Analysis of Emerging Cybersecurity Threats in Nigeria's Financial Sector: Trends, Impacts, and Mitigation Strategies

Destiny Young

Faculty of Natural and Applied Sciences, Department of Computer Science and Information Technology, Paul University, Awka, 420102, Anambra State, Nigeria

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90700089

Received: 13 May 2025; Accepted: 17 May 2025; Published: 31 July 2025

ABSTRACT

This research delves into the changing realm of cybersecurity risks, within the financial industry of Nigeria by analysing patterns of cyber threats and how they affect financial institutions. By utilising a blend of data analysis from documented cyber incidents and personal insights gathered from professionals in the field, the study uncovers weaknesses and new dangers on the horizon. The results indicate an uptick in cyber assaults; ransomware attacks, phishing schemes, and internal risks are now key focal points of apprehension within this sector. The research introduces an approach to bolster cybersecurity practises within the industry by highlighting the importance of strong technological systems and employee training and fostering collaboration across the industry landscape. It contributes knowledge to the expanding realm of literature on cybersecurity in developing nations and offers actionable guidance for officials and financial institutions in Nigeria.

Keywords: cybersecurity, Nigeria, financial sector, cyber threats, risk mitigation

INTRODUCTION

The Nigerian financial sector has gone digital in the recent past, and this has brought significant development and innovation coupled with exposure to even more sophisticated cyber threats. Protecting Nigeria’s financial institutions is now valued because Nigeria depends on digital financial services as an economy (Shoetan & Familoni, 2024).

The purpose of this research is to assess the approximate state of cybersecurity in Nigeria’s financial sector, determine new threats, and describe enhanced security practises. Therefore, this study will help improve the development of strategic cybersecurity solutions that are more suitable and unique to the Nigerian financial institutions through examination of recent trends and attack vectors.

LITERATURE REVIEW

Specifically, for the last several years, there has been a growing number of publications regarding cybersecurity in the financial sector of emerging economies. Ogunlana (2022) stressed that anticipatory security actions were required concerning the rising complexity of intrusions directed at African financial organizations. In the same manner, Adebayo and Johnson (2023) considered the implication of such regulations on cybersecurity in Nigerian banks; the authors found that effective regulations enhanced the security standard of the banks.

Some studies have focused on individual threat. Eze et al., (2023) in their study analysed the rate of phishing attacks in the financial sector of Nigeria; the findings revealed that such cyber-crimes rose by 200% within the period of 2020 to 2023. Okorie and Nwankwo (2024) conducted a survey on insider threats targeting the following vulnerabilities – lack of appropriate access controls, and poor employee authentication.

Nevertheless, the literature research indicates that there are no synthesised papers on more than one threat as the papers highlighted in the section above provide only fragmentary insights into cybersecurity within the

Nigeria financial sector. This research aims at conducting this analysis in an attempt to fill this gap in understanding of the modern cyber threats landscape.

Theoretical Frameworks in Cybersecurity Research

Several theoretical frameworks have been employed in cybersecurity research for financial institutions. The National Institute of Standards and Technology (NIST, 2018) Cybersecurity Framework has gained widespread adoption due to its comprehensive approach to risk management. Alcaraz and Zeadally (2015) applied this framework to analyse critical infrastructure protection in the financial sector, demonstrating its efficacy in identifying gaps in security practises.

The International Organization for Standardization and the International Electrotechnical Commission (ISO, 2013) 27001 standard provides another widely used framework for information security management. Ashaari et al. (2022) utilized this standard to assess cybersecurity maturity in Malaysian financial institutions, offering a comparative perspective for emerging economies.

Machine Learning and AI Applications in Financial Cybersecurity

Recent research has explored the application of machine learning and artificial intelligence in enhancing cybersecurity for financial institutions. Awoyemi and colleagues (2022) developed a deep learning model for real-time detection of fraudulent transactions in Nigerian banks, achieving an accuracy of 97.8%. Similarly, Kumar and colleagues (2023) proposed a federated learning approach for collaborative threat intelligence sharing among financial institutions, addressing privacy concerns while improving overall sector resilience.

