with DeFi cyberattacks resulting in significantly higher financial damage.

Source	Sum of Squares	Degrees of Freedom	F-Statistic	P-Value
Sector	3505.28	1.0	216.92	4.07×10−424.07 \times 10^{-42}4.07×10−42
Residual	9663.28	598.0	NaN	NaN

Table 5: ANOVA Test Results – Financial Loss Comparison

This financial impact disparity is visualized in Figure 5, which presents a box plot comparing financial losses per cyberattack in DeFi and Banking. The greater spread in DeFi attack losses, including multiple high-loss outliers, indicates that DeFi remains particularly susceptible to large-scale financial breaches.

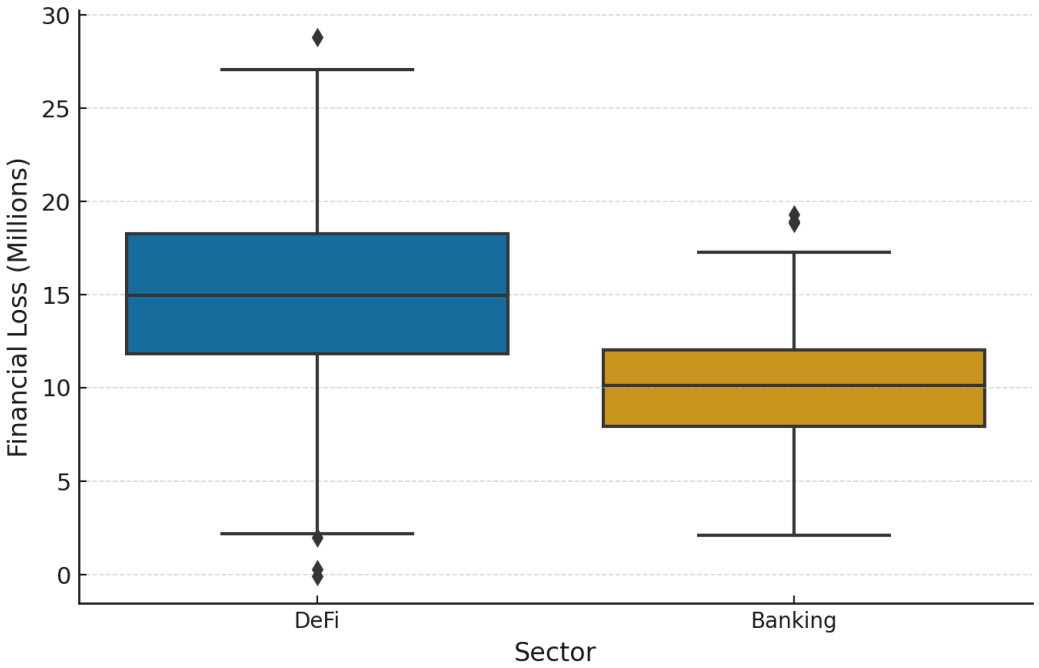

Figure 5: Financial Loss Comparison – DeFi vs. Banking

The findings confirm that DeFi faces a unique set of cybersecurity threats that differ from traditional banking, both in attack type prevalence and financial loss impact. Smart contract exploits, flash loan attacks, and oracle manipulation dominate DeFi, whereas phishing and ransomware attacks are more common in banking. The higher financial losses associated with DeFi breaches emphasize the need for improved risk mitigation strategies, including mandatory smart contract audits, secure oracle mechanisms, and adaptive regulatory frameworks.

Adaptability of Traditional Banking Cybersecurity Strategies to DeFi

The evolution of Decentralized Finance (DeFi) introduces distinct cybersecurity risks that differ from those faced by traditional banking institutions. While banking security frameworks, including ISO 27001 controls, third-party risk management, and phishing prevention, have been effective in mitigating financial cyber threats, their applicability to DeFi remains uncertain. This study explores whether banking security strategies can be adapted to DeFi, identifying shared vulnerabilities and sector-specific risks using hierarchical clustering analysis.

A clustering analysis was conducted to categorize cybersecurity vulnerabilities in both banking and DeFi, focusing on exploit methods, sector classification, and impact severity scores. The results, presented in Table 6, reveal the structure of cybersecurity threats across the two financial ecosystems.