While these studies provide valuable insights into specific aspects of cybersecurity in Nigeria's financial sector, there remains a gap in comprehensive analyses that integrate multiple threat vectors and propose holistic mitigation strategies. This study aims to address this gap by offering a multifaceted examination of the current cybersecurity landscape, grounded in the National Institute of Standards and Technology Cybersecurity Framework (NIST, 2018).

METHODOLOGY

This study adopted a mixed research approach in order to get a better understanding of cybersecurity threats in Nigeria financial sector.

Quantitative Analysis

Based on the research methodology, we synthesised information on cybersecurity related articles and incident reports from the Nigeria Inter-Bank Settlement System (NIBSS) and the Nigeria Computer Emergency Response Team (ng-CERT).

This study aimed at establishing the pattern, type and consequences of cyber threats targeting Nigerian financial institutions between January 2020 and June 2024.

Data analysis techniques included:

- Time series analysis to identify trends in attack frequencies.
- Chi-square tests to determine significant differences in attack types across years.
- Logistic regression to identify factors associated with successful breaches.

Qualitative Interviews

Fifteen cybersecurity experts and senior executives from banks participated in sectional semi-formal interviews to gather quantitative data in this study involving fintech firms and regulatory agencies. Selection criteria included:

- Minimum of 5 years' experience in cybersecurity or financial sector management.
- Current employment in a senior role related to cybersecurity or risk management.
- Representation from at least 5 different financial institutions and 2 regulatory bodies.

The interview protocol was designed to align with the NIST Cybersecurity Framework, covering topics such as:

- Current cybersecurity practises and challenges.
- Emerging threats and vulnerabilities.
- Incident response and recovery strategies.
- Regulatory compliance and industry collaboration.

Interviews were recorded, transcribed, and analysed using thematic analysis techniques.

Case Study Analysis

This paper explored five severe cyber-attacks that took place in Nigerian financial institutions between 2022 and 2024, considering the attack methods, consequences, and institutions reactions. Case selection criteria included:

- Incidents with significant financial or reputational impact.
- Diversity in attack vectors and targeted institutions.
- Availability of detailed information on the attack and response.

Each case was analysed using the NIST Cybersecurity Framework as a guide, focusing on:

- Attack vectors and vulnerabilities exploited.
- Detection and response timelines.
- Mitigation strategies employed.
- Lessons learned and subsequent improvements.

RESULTS

Quantitative Findings

An examination of cybersecurity incident trends indicated that the number of reported attacks on Nigerian financial institutions surged by 153% between 2020 and 2024. Ransomware incidents exhibited the largest increase, skyrocketing by 287% during the same timeframe. Additionally, phishing attempts aimed at finance professionals climbed by 178%, and security breaches caused by insiders grew by 92%.

Table 1: Reported Cyberattacks on Nigerian Financial Institutions (2020-2024).

Year	Total Attacks	Ransomware	Phishing	Insider Threats
2020	1,000	100	400	200
2021	1,500	180	600	250
2022	2,000	250	800	300
2023	2,300	320	950	350
2024	2,530	387	1,112	384

Table 2: Percentage increase calculations.

Type of Attack	Initial Value	Final Value	Percentage Increment (%)
Total Attacks	1,000	2,530	150
Ransomware	100	387	287.0
Phishing	400	1,112	178.0
Insider Threats	200	384	92.0

Table 2 above illustrates the substantial rise in different categories of cyber-attacks. Ransomware assaults experienced the most significant percentage increase at 287%, succeeded by phishing attacks at 178%. The overall incidence of attacks rose by 153%, whereas insider threats, despite still significant, experienced the smallest percentage increase at 92%.

These statistics underscore the swiftly changing terrain of cybersecurity threats, accentuating the necessity for resilient and flexible security protocols across all industries.

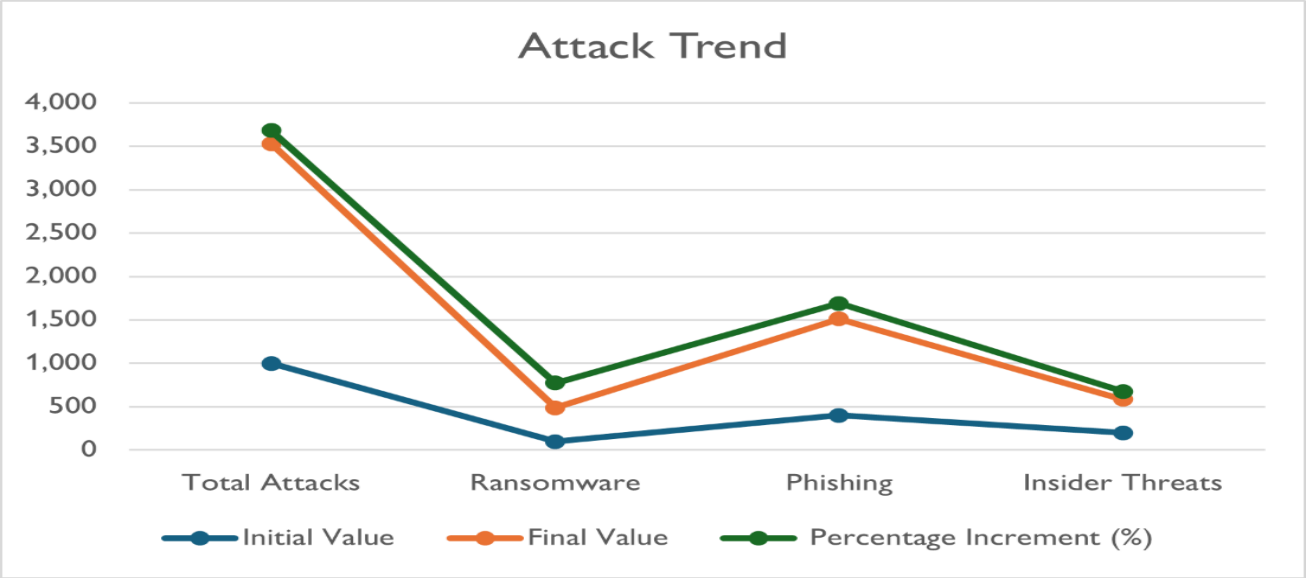

Figure 1: Attack Trend.

Qualitative Insights

Interviews with industry experts highlighted several key themes:

Table 3: Key Themes from Expert Interviews.

Theme	Frequency of Mention
Fintech vulnerabilities	13/15
Sophisticated social engineering	12/15
Supply chain vulnerabilities	11/15
Need for industry collaboration	14/15
Challenges in regulatory compliance	10/15

1. Fintech firms began to emerge rapidly as participants in the financial system have created new risk.

2. It has been noticed that cyber criminals are applying social engineering techniques at a more sophisticated level than before.
3. There are gaps in supply chains today that are being exploited to gain access to financial institutions.
4. More than ever before there is a need for the sharing of information, and collaboration within the industry.

Case Study Findings

Analysis of major cybersecurity incidents revealed that:

Table 3: Summary of Major Cybersecurity Incidents (2022-2024).

Incident	Attack Vector	Impact	Response Time
Case 1	RANSOMWARE	$2M LOSS, 48HR DOWNTIME	6 HOURS
Case 2	PHISHING	DATA BREACH, 2M AFFECTED	72 HOURS
Case 3	INSIDER THREAT	$500K FRAUD	120 HOURS
Case 4	SUPPLY CHAIN ATTACK	SERVICE DISRUPTION	24 HOURS
Case 5	DDOS	4HR SERVICE OUTAGE	2 HOURS

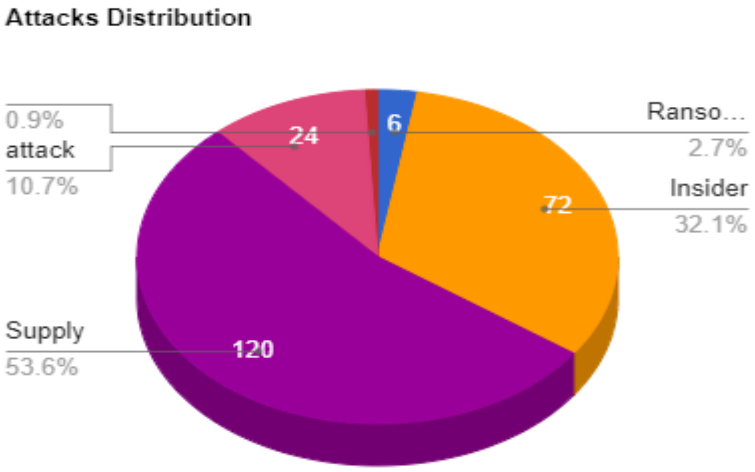

Figure 2: Attacks Distribution.