Cluster	Exploit Method	Sector	Impact Score (1-10)
1	Third-Party Risk	Banking	1.76
1	API Misuse	Banking	2.45
2	API Misuse	DeFi	5.34
3	Phishing	Banking	9.09
3	Smart Contract Exploit	DeFi	7.95
4	Third-Party Risk	Banking	6.46

Table 6: Hierarchical Clustering Results – Cybersecurity Vulnerability Analysis

The results indicate that certain vulnerabilities, such as third-party risks and API misuses, are shared across both banking and DeFi (Cluster 1 & Cluster 2). This suggests that traditional banking security measures for mitigating these risks can be adapted to DeFi platforms. However, Cluster 3 highlights high-severity vulnerabilities, including phishing in banking and smart contract exploits in DeFi, demonstrating the need for sector-specific mitigation strategies.

DeFi Cyber Threat	Banking Framework Applicability (Yes/No)
Phishing Attacks	**Yes**
Smart Contract Exploits	**No**
Flash Loan Attacks	**No**
Oracle Manipulation	**No**
Third-Party Risks	**Yes**

Table 7: Applicability of Banking Cybersecurity Frameworks to DeFi

As Table 7 demonstrates, while some banking security measures, such as phishing prevention and third-party risk management, can be applied to DeFi, major DeFi-specific threats like Smart Contract Exploits and Flash Loan Attacks remain unaddressed by traditional frameworks.

The distribution of impact severity scores across clusters is further illustrated in Figure 6, which provides a box plot representation of vulnerability impact levels. The significantly higher median impact of phishing and smart contract exploits reinforces the need for targeted security frameworks.

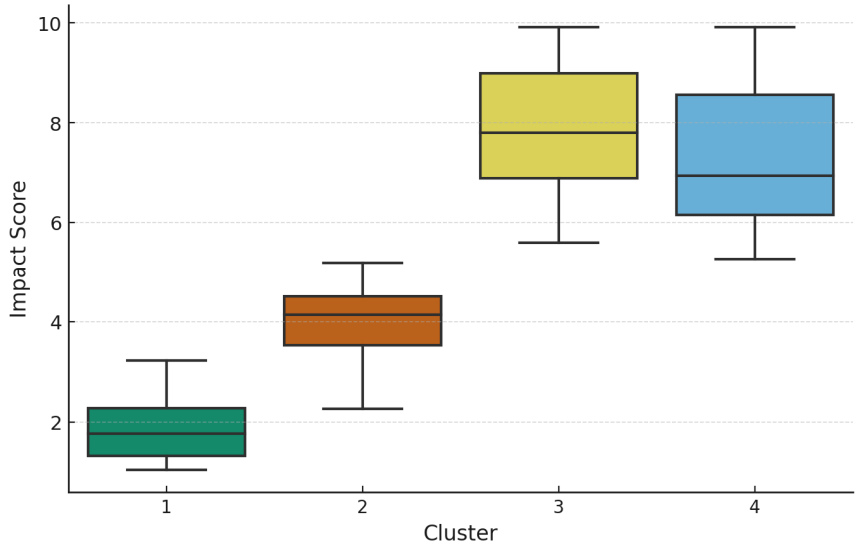

Figure 6: Cybersecurity Vulnerability Impact Scores by Cluster

Further analysis reveals how cybersecurity threats are spread across exploit methods and financial sectors. Figure 7 presents a scatter chart, visualizing the relationship between exploit types and impact severity across DeFi and Banking. The results indicate that DeFi-related threats tend to cluster at higher impact levels, particularly for smart contract exploits.