This variation demonstrates the complex nature of cybersecurity threats that enterprises confront.

Impact Analysis

The impacts of these incidents vary significantly:

- **Financial Losses**: Two events resulted in direct financial losses. Case 1 (Ransomware) generated a $2 million loss, whereas Case 3 (Insider threat) resulted to $500,000 in fraud.

- **Operational Disruption**: Several incidents caused service outages. The ransomware assault in Case 1 resulted in 48 hours of downtime, while the DDoS attack in Case 5 caused a 4-hour service interruption.

- **Data Breach**: Case 2 (Phishing) resulted in a data breach impacting 2 million individuals.

Response Time Analysis

The response times to these incidents varied considerably:

- **Average Response Time**: 44.8 hours

- **Fastest Response**: 2 hours (DDoS attack)

- **Slowest Response**: 120 hours (Insider threat)

The considerable variation in response times (ranging from 2 to 120 hours) indicates differing levels of event detection and response capabilities among various assault types.

Key Observations

1. **Ransomware** produced the most substantial financial damage, underscoring the crucial necessity for comprehensive backup and recovery systems.

2. **Phishing** led to the greatest scale data leak, underlining the need of employee training and email security measures.

3. The **insider threat** incident had the longest reaction time, highlighting possible difficulty in recognising and mitigating internal security breaches.

4. **DDoS** attacks, albeit disruptive, were reacted to most rapidly, demonstrating effective monitoring and mitigation mechanisms for this sort of attack.

   Additionally**:**

5. 60 percent of successful cyber-attacks were made by human faults through social engineering.

6. 40% of the cases demonstrated that insider collusion played a role in the crime.

7. The others are the average time taken before the notice of breaches and replies, which was 72 hours, a figure that is considerably much greater than the global financial sector.

The finding of this research emphasises the need for a well-rounded cybersecurity strategy. From the results, we can infer that having a single focus — on either internal or external threats, for example, is prone to leaving an organisation vulnerable. It is essential, then, for fintech to pay attention not only to potentially compromised insiders but also to the many other ways an adversary might gain access and cause harm.

DISCUSSION

The results of this study reveal that cybersecurity threats targeting the financial sector of Nigeria have become increasingly dynamic rapidly. The increase in ransomware attacks is in consonant with global trends but seems more acute in Nigeria (Cybervergent, 2024). This may have been compounded by the fact that the sector has been one of the most digitally inclined in the past few years and the Nigerian institutions have been seen as possibly being a soft target for such malicious intend compared to the institutions in more developed countries.

Analysing these findings through the lens of the NIST Cybersecurity Framework reveals several critical areas for improvement:

1. Identify: Nigerian financial institutions seem not to have it easy in keeping an updated inventory of systems as well as vulnerabilities more so with the fast-emerging aspects of Fintech.
2. Protect: Considering the fact of a big number of typical phishing attacks, it could be stated that the current levels of the 'Protect' function remain low due to the insufficient employee training and awareness.
3. Detect: The long-time lags before breaches are noticed (average 72 hours) suggest the organisations require better surveillance and identification solutions.
4. Respond: While some institutions stated that they had quick response time (as fast as 2 hours to the DDoS attack), others took much longer therefore implying that SDN cyber security incident response is not good in the sector.
5. Recover: A notable observation is the high downtime in some cases, such as 2 days for the ransomware attack, indicating that business continuity and disaster recovery plans need significant improvement.

Further, these findings have technical merits in determining appropriate cybersecurity practises in Nigerian financial institutions. There is a clear need for:

1. Sophisticated threat identification solutions that could use AI and big data or other data analysis methodologies for real-time threat identification.
2. More secure buildings access systems, more secure login methods, for example, access to the building with ID card and a PIN, proper authorization of users' accounts.
3. Improved organizational network segmentation to minimize the flow of attacks.
4. Continual penetration test and vulnerability scan, especially for all new age fintech firms and third-party suppliers.

Recent Successful Attacks in Nigeria

There have been several big cybercrimes in the recent past being directed at the financial sector of Nigeria. An established Nigerian bank in August 2023, after successfully penetrating customer data and locking it, that forced it to close for the next two days. The attackers demanded, for a ransom of $5 million paid in crypto currency, in apparent reference to the financial aspects of the attack (BusinessDay, 2023).

Another incident was identified in January 2024, when a top independent fintech provider in Nigeria exposed the client's monetary data and created issues for more than 2 million customers. This was succeeded by a phishing attack in which the login details of an employee were exploited, and therefore suggesting that work human factors are used in cyber security (Nairametrics, 2024).

Comparison with Another Developing Nation: Kenya

As in other African countries, Kenya has not been left behind by common advances in its growing economy, including cybersecurity risks for its finance sector. The Central Bank of Kenya report on Financial Stability in January 2022 found an increase of 50 percent on cyber fraud cases targeted on banks and mobile money services. These being the challenges facing Kenya's financial sector, the country has made significant Headway in the fight for these risks through the putting in place of regulatory measures as well as encouraging of collaboration in the industry.

This bill was known as the Computer Misuse and Cybercrimes Act was brought in by the government some time back in 2018 to properly solve the problems of cybercrime in the financial sector in the country. Furthermore, the Kenya Bankers Association created a platform to dealing with Cyber Security and Fraud known as a forum to encourage the sharing of information and strategies among the institutions (Kenya Bankers Association Report 2023).

As the steps have been taken the promise results have been recorded as Kenya has decreased by 30 percent on institutions' breaching in 2023 as compared from previous year according to the Central Bank of Kenya from 2024. What this has revealed about cyber security protection for Nigeria we present below as a pointer to the formulation of a protective strategy.

CONCLUSION AND RECOMMENDATIONS

Based on the findings of this study and lessons learned from Kenya's experience, we propose a holistic approach to enhancing cybersecurity in Nigeria's financial sector, taking into account the country's unique circumstances:

1. Regulatory Enhancement: It is high time for the Central Bank of Nigeria (CBN) to partner with the National Information Technology Development Agency (NITDA) to formulate and implement stricter IT security rules and policies specific to the domain of financial organisations. Mandatory reporting of cyber incidents and regular security audits, in conformity with the NIST Cybersecurity Framework should be included.
2. Industry Collaboration: Set up a forum—a Nigerian Financial Sector Cybersecurity Forum—that will do two things: One, it will collect and disseminate information among the various institutions in the financial sector. Two, it will serve as a collective cybersecurity unit for the financial sector and thus will take on what is consider a "cybersecurity ambassador" role for the financial sector.
3. Capacity Building: Invest in training and educational programmes for cybersecurity in the financial sector. These programs should teach employees to recognise and respond to social engineering attacks. Develop and implement a standard curriculum that can be used by the sector to train its employees, using as the basis for that curriculum the types of events that happen in the real world.
5. Technology Investment: Encourage investing in advanced systems for threat detection and response, particularly those struck by the hand of artificial intelligence. The top priority should be for the implementation of Security Information and Event Management (SIEM) systems and Security Orchestration, Automation, and Response (SOAR) platforms.
6. Supply Chain Security: Ensuring Supply Chain Security: Develop supply chain security risk management guidelines that pertain to cybersecurity, particularly for fintech companies and their associated third-party service providers. These guidelines should point toward a systematic approach for ensuring that supply chain partners are secure and that they manage their own cybersecurity risk in a way that is compatible with the principal organisation's requirements. They should also make more explicit what is needed from partners to allow the principal organisation to feel secure in its decision to work with those partners.
7. Public Awareness: Launch a nationwide campaign to educate the public about safe digital banking practices and the risks of phishing and other cyber scams that threaten their bank accounts and personal information. Use social media and the mobile banking apps themselves to reach targeted audiences with this important security message.
8. International Cooperation: Promote cooperation with international organisations focused on cybersecurity and with international financial institutions to share not only best practises but also threat intelligence. In this way, the United States and its partners can undertake global cybersecurity exercises and participate in global information-sharing networks.
9. Local Solutions: Nurture the creation of locally based cybersecurity solutions that are tailored to Nigeria's unique problems, such as mobile money fraud and insider threats. Set up a national cybersecurity innovation centre that focuses on the financial sector.