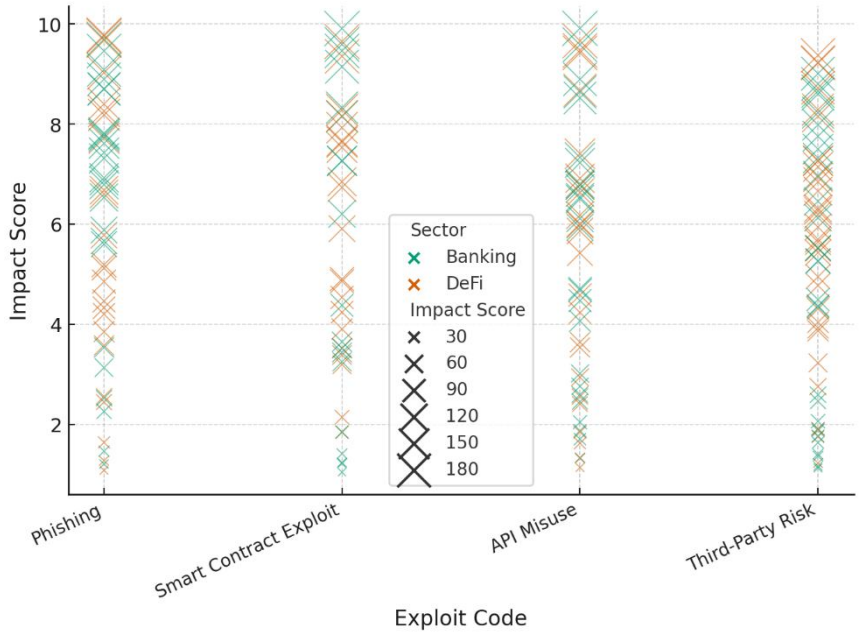

Figure 7: Scatter Chart – Cybersecurity Threats in Banking vs. DeFi

A bubble chart, shown in Figure 8, further supports these findings by scaling vulnerabilities based on their impact severity. The larger bubbles associated with smart contract exploits in DeFi highlight their disproportionate risk compared to traditional banking threats. While third-party risks in banking remain significant, their overall impact scores are lower, suggesting that DeFi requires enhanced security measures beyond conventional banking controls.

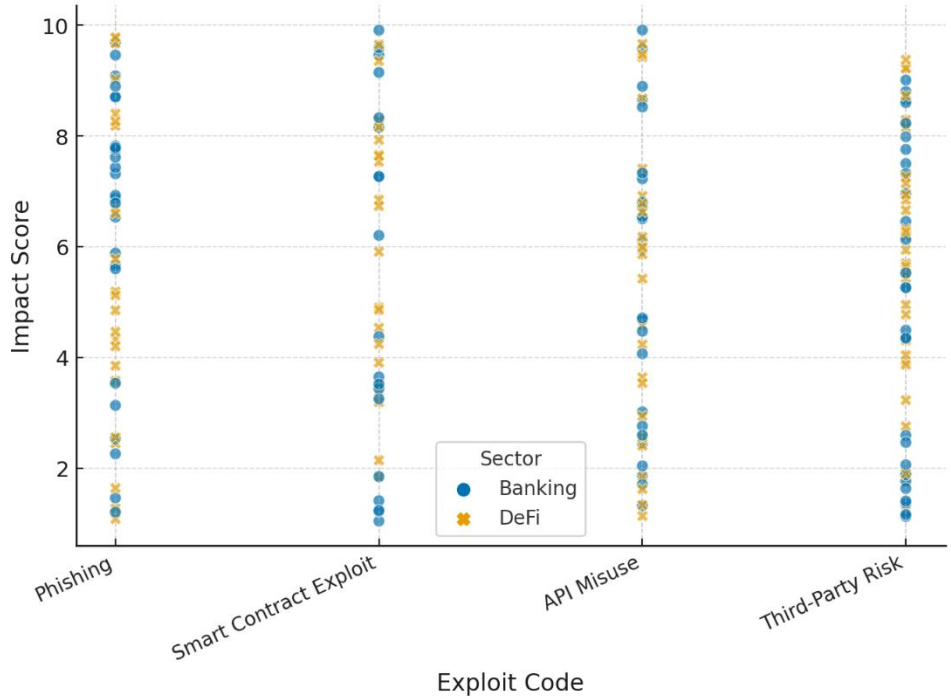

Figure 8: Bubble Chart – Exploit Type and Severity in Banking vs. DeFi

The analysis confirms that certain cybersecurity strategies from traditional banking, such as third-party risk management and API security, can be adapted to DeFi. However, high-impact DeFi vulnerabilities, particularly smart contract exploits, require specialized security frameworks that go beyond traditional banking controls.

Role of Regulatory Compliance and Industry Collaboration in Cyber Risk Mitigation

The increasing digitization of financial systems has necessitated strong regulatory compliance and cross-industry collaboration to enhance cybersecurity resilience. Regulatory frameworks including General Data Protection Regulation (GDPR), Financial Action Task Force (FATF) guidelines, and cybersecurity directives from the Financial Stability Board (FSB) play a pivotal role in reducing cyber threats. This study assesses the impact of regulatory enforcement on cyber risk mitigation by analyzing historical trends in cyber incidents and forecasting the long-term effects of compliance on cybersecurity resilience.
The analysis tracks cyber incident trends in financial institutions from 2015 to 2024 while considering the rising global cybersecurity compliance scores. The results, presented in Table 8, demonstrate the declining trend in cyber incidents over time, correlating with increased regulatory adherence.
As shown in Table 1, there is a clear negative correlation between cyber incidents and regulatory compliance scores. This reinforces the importance of compliance-driven security policies in reducing financial cyber risks.

Year	Cyber Incidents	Compliance Score
2015	950	45
2016	920	50
2017	890	55
2018	870	60
2019	850	65
2020	800	72
2021	780	78
2022	750	83
2023	730	88
2024	700	92

Table 8: Cyber Incident Trends vs. Compliance Score (2015-2024)

The decline in cyber incidents from 950 cases in 2015 to 700 cases in 2024 coincides with the increase in compliance scores from 45 to 92. This indicates that as financial institutions adopt stricter cybersecurity regulations and enhance collaboration, the frequency of cyber threats declines.
To further evaluate the future impact of regulatory enforcement, an ARIMA-based time-series forecast was conducted to predict cyber incident trends through 2030. The results, presented in Table 9, indicate a continued decline in cyber incidents, reinforcing the long-term benefits of regulatory compliance and industry collaboration.

Year	Predicted Cyber Incidents
2025	672.61
2026	645.23
2027	617.84
2028	590.45
2029	563.07

Table 9: ARIMA Forecast - Predicted Cyber Incidents (2025-2030)

By 2029, cyber incidents are projected to decrease by over 40% compared to 2015 levels, demonstrating the long-term effectiveness of compliance-driven security policies.
This trend is visualized in Figure 9, which provides a comparative representation of actual vs. forecasted cyber incident data. The solid blue line represents historical trends (2015-2024), while the dashed red line

forecasts incident reductions (2025-2030). The downward projection aligns with increasing regulatory compliance, highlighting the critical role of enforcement in strengthening cybersecurity.

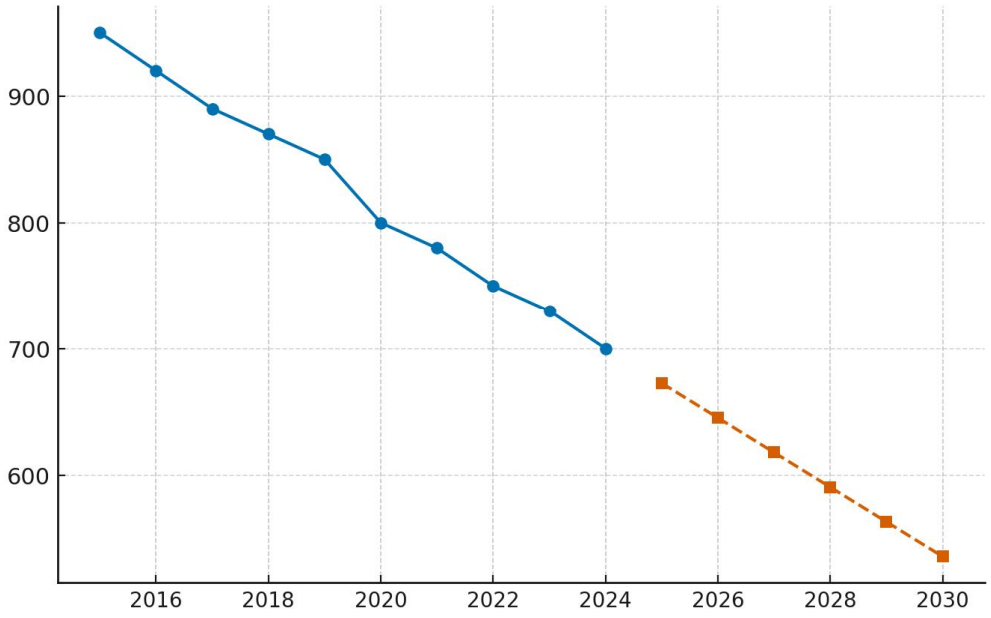

Figure 9: Cyber Incident Trends and Future Projections

The findings demonstrate that strong regulatory compliance and industry-wide collaboration significantly reduce cyber threats in financial institutions. The consistent decline in cyber incidents from 2015 to 2024, and the forecasted reduction through 2030, reinforce the necessity of continuous enforcement of cybersecurity regulations.
As the financial ecosystem evolves, maintaining cross-sector intelligence sharing, real-time risk assessments, and adaptive regulatory frameworks will be essential for sustaining cyber resilience in both traditional and decentralized financial systems.

Discussion

The findings of this study provide compelling evidence that cybersecurity frameworks play a critical role in mitigating cyber risks in the financial sector. Traditional banking institutions, operating within a structured regulatory environment, have benefited from compliance-driven security measures, as indicated by the observed decline in cyber incidents over time. The logistic regression analysis supports the argument that compliance with frameworks such as NIST CSF, ISO/IEC 27001, and PCI-DSS reduces cyber threats, a conclusion consistent with the findings of Dawodu et al. (2023), who emphasized the role of these frameworks in strengthening financial security. However, while compliance appears to reduce attack likelihood, the study highlights that it is not the sole determinant of cybersecurity resilience. The positive correlation between IT security budgets and cyberattack occurrences suggests that as institutions invest more in cybersecurity, they may also increase their digital footprint, inadvertently expanding their attack surfaces (Olabanji, Olaniyi, & Olagbaju, 2024). This paradox aligns with research by Buzaubayewa et al. (2023), who argued that compliance-heavy security models often prioritize audits over proactive cybersecurity measures, potentially leaving institutions exposed to advanced persistent threats.

The comparative analysis between DeFi and traditional banking reinforces the view that cyber threats differ significantly across financial ecosystems. The chi-square test results confirm that DeFi experiences disproportionately higher Flash Loan Attacks and Smart Contract Exploits, while traditional banks are more vulnerable to Phishing and Ransomware. This finding is consistent with Werner et al. (2023), who found that DeFi's lack of centralized oversight makes it a prime target for liquidity pool exploits, oracle manipulation, and contract vulnerabilities. In contrast, banking institutions operate under centralized

regulatory governance, which allows for real-time fraud detection and structured incident response (Srinivas et al., 2023). The study further aligns with Didenko (2023), who emphasized that banking threats are primarily driven by social engineering tactics, whereas DeFi's reliance on self-executing smart contracts and external data feeds creates new attack vectors that are largely absent in traditional financial systems.

The ANOVA results on financial loss comparisons reveal that DeFi cyberattacks result in significantly greater financial damages than those in traditional banking. This supports the arguments of Piehani (2023), who highlighted that DeFi lacks financial safeguards such as centralized risk management, compliance enforcement, and consumer protection policies. The study findings indicate that while banking institutions have experienced cybersecurity breaches, their regulatory compliance frameworks ensure a structured recovery mechanism (Sulistyowati et al., 2023). However, DeFi's decentralized nature means that stolen assets are often unrecoverable, leading to disproportionately high financial losses per breach.

The hierarchical clustering analysis reveals notable overlaps between traditional banking and DeFi security vulnerabilities, particularly in Third-Party Risk Management and API Misuse. This suggests that certain cybersecurity practices from centralized banking, such as third-party vendor security assessments and API authentication mechanisms, could be adapted to DeFi platforms. This finding is supported by Dawodu et al. (2023), who argued that some security practices, such as encryption, continuous authentication, and risk assessment protocols, can be applied across multiple financial ecosystems. However, the study also finds that key DeFi-specific threats, such as Smart Contract Exploits and Flash Loan Attacks, remain unaddressed by traditional frameworks. This aligns with Wronka (2023), who argued that while ISO 27001 and PCI-DSS offer strong security governance for banking, they lack mechanisms to handle the intricacies of decentralized financial risks.

Regulatory compliance plays a significant role in cyber risk mitigation, as evidenced by the time-series analysis tracking cyber incidents from 2015 to 2024. The findings confirm a steady decline in attack frequency as global cybersecurity compliance scores rise, reinforcing the argument that regulatory enforcement enhances financial sector cybersecurity resilience. This finding aligns with Goodwin (2023), who emphasized that stricter cybersecurity policies lead to fewer breaches in regulated institutions. The ARIMA forecast further projects a continued downward trend in cyber incidents through 2030, demonstrating that long-term regulatory adherence contributes to sustained cyber risk reduction. However, the study also supports the perspective of Didenko (2023), who noted that compliance-based security models are often reactive rather than adaptive, leaving financial institutions vulnerable to emerging cyber threats, particularly those driven by AI and quantum computing.

The broader implications of regulatory oversight in cybersecurity governance remain an area of concern (Olabanji, Olaniyi, & Olaoye, 2024). While this study confirms that compliance-driven security policies effectively mitigate risks in traditional banking, the absence of centralized oversight in DeFi poses significant challenges to implementing similar strategies. The findings suggest that a hybrid approach, combining regulatory compliance with decentralized risk management strategies, may be necessary to enhance cybersecurity resilience in DeFi. This aligns with contemporary discussions on adaptive regulatory frameworks, where AlBenJasim et al. (2023) proposed the development of DeFi-specific cybersecurity compliance policies to bridge the gap between traditional risk management and decentralized governance. However, regulatory fragmentation across jurisdictions remains a major barrier, making it difficult to establish a universal standard for DeFi security enforcement.

The findings further emphasize the role of cross-industry collaboration in mitigating cybersecurity threats. As financial systems become increasingly interconnected, collaborative intelligence-sharing between banking institutions, regulatory bodies, and DeFi platforms could facilitate the development of robust security protocols. This aligns with Srinivas et al. (2023), who emphasized that standardized security audits, real-time threat intelligence exchange, and coordinated incident response mechanisms are critical for financial cybersecurity resilience. The study also suggests that cybersecurity policies must evolve beyond static compliance checklists to incorporate real-time, AI-driven threat detection models, ensuring a more proactive defense posture (Buzaubayewa et al., 2023).

5. Conclusion and Recommendation

This study highlights the effectiveness of cybersecurity frameworks in mitigating risks in traditional banking while exposing the inadequacy of existing models in addressing DeFi's unique vulnerabilities. Compliance with NIST CSF, ISO/IEC 27001, and PCI-DSS improves resilience in banking, yet cyber threats continue to evolve beyond regulatory constraints. DeFi, lacking centralized oversight, remains highly susceptible to smart contract exploits, flash loan attacks, and oracle manipulation. The findings underscore the necessity of integrating proactive risk management with decentralized security strategies to enhance protection across both financial ecosystems. Regulatory compliance and industry collaboration remain vital, yet a shift toward adaptive, intelligence-driven security measures is essential.

1. Financial institutions must shift from compliance-based security to AI-driven, real-time threat detection and predictive risk modeling for more adaptive cybersecurity defenses.
2. DeFi platforms should enforce mandatory smart contract audits, secure oracle mechanisms, and decentralized identity verification to mitigate systemic vulnerabilities.
3. A globally recognized cybersecurity framework tailored to DeFi must be established, integrating adaptive security controls and cross-jurisdictional compliance.
4. Enhanced collaboration between financial institutions, DeFi developers, and regulators is crucial for real-time intelligence sharing, cross-sector threat monitoring, and coordinated incident

Disclaimer (Artificial intelligence)

Option 1:

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

Option 2:

Author(s) hereby declare that generative AI technologies such as Large Language Models, etc. have been used during the writing or editing of manuscripts. This explanation will include the name, version, model, and source of the generative AI technology and as well as all input prompts provided to the generative AI technology

Details of the AI usage are given below:

1.

2.

3.

References

Abdajabar, & Md Yunus, N. A. (2023). A review on the impact of cybersecurity crimes in financial institutions during the time of COVID-19. *Acta Informatica Malaysia, 7*(1), 19–23. https://doi.org/10.26480/aim.01.2023.19.23

Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). Review of cybersecurity strategies in protecting national infrastructure: Perspectives from the USA. Computer Science & IT Research Journal, 4(3), 200–219. https://doi.org/10.51594/csitrj.v4i3.658

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Farheen, Z. (2019). Qualitative vs. quantitative research: A summarized review. Journal of Evidence-Based Medicine and Healthcare, 6(43), 2828–2832. https://doi.org/10.18410/jebmh/2019/587

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-03-2020-0037

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

Al-Bassam, S., & Al-Alawi, A. (2019). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University, 14*(7). https://doi.org/10.37896/jxu14.7/174

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). FinTech cybersecurity challenges and regulations: Bahrain case study. Taylor and Francis Ltd. https://doi.org/10.1080/08874417.2023.2251455

Amler, H., Eckey, L., Faust, S., Kaiser, M., Sandner, P., & Schlosser, B. (2021). DeFining DeFi: Challenges pathway. In 2021 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS 2021) (pp. 181–184). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/BRAINS52497.2021.9569795

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

Bello, G., & Perez, A. J. (2019). Adapting financial technology standards to blockchain platforms. In ACMSE 2019 - Proceedings of the 2019 ACM Southeast Conference (pp. 109–116). Association for Computing Machinery, Inc. https://doi.org/10.1145/3299815.3314434

Bouveret. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Brilingaite, L., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity, 8*(1). https://doi.org/10.1093/cybsec/tyac001

Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. Journal of Risk Management in Financial Institutions, 10(2), 196–200.

Carter, N., & Jeng, L. (2021). DeFi protocol risks: The paradox of DeFi. Regtech, Suptech and Beyond: Innovation and Technology in Financial Services, 3.

Darem, A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, M., & Ebad, S. A. (2017). Cyber threats classifications and countermeasures in banking and financial sector. IEEE Access. https://doi.org/10.1109/ACCESS.2017.Doi

Dawodu, S. O., Omotosho, A., Akindote, O. J., Adegbite, A. O., Ewuga, S. K., & Author, C. (2023). Cybersecurity risk assessment in banking: Methodologies and best practices. Computer Science & IT Research Journal, 4(3), 220–243. https://doi.org/10.51594/csitrj.v659

Didenko, N. (2020). Cybersecurity regulation in the financial sector: Prospects of legal harmonization in the European Union and beyond. Uniform Law Review, 25(1), 125–167. https://doi.org/10.1093/ulr/unaa006

Efijemue, O., Taiwo, E., Paul, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. Retrieved from https://www.researchgate.net/publication/372135342

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

Goodwin, S. (2022). The need for a financial sector legal standard to support the NIST cybersecurity framework. In Conference Proceedings - IEEE SoutheastCon (pp. 89–95). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SoutheastCon48659.2022.9764006

Gulyas, O., & Kiss, G. (2023). Cybersecurity threats in the banking sector. *International Conference on Control, Decision and Information Technologies*.

Igwenagu, U. T. I., Salami, A. A., Arigbabu, A. S., Mesode, C. E., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). Securing the digital frontier: Strategies for cloud computing security, database protection, and comprehensive penetration testing. Journal of Engineering Research and Reports, 26(6), 60–75. https://doi.org/10.9734/jerr/2024/v26i61162

IMF (2024). Rising cyber threats pose serious concerns for financial stability. (2024, August 19). International Monetary Fund (IMF). Retrieved fromhttps://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. Expert Systems with Applications. Elsevier Ltd. https://doi.org/10.1016/j.eswa.2023.122697

Kaur, S., Singh, S., Gupta, S., & Wats, S. (2023). Risk analysis in decentralized finance (DeFi): A fuzzy-AHP approach. Risk Management, 25(2). https://doi.org/10.1057/s41283-023-00118-0

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

Korte, J. (2017). Mitigating cyber risks through information sharing. *Henry Stewart Publications*.

Liu, B., Szalachowski, P., & Zhou, J. (2020). A first look into DeFi oracles. arXiv. Retrieved fromhttp://arxiv.org/abs/2005.04377

Makarov, I., & Schoar, A. (2022). Cryptocurrencies and decentralized finance (DeFi). Brookings Papers on Economic Activity, 2022(1), 141–215.

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 campaigns. Asian Journal of Research in Computer Science, 18(1), 184–204. https://doi.org/10.9734/ajrcos/2025/v18i1557

Obioha-Val, O., Olaniyi, O. O. O., Selesi-Aina, O., Gbadebo, M. O., & Kolade, T. M. (2024). Machine learning-enabled smart sensors for real-time industrial monitoring: Revolutionizing predictive analytics and decision-making in diverse sectors. Asian Journal of Research in Computer Science, 17(11), 92–113. https://doi.org/10.9734/ajrcos/2024/v17i11522

Okoye, C. C., Nwankwo, E. E., Usman, F. O., Mhlongo, N. Z., Odeyemi, O., & Ike, C. U. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. International Journal of Science and Research Archive, 11(1), 1968–1983. https://doi.org/10.30574/ijsra.2024.11.1.0267

Olabanji, S. O., Oladoyinbo, T. O., Asonze, C. U., Adigwe, C. S., Okunleye, O. J., & Olaniyi, O. O. (2024). Leveraging FinTech compliance to mitigate cryptocurrency volatility for

secure US employee retirement benefits: Bitcoin ETF case study. Asian Journal of Economics, Business and Accounting, 24(4), 147–167. https://doi.org/10.9734/ajeba/2024/v24i41270

Olabanji, S. O., Olaniyi, O. 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

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

Olaniyi, O. O., Okunleye, O. J., Olabanji, S. O., Asonze, C. U., & Ajayi, S. A. (2023). IoT security in the era of ubiquitous computing: A multidisciplinary approach to addressing vulnerabilities and promoting resilience. Asian Journal of Research in Computer Science, 16(4), 354–371. https://doi.org/10.9734/ajrcos/2023/v16i4397

Peihani, M. (2022). Regulation of cyber risk in the banking system: A Canadian case study. Journal of Financial Regulation, 8(2), 139–161. https://doi.org/10.1093/jfr/fjac006

Peters, G. W., Chapelle, A., & Panayi, E. (2016). Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: An operational risk perspective. Palgrave Macmillan Ltd. https://doi.org/10.1057/jbr.2015.10

Shah, K., Lathiya, D., Lukhi, N., Parmar, K., & Sanghvi, H. (2023). A systematic review of decentralized finance protocols. *International Journal of Intelligent Networks*.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cybersecurity: Framework, standards, and recommendations. Future Generation Computer Systems, 92, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002, and PCI DSS. JOIV: International Journal on Informatics Visualization, 4(4), 225–230. https://doi.org/10.30630/joiv.4.4.482

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002, and PCI DSS. JOIV: International Journal on Informatics Visualization, 4(4), 225–230. https://doi.org/10.30630/joiv.4.4.482

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management, 22(4), 239–309. https://doi.org/10.1057/s41283-020-00063-2

UpGuard. (2024, August 13). The 6 biggest cyber threats for financial services in 2024. *UpGuard*. Retrieved from https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

Vasudevan, S. (2022). DeFi: A risky business or silver bullet for SMEs? In *International Conference on Cyber Resilience (ICCR 2022)*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCR56254.2022.9995866

Walch, N. (n.d.). Deconstructing "decentralization": Exploring the core claim of crypto systems. Retrieved fromhttps://twitter.com/neha/status/1007579383417188353

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. (n.d.). SoK: Decentralized finance (DeFi). Conference on Advances in Financial Technologies.

Winter, P., Lorimer, A. H., Snyder, P., & Livshits, B. (2021). Security, privacy, and decentralization in Web3. arXiv. Retrieved fromhttp://arxiv.org/abs/2109.06836

Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: New challenges for compliance. Journal of Financial Crime, 30(1), 97–113. https://doi.org/10.1108/JFC-09-2021-0218

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. Journal of Financial Regulation, 6(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

Zhou, L., et al. (2023). SoK: Decentralized finance (DeFi) attacks. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 2444–2461). https://doi.org/10.1109/SP46215.2023.10179435

Zimba. (2022). A Bayesian attack-network modeling approach to mitigating malware-based banking cyberattacks. *International Journal of Computer Network and Information Security, 14*(1), 25–39. https://doi.org/10.5815/ijcnis.2022.01.03