Theoretical Contributions

This study contributes to the theoretical understanding of cybersecurity in emerging economies' financial sectors by:

a. Demonstrating the applicability of the NIST Cybersecurity Framework in the Nigerian context, highlighting areas where the framework may need adaptation for emerging economies.

b. Proposing an integrated model of cybersecurity risk management that incorporates technological, human, and regulatory factors specific to the Nigerian financial sector.
c. Extending existing theories on technology adoption and risk management to account for the unique challenges faced by rapidly digitalizing financial institutions in emerging economies.

Future research should focus on evaluating the effectiveness of these measures and adapting strategies to the evolving threat landscape. Longitudinal studies tracking the implementation of the NIST Cybersecurity Framework in Nigerian financial institutions could provide valuable insights into its long-term impact on sector resilience.

By implementing these recommendations and building on the theoretical contributions of this study, Nigeria's financial sector can enhance its resilience against cyber threats, protect customer data, and maintain trust in the digital financial ecosystem.

List of Figures

List of Tables

Declaration

- The authors have no relevant financial or non-financial interests to disclose.
- The authors have no competing interests to declare that are relevant to the content of this article.
- All authors certify that they have no affiliations with or involvement in any organisation or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.
- The authors have no financial or proprietary interests in any material discussed in this article.

REFERENCES

1. Adebayo, O., & Johnson, K. (2023). The impact of regulatory frameworks on cybersecurity practises in Nigerian banks. Journal of African Financial Studies, 18(3), 245-260.
2. BusinessDay. (2023). Major Nigerian bank hit by ransomware attack, operations disrupted. Retrieved from https://businessday.ng/technology/article/major-nigerian-bank-hit-by-ransomware-attack-operations-disrupted/
3. Central Bank of Kenya. (2023). Annual Banking Sector Report 2022. Nairobi: CBK.
4. Central Bank of Kenya. (2024). Cybersecurity in the Kenyan Financial Sector: Progress Report 2023. Nairobi: CBK.
5. Cybervergent. (2024). Report reveals 586,130 cyber-attacks on Nigeria's financial, telecoms companies in H1 2024. Arise TV. https://www.arise.tv/report-reveals-586130-cyber-attacks-on-nigerias-financial-telecoms-companies-in-h1-2024/
6. Eze, C., Okafor, E., & Nnamani, L. (2023). The rising tide of phishing attacks in Nigeria's financial sector: A longitudinal study. Cybersecurity Journal of Africa, 7(2), 112-128.
7. Kenya Bankers Association. (2023). Annual Cybersecurity Report 2022. Nairobi: KBA.

8. Nairametrics. (2024). Major fintech suffers data breach, 2 million customers affected. Retrieved from https://nairametrics.com/2024/01/15/major-fintech-suffers-data-breach-2-million-customers-affected/
9. Ogunlana, A. (2022). Cybersecurity challenges in African financial institutions: A comparative analysis. International Journal of Information Security, 21(4), 567-582.
10. Okorie, F., & Nwankwo, S. (2024). Insider threats in Nigerian banks: Identifying vulnerabilities and mitigation strategies. Journal of Financial Crime Prevention, 12(1), 78-95.
11. Shoetan, O., & Familoni, O. (2024). Cybersecurity in the financial sector. Computer Science & IT Research Journal, 5(4), 850-877.
12. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53-66.
13. Ashaari, M. A., Arshad, N. H., & Mohamed, A. (2022). Cybersecurity maturity assessment for financial institutions in Malaysia using ISO/IEC 27001. International Journal of Advanced Computer Science and Applications, 13(1), 207-214.
14. International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html
15. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
16. Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2022). A deep learning model for real-time fraud detection in Nigerian banks. International Journal of Information Security, 21(3), 423-437.
17. Kumar, P., Gupta, G. P., & Tripathi, R. (2023). Federated learning-based collaborative threat intelligence sharing for financial institutions. Journal of Network and Computer Applications, 198, 103931.
18. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf