International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Cybersecurity threats in the financial sector: Analyzing attack types, Vulnerabilities, and response mechanisms across geopolitical contexts (2015–2024)

Abdul-waliyyu Bello [1,*], Idris Wonuola [1], Anastesia Izundu [2] and Jacinta Izundu [3]

[1] *Department of Mathematics and Statistics, Austin Peay State University, Tennessee, USA.*
[2] *Department of Public Health, University of Illinois at Springfield, Illinois, USA.*
[3] *Department of Cybersecurity Management, University of Illinois at Springfield, Illinois, USA.*

International Journal of Science and Research Archive, 2025, 16(01), 134-150

Publication history: Received on 25 May 2025; revised on 28 June 2025; accepted on 02 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2007

Abstract

The digital transformation of the financial sector between 2015 and 2024 has brought efficiency and innovation, but it has also increased exposure to a wide range of cybersecurity threats. This study investigates the rise and evolution of major cyberattack types targeting financial institutions, including phishing, ransomware, man-in-the-middle attacks, and distributed denial-of-service (DDoS) attacks. Using a structured dataset of real-world incidents across multiple countries, the research applies supervised machine learning techniques like Random Forest and XGBoost to classify attack types and uncover their underlying drivers. Phishing emerged as the most frequent threat, with social engineering, weak passwords, and zero-day exploits identified as major contributors to successful breaches.

The XGBoost model outperformed Random Forest, achieving 80.9% accuracy and a weighted F1-score of 80.98%. Feature importance analysis revealed that financial loss, number of affected users, and incident resolution time were key predictors. The study also highlights how countries with high digital connectivity, but weaker regulations, face more frequent attacks, underlining the geopolitical nature of cyber risks.

Ultimately, this paper demonstrates the value of ensemble learning models in predictive cybersecurity and stresses the importance of layered defenses, employee awareness, and international collaboration. Its insights support the development of proactive strategies to strengthen cyber resilience across the global financial sector.

Keywords: Cybersecurity; Financial sector; Machine learning; Geopolitical risk; Threat classification; Predictive modeling

1. Introduction

The financial sector over the past decade has seen massive digital growth fueled by FinTech innovation, mobile banking, and blockchain. But with this progress comes growing cybersecurity risks. Banks, payment platforms, and investment firms have become top targets for cybercriminals, political hackers, and state-sponsored attackers (Adeyeri & Abroshan, 2024). From 2015 to 2024, cyberattacks in the financial world have become more frequent and more damaging, resulting in billions in losses and weakening public trust (Meiqi, 2024).

Geopolitical tensions often drive these threats. For example, North Korea's Lazarus Group was behind the 2016 Bangladesh Bank heist, while Russian-affiliated groups like Cozy Bear have targeted Western financial systems during conflicts like the Russia-Ukraine war (Naseeb & Tariq, 2024) (Azubuike, 2023). Developing countries, especially in Africa, face unique risks due to limited cybersecurity resources despite growing digital finance adoption (Gul & Malik,

* Corresponding author: Abdul-waliyyu Bello

Cyber conflict and international security: Legal challenges and strategic solutions in cyberspace, 2024). In contrast, regions like the U.S. and the EU have strong regulations but still deal with advanced threats.

The interconnected nature of today's financial systems has only increased their exposure. Attack types such as ransomware, DDoS, phishing, and advanced persistent threats (APTs) have surged. Ransomware groups like LockBit and Conti target critical systems for multimillion-dollar payouts, while phishing campaigns now use AI-generated deepfakes to trick users (Montasari, 2024); (Saaida, 2023). High-profile breaches like those of Equifax and Binance reveal just how valuable and vulnerable financial data can be.

Root causes of these cyber risks include outdated systems, human error, and flawed infrastructure. Legacy technology, such as decades-old COBOL-based platforms, creates security gaps (Alavi, 2023). Meanwhile, employee mistakes like falling for phishing or using weak passwords often open doors to an attacker. Events like the 2020 Twitter breach and the rise of remote work during COVID-19 highlight how these vulnerabilities can impact financial stability (Rugina, 2023).

In response, institutions are turning to technologies like AI-based threat detection, zero-trust security models, and blockchain. Major players like JPMorgan Chase now use machine learning to spot suspicious transactions. However, many still struggle to integrate these new tools with older systems (Mwangi, 2024). Efforts such as the EU's NIS Directive and FS-ISAC aim to strengthen regulations and encourage information sharing, though smaller institutions often face challenges keeping up.

Cyber defense is evolving, but so are the threats. That's why this paper aims to explore and classify the main types of cyberattacks, phishing, ransomware, DDoS, and APTs, targeting the financial sector between 2015 and 2024. By identifying patterns, vulnerabilities, and trends, the study provides insights to support better cybersecurity strategies across financial institutions worldwide.

2. Literature Review

Cybersecurity has emerged as a critical concern for the global financial sector, particularly in the face of rising digital transformation and evolving cyber threats. This literature review explores existing research on the types of cyberattacks targeting financial institutions, the underlying vulnerabilities that expose them, and the mechanisms employed to mitigate these threats. Emphasis is placed on the period from 2015 to 2024, analyzing how response strategies vary across different geopolitical contexts.

2.1. Cybersecurity Threats

Cyber threat activity against financial institutions has escalated sharply since 2015, fueled by rapid digital transformation, ubiquitous API connectivity, and intensifying geopolitical frictions (Ahsan, et al., 2022). Also, (Umoga, Sodiya, Amoo, & Atadoga, 2024) noted that between 2022 and 2023 alone, the sector saw a 154 percent surge in major incidents such as distributed-denial-of-service attacks, overtaking gaming as the most-targeted vertical; a clear sign that banks, insurers and payment firms now sit at the epicenter of the global cyber battlefield. Together, these threat classes create a multi-layered risk matrix: ransomware extracts direct monetary ransoms, phishing seeds' initial access, DDoS undermines confidence and availability, supply-chain flaws widen attack surfaces, insiders erode trust from within, and nation-state actors add strategic complexity (Altulaihan, 2022). The types of cybersecurity threats are:

2.1.1. Ransomware and Multi-Layer Extortion

Ransomware remains the most financially destructive threat. Ransomware-as-a-Service (RaaS) platforms such as LockBit, ALPHV/BlackCat, and the Cl0p syndicate have commoditized advanced tooling, letting affiliates launch high-impact campaigns for a revenue share. Modern crews blend encryption with data theft (double extortion) and pressure downstream partners or customers (triple extortion), forcing victims to pay to avoid regulatory fines and reputational damage (Amoo, et al., 2024). LockBit alone has netted more than $200 million USD in Bitcoin since 2022, despite high-profile takedown efforts (Ahsan, et al., 2022).

2.1.2. Phishing, Social Engineering & Brand Impersonation

Credential-harvesting and malware-laden lures remain the dominant entry vectors because finance staff sit behind rich troves of customer data and payment rails. In the first half of 2024, social-engineering tactics accounted for 65 percent of successful breaches in banks, double the previous year (Umoga, Sodiya, Amoo, & Atadoga, 2024). Attackers increasingly impersonate trusted brands such as DocuSign or SWIFT transfer notices; 68 percent of counterfeit domains

targeting finance are pure phishing sites. The growth of adversary-in-the-middle kits and AI-generated "deep-phish" content lowers the barrier further, allowing criminals to sidestep MFA and initiate high-value wire fraud (Altulaihan, 2022).

2.1.3. DDoS and Hacktivist Swarms

Layer 3/4 and application-layer DDoS assaults have resurged as geopolitical "cyber-protest." Financial services now absorb roughly one-third of all global DDoS traffic. Botnets driven by malware such as Mirai variants can marshal tens of millions of hijacked IoT devices, while hacktivist collectives linked to the Russia-Ukraine war and conflicts in the Middle East openly coordinate takedowns of payment gateways and online banking portals (Galushchenko, Pidbereznykh, Piroh, Khrapach, & Tolmachov, 2024). Some 2024 events combined up to 69 discrete vectors in a single barrage, making mitigation resource-intensive and costly (Amoo, et al., 2024).

2.1.4. Supply-Chain and Third-Party Platform Breaches

The 2023–24 MOVEit file-transfer compromise exposed a systemic blind spot: software used by thousands of firms worldwide can become a single point of failure. Cl0p exploited a SQL-injection flaw, stealing data from more than 2,700 organizations, including global banks, credit unions, and payment processors, and exposing over 90 million personal records. A second wave in mid-2024 highlighted how sluggish patch uptake leaves loopholes open for encore attacks. Such incidents underscore how interconnected vendor ecosystems magnify risk far beyond any one institution's perimeter (Amoo, et al., 2024).

2.1.5. Insider Threats

Not all breaches come from outside. A study conducted by (Umoga, Sodiya, Amoo, & Atadoga, 2024) shows that the finance vertical bears the world's highest insider-incident costs, averaging US$14–16 million per event. Also, low-paid call-center or back-office workers have been caught selling customer PII to fraud rings, while senior staff with privileged access perpetrate long-running embezzlement or data-exfil schemes (Alavi, 2023). Remote-work models increase exposure: unsecured home networks, shared devices, and diminished oversight give neglectful or malicious insiders more opportunities to siphon data undetected (Galushchenko, Pidbereznykh, Piroh, Khrapach, & Tolmachov, 2024).

2.2. Sector-Specific Vulnerabilities

The financial sector occupies a central role in modern economies, serving as the backbone of global commerce, savings, and investment (George, Baskar, & Srikaanth, 2024). However, its prominence also makes it an attractive and high-impact target for cybercriminals, hacktivists, and state-sponsored actors. Unlike other industries, financial institutions handle vast volumes of sensitive data and real-time monetary transactions, creating a unique set of vulnerabilities (Górnicka, Ogawa, & Xu, 2023). These vulnerabilities are compounded by technological complexity, regulatory pressures, and geopolitical exposure.

2.2.1. High-Value Data and Transaction Volume

Financial institutions process an immense volume of sensitive data daily, including personal identifiable information (PII), payment card details, loan records, and business account credentials. This data is a valuable commodity for cybercriminals engaged in identity theft, financial fraud, and black-market trading (Cappa, Oriani, Peruffo, & McCarthy, 2021). Moreover, the real-time nature of financial transactions means that even a brief compromise can result in substantial monetary losses before containment is possible. Attackers are drawn to this "high payoff" environment, which elevates the financial sector's risk profile compared to other industries (Saaida, 2023).

2.2.2. Legacy Systems and Infrastructure Gaps

Many banks, insurance firms, and credit unions rely heavily on legacy IT infrastructure that has not been updated to withstand modern cyber threats. Outdated software, unsupported operating systems, and obsolete network protocols are common in back-end operations, especially in traditional institutions that have grown through mergers and acquisitions (George, Baskar, & Srikaanth, 2024). These systems are often difficult to patch or integrate with newer technologies, creating exploitable weaknesses. Legacy platforms frequently lack essential security features such as encryption-at-rest or multi-factor authentication, giving adversaries easier access points (Altulaihan, 2022).

2.2.3. Complex Digital Ecosystems and API Exposure

With the rise of digital banking, fintech collaborations, and open banking frameworks, financial institutions are increasingly interconnected through APIs (Application Programming Interfaces) (George, Baskar, & Srikaanth, 2024).

Also, (Montasari, 2024) stated that while this promotes innovation and customer convenience, it also expands the attack surface dramatically. Poorly secured APIs or third-party applications can serve as a conduit for cyber intrusion. However, the integration of multiple systems, payment gateways, mobile banking apps, trading platforms, and customer service bots introduces architectural complexity, often making it difficult for organizations to maintain consistent security protocols across all layers (Naseeb & Tariq, 2024).

2.2.4. Regulatory and Compliance Pressures

The financial sector is among the most heavily regulated industries globally. While compliance standards like the Payment Card Industry Data Security Standard (PCI DSS), Basel III, GDPR, and NDPR are designed to protect data and promote operational integrity, they can also present challenges (Mwangi, 2024). Alavi (2023) study noted that institutions may focus on "ticking the box" rather than implementing adaptive, risk-based security. The lag between evolving cyber threats and regulatory updates also means that compliance alone is not sufficient to ensure robust protection. Furthermore, regulatory fragmentation across borders makes it difficult for multinational institutions to apply uniform cybersecurity strategies (Cavelty, 2024).

2.2.5. Human Factor and Insider Threats

Human error remains one of the leading causes of data breaches in the financial sector. Frontline employees, customer service representatives, and IT personnel may fall victim to phishing emails, social engineering tactics, or accidental data exposure (Naseeb & Tariq, 2024). In high-pressure environments, security protocols may be bypassed for convenience or productivity. Moreover, insider threats, whether from disgruntled employees or those colluding with external actors, can be particularly devastating due to the privileged access they often receive. The use of personal devices for remote work, especially after the COVID-19 pandemic, has further blurred the boundary between secure corporate systems and vulnerable external networks (Gul & Malik, 2024).

2.3. Response Mechanisms to Cybersecurity Threats

The financial sector is a prime target for cyberattacks due to its direct connection to wealth, sensitive personal and corporate data, and its critical role in maintaining national and international economic stability (Okoli, Obi, Adewusi, & Abrahams, 2024). Also, (Sankaram, Roopesh, Rasetti, & Nishat, 2024) noted that as threats have grown more complex and damaging from 2015 to 2024, response mechanisms in the financial sector have also evolved, moving beyond basic reactive approaches to incorporate proactive, strategic, and coordinated responses. These mechanisms are implemented at both institutional and national levels, with some degree of international cooperation. They include technical solutions, organizational processes, regulatory frameworks, incident management protocols, and capacity-building measures designed to detect, contain, and mitigate cyber threats (Aljumah & Ahanger, 2020).

Also, Okoli, et al., (2024) stated that one of the primary response mechanisms adopted by financial institutions is the implementation of robust cybersecurity frameworks and architectures. These often include advanced firewalls, intrusion detection and prevention systems (IDPS), endpoint protection platforms (EPP), and Security Information and Event Management (SIEM) systems. These tools collectively provide continuous monitoring and real-time alerting capabilities, helping institutions detect abnormal activities that could signal a breach. Over the past decade, many financial firms have moved toward a "defense-in-depth" model, which incorporates multiple layers of security to protect networks, applications, data, and end-user devices. This approach ensures that even if one layer is breached, others can serve as barriers to further compromise (Aljumah & Ahanger, 2020).

Furthermore, an increasingly prominent framework being adopted globally is the Zero Trust Architecture (ZTA) (Safitra, Lubis, & Fakhrurroja, 2023). Zero Trust operates on the principle of "never trust, always verify," meaning that no user or system, whether internal or external, is automatically trusted. Access is granted only after strict authentication and authorization, often tied to identity, device posture, location, and behavioral patterns. This framework has gained popularity in the financial sector, where insider threats and credential theft remain significant vulnerabilities (Umar & Butler, 2021). By implementing role-based access controls, multi-factor authentication (MFA), and micro-segmentation of networks, financial institutions can limit lateral movement within their systems in case of a breach (Hong, 2021).

Additionally, beyond technical measures, financial institutions are increasingly investing in their organizational response capabilities. This fact includes the development and regular testing of incident response plans (IRPs), which define the roles, responsibilities, and procedures to be followed in the event of a cyber incident (Aljumah & Ahanger, 2020). Well-structured IRPs include stages such as preparation, detection and analysis, containment, eradication, recovery, and post-incident review. Many institutions also run table-top exercises and red teaming simulations to test

their preparedness and refine their responses under realistic conditions. These exercises often reveal critical weaknesses in decision-making processes, communication channels, and system dependencies that can be addressed proactively (Safitra, Lubis, & Fakhrurroja, 2023).

Also, cybersecurity awareness and training are another vital component of institutional response mechanisms. Human error continues to be a leading cause of data breaches, with phishing and social engineering accounting for a significant proportion of initial intrusion vectors (Okoli, Obi, Adewusi, & Abrahams, 2024). In response, many financial institutions have introduced mandatory cybersecurity training for employees at all levels. This idea includes simulated phishing campaigns, regular policy updates, and real-time guidance on identifying suspicious activity (Jeyaraj, Zadeh, & Sethi, 2021). Frontline workers, particularly in customer service, loan processing, and IT support, are trained to recognize red flags and escalate concerns quickly. Senior executives and board members are also being educated on cyber risk, given their role in governance and risk oversight (Hong, 2021).

However, collaboration between financial institutions has become a powerful response mechanism. Information Sharing and Analysis Centers (ISACs), such as the Financial Services ISAC (FS-ISAC), have become vital platforms for exchanging threat intelligence, best practices, and technical indicators of compromise (IOCs) (Jimmy, 2021). By working together, financial institutions can detect and respond to attacks more rapidly, identify common vulnerabilities, and coordinate defenses against sophisticated threats like ransomware cartels or nation-state actors. In Africa, regional cybersecurity forums have emerged to promote cross-border cooperation, especially as digital banking and fintech adoption grow (Okoli, Obi, Adewusi, & Abrahams, 2024).

In addition to institutional and national responses, international cooperation has gained importance, especially considering the borderless nature of cyber threats. The Budapest Convention on Cybercrime, for example, serves as a legal framework for international collaboration on investigation and prosecution (Umar & Butler, 2021). International bodies such as the Financial Stability Board (FSB), the International Monetary Fund (IMF), and the World Bank have also issued guidance and conducted assessments on cyber resilience in the financial sector. These organizations support capacity building, promote harmonization of standards, and encourage sharing knowledge across countries with different levels of technological maturity (Jimmy, 2021).

2.4. Geopolitical Contexts in Cybersecurity Threats

Geopolitical contexts significantly shape the nature, frequency, and impact of cybersecurity threats in the financial sector. As digital finance becomes more deeply embedded in the global economy, financial institutions are increasingly exposed not just to cybercriminals seeking profit, but to politically motivated actors, state-sponsored groups, and geopolitical tensions that influence the cyber threat landscape (Khan, Saeed, & Kakar, 2024). Between 2015 and 2024, (Adeyeri & Abroshan, 2024) stated that the rise in politically charged cyberattacks has underscored the inextricable link between global power dynamics and digital financial security.

However, in regions experiencing political instability or international conflict, financial institutions are often targeted as symbols of national strength or as tools for economic disruption (Ibekwe, Nwokediegwu, Umoh, Adefemi, & Ilojianya, 2024). Similarly, institutions in the United States, Israel, and other Western countries have been targeted by state-sponsored groups from adversarial nations such as Iran, North Korea, and China. These attacks are not always aimed at financial gain; rather, they seek to undermine trust, gather intelligence, or retaliate against sanctions and foreign policy decisions (Adeyeri & Abroshan, 2024). In such contexts, the financial sector becomes both a battlefield and a barometer of cyber-hostile geopolitical relations.

Geopolitics also influences the regulatory frameworks that govern cybersecurity in the financial sector. Countries in the European Union benefit from the GDPR, the Network and Information Security (NIS) Directive, and shared initiatives by the European Central Bank to harmonize and strengthen cyber resilience (Umar & Butler, 2021). Regulatory environments vary widely in Africa and Asia, where inconsistent enforcement, policy fragmentation, and competing national interests hinder coordinated response mechanisms. The result is an uneven cybersecurity terrain in which multinational financial institutions must navigate vastly different threat environments, compliance requirements, and geopolitical risks depending on the regions in which they operate (Khan, Saeed, & Kakar, 2024).

2.5. Theoretical Review

2.5.1. Technology Threat Avoidance Theory (TTAT)

Technology Threat Avoidance Theory (TTAT) was developed by Liang and Xue in 2009 to explain how individuals and organizations recognize, evaluate, and respond to technological threats, particularly in the context of cybersecurity

(Carpenter, Young, Barrett, & McLeod, 2019). The theory is grounded in the psychological and behavioral sciences and draws from the broader Protection Motivation Theory (PMT), which posits that people protect themselves based on perceived severity, susceptibility, and the efficacy of possible responses (Chen & Liang, 2019).

The basic tenet of TTAT is that individuals and organizations engage in threat avoidance behaviors when they perceive a significant cybersecurity threat and believe they possess both the ability and the means to avoid or mitigate the risk (Gillam & Waite, 2021). Theory identifies four primary constructs that influence avoidance motivation: perceived threat severity, perceived threat susceptibility, safeguard effectiveness, and safeguard cost. Together, these factors shape the perceived threat and coping appraisal, which in turn determines whether an entity will take preventative or protective action (Boysen, Hewitt, Gibbs, & McLeod, 2019). Perceived threat severity refers to how harmful an individual or institution believes the threat could be if realized, while threat susceptibility captures the likelihood of being targeted or affected. Safeguard effectiveness involves the belief that specific measures (e.g., firewalls, training, and encryption) can prevent the attack, whereas safeguard cost reflects the financial, operational, or psychological costs associated with implementing those measures. If the perceived threat is high and the safeguards are deemed effective and affordable, the motivation to avoid the threat increases (Carpenter, Young, Barrett, & McLeod, 2019).

In the context of cybersecurity threats in the financial sector, TTAT offers valuable insights into how financial institutions perceive and respond to the growing spectrum of cyberattacks. From 2015 to 2024, banks and other financial entities have been under increasing pressure to prevent breaches caused by ransomware, phishing, insider threats, and advanced persistent threats (Chen & Liang, 2019). According to TTAT, a bank's willingness to adopt proactive cybersecurity strategies such as zero-trust architecture, AI-driven threat detection, or employee awareness programs depends not only on the perceived risk of attack, but also on its assessment of the cost and effectiveness of such countermeasures (Boysen, Hewitt, Gibbs, & McLeod, 2019).

2.6. Empirical Studies

(Adeyeri & Abroshan, 2024) investigate the geopolitical ramifications of cybersecurity threats, focusing on state responses and international cooperation in the digital warfare era. Key findings highlight that cybersecurity challenges have prompted nations to enhance their defensive strategies and foster collaboration through international agreements. The study argues that the increasing frequency of cyberattacks necessitates a unified global response to safeguard national security and economic stability. They emphasize the importance of sharing intelligence and resources among states to mitigate threats and maintain cybersecurity resilience. Overall, the study underscores the critical role of international cooperation in addressing the evolving landscape of digital threats.

(Rugina, 2023) presents a comprehensive analysis of cybersecurity strategies in international relations from the perspective of attackers. Utilizing qualitative methods, including case studies and expert interviews, the study examines how malicious actors exploit vulnerabilities in national cybersecurity frameworks. Key findings suggest that attackers often target critical infrastructure and leverage social engineering techniques to breach defenses. The study highlights the need for nations to adopt proactive cybersecurity measures and enhance collaboration across borders to combat these threats effectively. The research underscores the evolving nature of cyber threats and the importance of adaptive strategies in maintaining national security in the digital age.

(Galushchenko, Pidbereznykh, Piroh, Khrapach, & Tolmachov, 2024) analyze the cybersecurity and geopolitical dimensions of external information interventions in Ukraine. Employing a mixed-methods approach, the study combines quantitative data analysis with qualitative case studies to assess the impact of foreign influence on Ukraine's information landscape. Key findings reveal a significant increase in cyberattacks and misinformation campaigns aimed at destabilizing the country. The authors emphasize the need for robust cybersecurity measures and strategic communication to counter these threats.

(Iftikhar, 2024) reviews cyber terrorism as a global threat, focusing on its repercussions and countermeasures. Utilizing a systematic literature review methodology, the study synthesizes existing research to identify patterns and impacts of cyber-terrorism on national security and public safety. Key findings indicate that cyberterrorism poses significant risks to critical infrastructure and can incite social unrest. The author emphasizes the necessity for comprehensive countermeasures, including enhanced cybersecurity protocols, international cooperation, and public awareness campaigns.

(Kundavaram, Onteddu, Nizamuddin, & Devarapu, 2023) examine cybersecurity risks in financial transactions and their implications for global trade and economic development. Using a mixed-methods approach, the study analyzes quantitative data on cyber incidents alongside qualitative interviews with industry experts. Key findings highlight that

cybersecurity vulnerabilities in financial transactions can lead to significant economic losses and undermine consumer trust. The authors emphasize the need for robust cybersecurity frameworks and regulatory measures to protect financial systems.

2.7. Gaps in the Reviewed Literatures

While cybersecurity threats in the financial sector have been widely studied, notable research gaps persist, particularly in empirical, data-driven investigations. Most prior studies adopt narrative or qualitative approaches, lacking quantitative analysis using structured data to classify and predict attack patterns. There is a gap in leveraging supervised machine learning models to predict cybersecurity attack types based on key features such as geographic origin, financial impact, user exposure, and specific vulnerabilities. Moreover, cross-country comparative studies are often theoretical, with limited use of multiclass classification to analyze how contextual factors like country, attack source, or vulnerability type influence attack typology.

Another underexplored area is the integration of time-series trends in cybersecurity incidents, although years are often captured, few studies use it analytically to assess temporal shifts in attack types. Moreover, the influence of sector-specific characteristics on attack severity and form remains understudied in quantitative modeling. Finally, while theoretic frameworks such as TTAT provide behavioral insights, there is limited alignment between theory and data science approaches that could enable early threat detection and proactive defense. This study addresses these gaps by using a classification model on a real-world dataset to identify predictive patterns and trends in financial sector cyber-attacks.

3. Methodology

3.1. Research Design

This study adopts a quantitative research design using a supervised machine learning approach, specifically a multiclass classification model, to analyze and predict cybersecurity attack types in the financial sector. The design is appropriate as it allows for systematic examination of patterns and relationships between structured variables such as country, year, financial loss, and security vulnerability types. Unlike qualitative methods, this design enables objective, data-driven insights and supports generalization across different geopolitical contexts.

The classification focus aligns with the research objective of identifying predictors of specific attack types (e.g., phishing, ransomware, DDoS). By employing this empirical approach, the study advances existing literature, which has primarily relied on descriptive or case-based analyses, offering a predictive perspective essential for real-time threat mitigation.

3.2. Data Source and Description

The dataset used in this study was obtained from Kaggle, a reputable platform for curated and peer-reviewed datasets. It contains structured information on cybersecurity incidents targeting the financial sector between 2015 and 2024. The key variables include country, year, financial loss, number of affected users, attack source, security vulnerability type, and the target variable, attack type. The dataset was filtered to include only records relevant to the financial industry to maintain sectoral specificity. Kaggle was chosen due to its accessibility, quality control, and relevance for machine learning applications. The data provides a rich foundation for developing predictive models and enables cross-national analysis of cyberattack trends based on real-world incidents.

3.3. Sampling Technique

This study adopts a purposive sampling technique, focusing exclusively on cybersecurity incidents in the financial sector extracted from the broader Kaggle dataset. Records not related to banking, insurance, fintech, or investment institutions were excluded to ensure sectoral relevance. The purposive approach is justified as it allows for the deliberate selection of data points that align with the research objective, understanding, and predicting attack types in the financial domain.

3.4. Analytical Techniques

This study adopts two supervised machine learning algorithms, Random Forest and XGBoost, to build a multiclass classification model for predicting cyberattack types in the financial sector. These algorithms are selected for their robustness, ability to handle mixed data types, and high performance with structured datasets. The dataset will be split into training and testing sets (80:20 ratio). Both models will be trained and evaluated using key metrics, including accuracy, precision, recall, F1-score, and the confusion matrix to assess predictive performance across attack categories. Additionally, feature importance scores will be abstracted to identify the most significant predictors of attack types.

Model development and evaluation will be carried out using Python's Scikit-learn and XGBoost libraries to ensure efficiency and reproducibility.

3.5. Data Pre-processing

Prior to model development, the dataset will undergo rigorous preprocessing to ensure quality and compatibility with machine learning algorithms. Missing values will be addressed through imputation or removal, depending on their frequency and significance. Categorical variables such as Country, Attack Source, and Security Vulnerability Type will be transformed using one-hot encoding to enable proper handling by Random Forest and XGBoost. Numerical features like Financial Loss and Number of Affected Users will be standardized where appropriate to improve model stability.

3.6. Ethical Considerations

This study relies on secondary data sourced from Kaggle, which is publicly available and anonymized, ensuring no direct involvement of human subjects or disclosure of personal information. Ethical approval is not required; however, the data will be used strictly for academic purposes. Proper attribution to the dataset source will be maintained. All analyses will be conducted with integrity, avoiding any form of data manipulation, while respecting the ethical standards of research transparency, reproducibility, and responsible data use.

4. Results

This section presents the results of the analysis and machine learning techniques applied to detect attack types based on the included features.

	Financial Loss (in Million $)	Number of Affected Users	Incident Resolution Time (in Hours)
count	445.00000	445.000000	445.000000
mean	51.17391	505839.114607	35.737079
std	28.94402	302354.003783	19.903044
min	1.01000	1326.000000	1.000000
25%	27.00000	240400.000000	19.000000
50%	50.75000	513005.000000	36.000000
75%	77.29000	772512.000000	52.000000
max	99.99000	998937.000000	72.000000

Figure 1 Descriptive Statistics of Key Incident Variables in Financial Sector Cyberattacks (2015–2024)

The average financial loss per incident was more or less $51.17 million (SD = $28.94 million), indicating a wide range in the monetary consequences of attacks, with some resulting in losses nearing $100 million. Correspondingly, the number of affected users per incident varied greatly, with a mean of 505,839 users (SD = 302,354), suggesting that while some breaches had limited reach, others compromised nearly a million individuals. Incident resolution time also showed a moderate dispersion, averaging 35.74 hours (SD = 19.90), which implies that while certain breaches were addressed within a day, others required more extended response efforts.

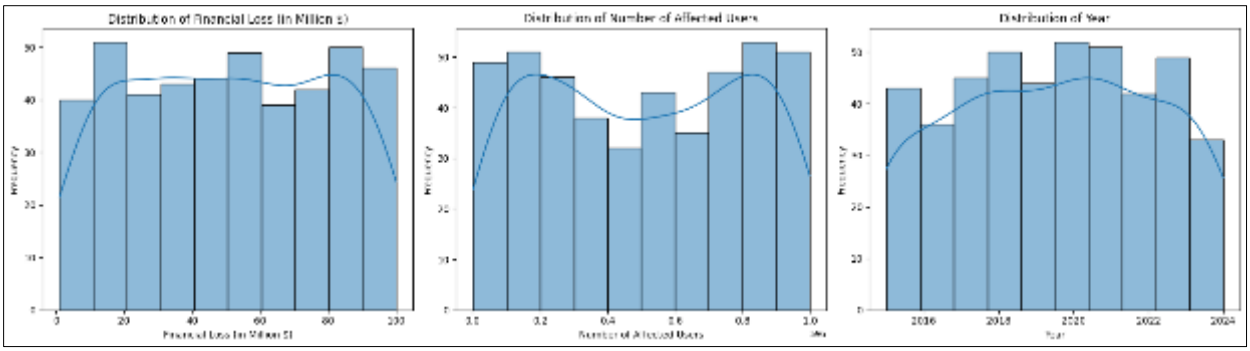

Figure 2 Distribution of Key Variables in Financial Sector Cybersecurity Incidents (2015–2024)

The distribution plots reveal that financial losses and the number of affected users are relatively uniform, indicating no significant skewness, though a slight concentration is visible toward higher loss values. Incident frequency over time shows a gradual increase from 2015, peaking around 2020–2021, and slightly declining by 2024. This trend suggests growing cyber risk in recent years, followed by possible improvements in detection or reporting. Overall, the data appears well-distributed, suitable for modeling without a significant transformation.

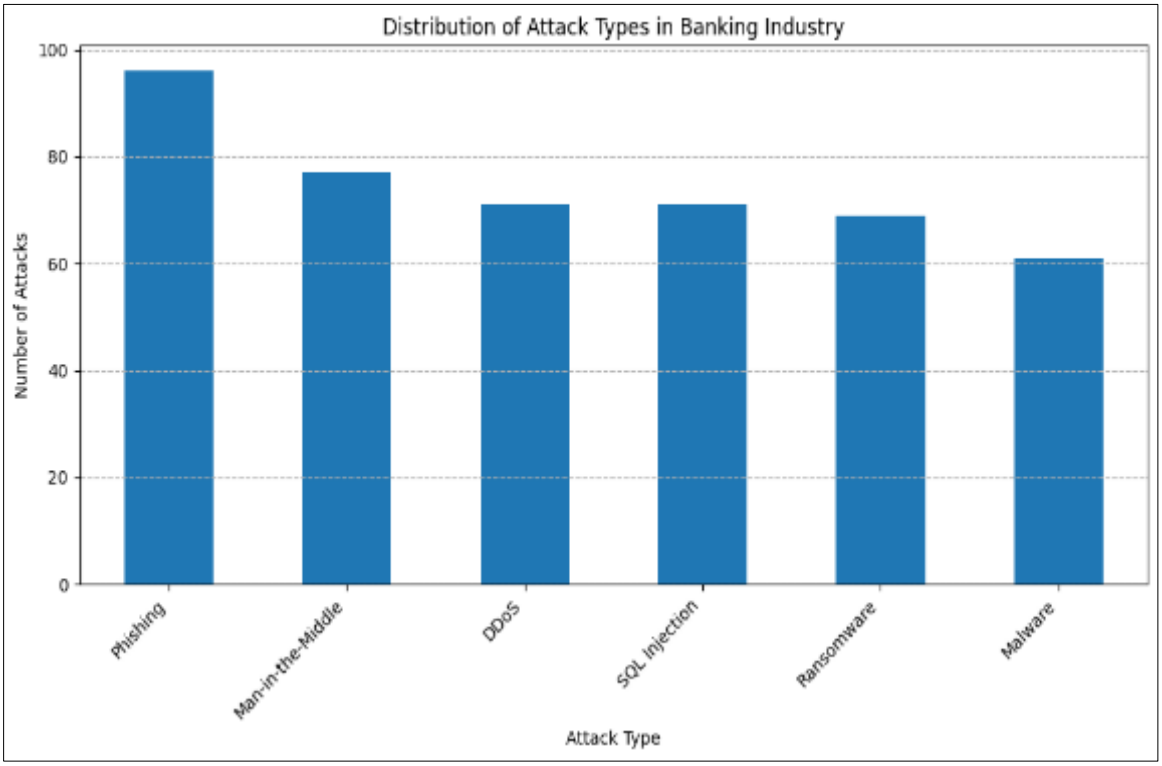

Figure 3 Frequency Distribution of Cyberattack Types in the Banking Industry (2015–2024)

An analysis of the distribution of cybersecurity attack types within the financial sector revealed that phishing was the most frequently reported incident, occurring in 96 cases. This observation was followed by man-in-the-middle attacks (n = 77), DDoS attacks (n = 71), and SQL injection attacks (n = 71), each demonstrating comparable prevalence. Ransomware incidents were also prominent, with 69 occurrences, while malware attacks were the least frequent among the recorded types, with 61 cases. The results suggest that phishing remains the most dominant threat vector, likely due to its low cost and high success rate through social engineering. The relatively high occurrence of man-in-the-middle and injection-based attacks indicates persistent vulnerabilities in network and application-level defenses, underscoring the need for strengthened authentication and code security measures in financial systems.

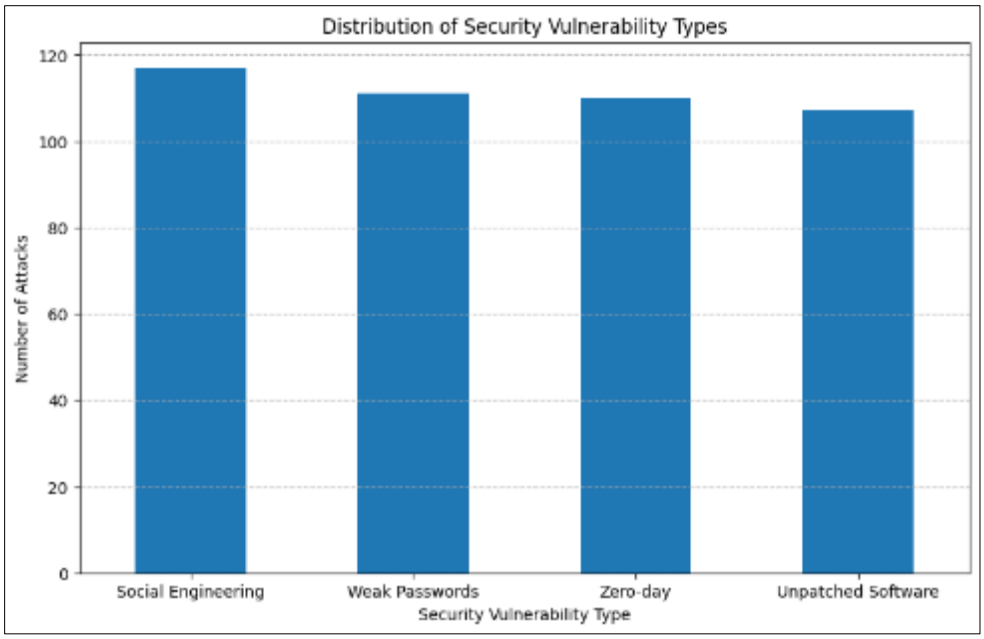

Figure 4 Distribution of Exploited Security Vulnerability Types in Financial Sector Cyberattacks (2015–2024)

The analysis of security vulnerability types exploited in financial sector cyberattacks indicates that social engineering was the most prevalent, reported in 117 cases. This was closely followed by weak password vulnerabilities (n = 111), zero-day exploits (n = 110), and unpatched software vulnerabilities (n = 107). These findings suggest that both human and technical weaknesses significantly contribute to the success of cyberattacks. The predominance of social engineering highlights the ongoing susceptibility of personnel to manipulation, reinforcing the need for robust cybersecurity awareness training. Similarly, the high frequency of weak passwords and unpatched systems reflects systemic lapses in basic security hygiene. The near-equal occurrence of zero-day exploits further underscores the advanced capabilities of threat actors and the necessity for proactive threat intelligence and real-time monitoring solutions within financial institutions.

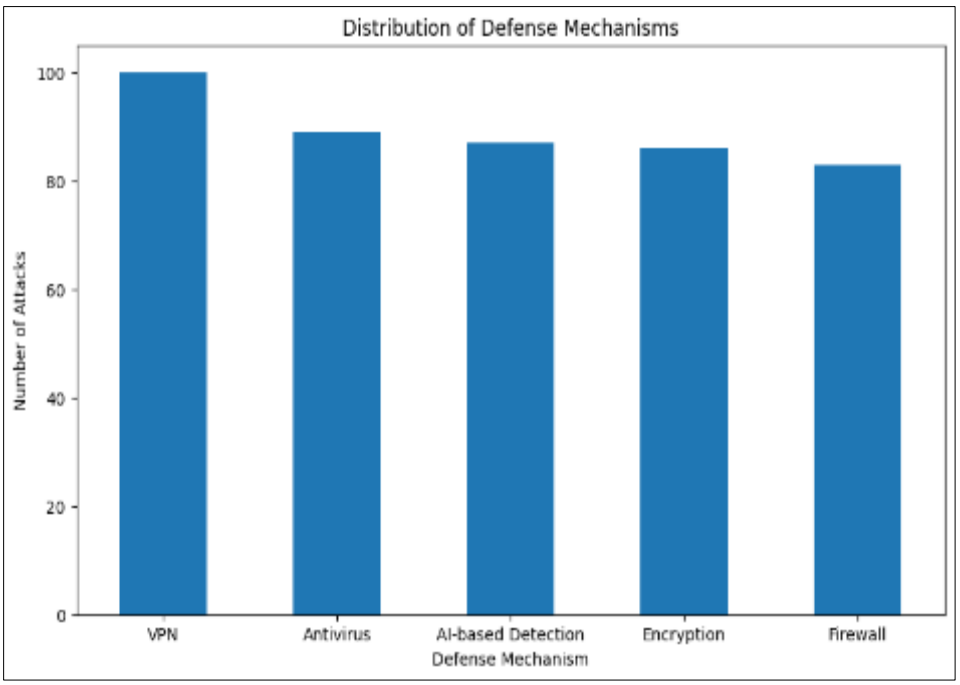

Figure 5 Distribution of Defense Mechanisms Used by Financial Institutions (2015–2024)

An examination of the defense mechanisms employed by financial institutions in response to cybersecurity threats reveals that Virtual Private Networks (VPNs) were the most used measure, with 100 reported instances. This was followed by antivirus software (n = 89), AI-based threat detection systems (n = 87), encryption technologies (n = 86), and firewalls (n = 83). The prominent use of VPNs suggests a strong emphasis on securing data transmission across networks, particularly in remote or distributed work environments. The frequent deployment of antivirus and encryption tools indicates adherence to foundational cybersecurity practices, while the notable use of AI-based detection reflects an emerging trend toward proactive and intelligent defense systems. However, the relatively close frequency across all defense types suggests a layered security approach, where institutions rely on multiple overlapping technologies to mitigate diverse threat vectors.

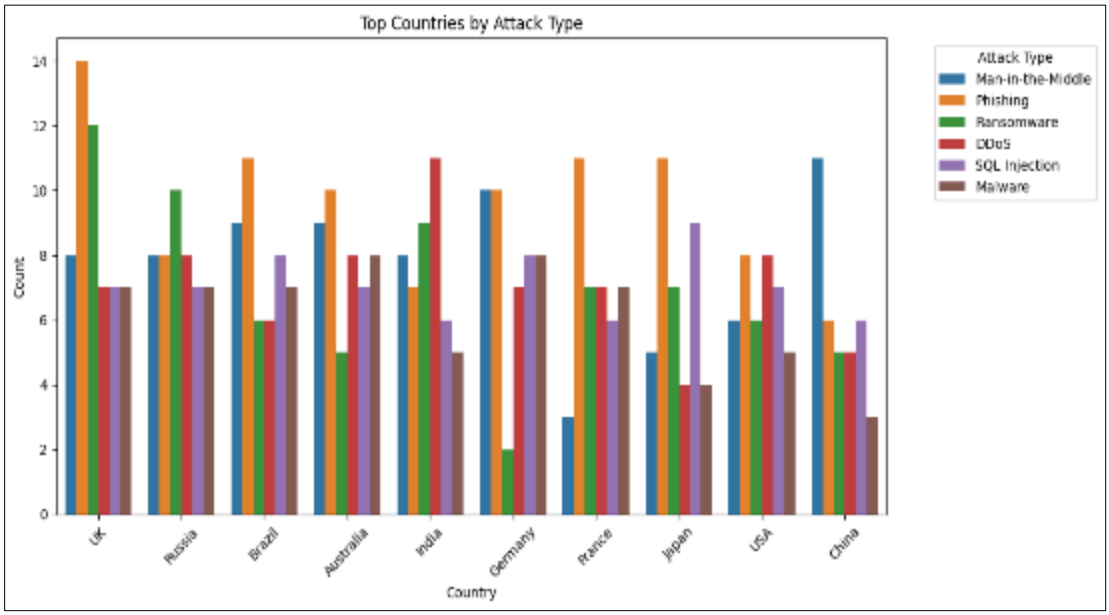

Figure 6 Cyberattack Type Distribution Across Top Ten Affected Countries (2015–2024)

The bar chart illustrates the distribution of various cyber-attack types across ten countries. Phishing consistently emerged as the most prevalent attack, with the UK (14) and France (11) reporting the highest counts. Ransomware incidents were notably high in the UK (12) and Russia (10). Man-in-the-middle attacks peaked in China (11) and Germany (10). DDoS attacks were most frequent in India (11). SQL injection and malware counts were generally moderate across countries. Overall, phishing remains the dominant threat, followed by ransomware and man-in-the-middle attacks.

4.1. Correlation Matrix

The correlation matrix shows weak relationships between variables in cybersecurity threats. No strong correlations appear, as most coefficients are near zero. Financial loss has a minimal association with the number of affected users (0.018) and incident resolution time (-0.082). Attack source and resolution also show a little correlation (-0.058). This implies that most of the variables operate independently in incidents.

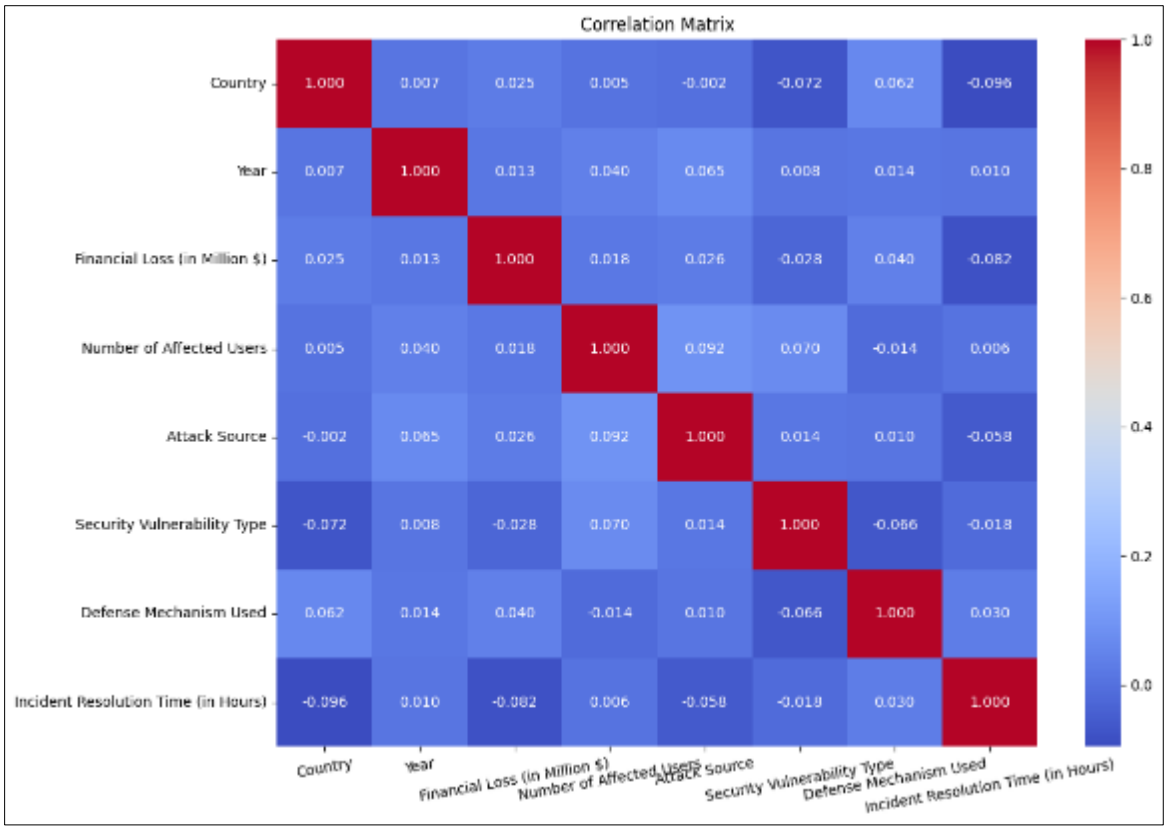

Figure 7 Correlation Matrix of Key Variables in Financial Sector Cybersecurity Incidents (2015–2024)

4.2. Model Performance Evaluation

4.2.1. Hyperparameters

Table 1 Optimal Hyperparameters for Random Forest and XGBoost Classifiers in Cyberattack Type Prediction

Metrics	Random Forest Classifier	XGBoost Classifier
Best n_estimators	300	100
Best max_depth	None (unlimited)	5
Best learning_rate	—	0.1
Best subsample	—	0.8
Best colsample_bytree	—	0.8
Best gamma	—	0
Best max_features	'log2'	Auto (default)
Best min_samples_split	2	—
Best min_samples_leaf	1	—

For the Random Forest Classifier (RFC), the optimal model utilized 300 trees (n_estimators = 300), with no maximum depth constraint (max_depth = None), a log base 2 strategy for feature selection (max_features = 'log2'), a minimum of 2 samples required to split a node (min_samples_split = 2), and a minimum of 1 sample per leaf node (min_samples_leaf = 1)..

In the Extreme Gradient Boosting Classifier (XGBC), the best-performing model used 100 boosting rounds (n_estimators = 100), a learning rate of 0.1 (learning_rate = 0.1), and a maximum depth of 5 (max_depth = 5). Additional optimal

parameters included a subsample ratio of 0.8 (subsample = 0.8), a column sampling ratio of 0.8 (colsample_bytree = 0.8), and a gamma value of 0 (gamma = 0).

Table 2 Performance Comparison of XGBoost and Random Forest Classifiers on Cyberattack Type Classification

Metric	XGBoost	Random Forest
Accuracy	0.809	0.787
Precision	0.816	0.789
Recall	0.809	0.787
F1 Score	0.809	0.786

The performance of the Random Forest Classifier (RFC) and XGBoost Classifier (XGBC) was evaluated using several classification metrics. The XGBoost Classifier consistently outperformed the Random Forest Classifier across all key metrics. Specifically, XGBC achieved an accuracy of 80.90%, higher than RFC's 78.65%. XGBC also demonstrated superior precision (81.62% vs. 78.87%), recall (80.90% vs. 78.65%), and F1 score (80.98% vs. 78.55%) based on weighted averages. These results show that the XGBoost model offers a more balanced and accurate approach to classifying cybersecurity attack types in the financial sector. Its stronger performance suggests a greater ability to capture complex patterns in the data, making it more suitable for real-world deployment in cyber threat detection systems.

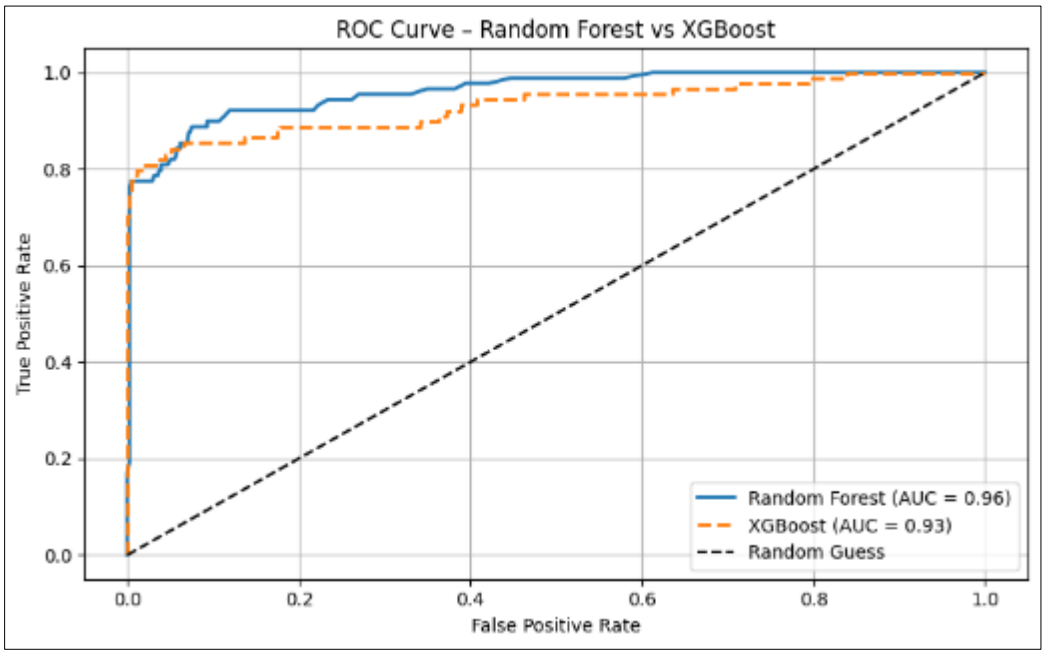

Figure 8 ROC Curve Comparison Between Random Forest and XGBoost Models for Cyberattack Type Classification

The receiver operating characteristic (ROC) curve analysis was conducted to evaluate the classification performance of the Random Forest and XGBoost models. The Random Forest classifier achieved an area under the curve (AUC) of 0.96, indicating excellent discrimination ability between classes. The XGBoost classifier also demonstrated strong performance with an AUC of 0.93. Both models significantly outperformed the baseline of random guessing (AUC = 0.50), as evidenced by the ROC curves lying well above the diagonal reference line. The higher AUC value of the Random Forest model suggests slightly superior classification accuracy and better sensitivity-specificity trade-off compared to the XGBoost model.

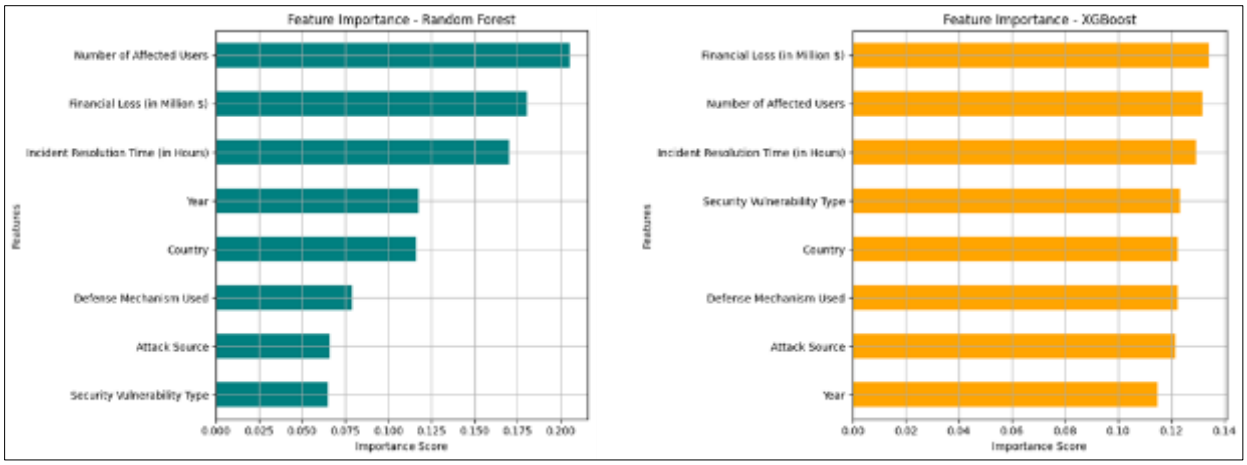

Figure 9 Feature Importance Comparison Between Random Forest and XGBoost Models

Analysis of the importance of the features revealed differences in how the Random Forest and XGBoost models prioritized predictors of cybersecurity attack types. In the Random Forest model, the number of affected users, financial loss, and incident resolution time emerged as the most influential features, indicating that the scale and impact of an incident heavily influence classification. In contrast, the XGBoost model distributed importance more evenly across features, though financial losses, number of affected users, and incident resolution time still ranked highest. Notably, XGBoost assigned relatively higher importance to categorical features such as security vulnerability type and attack source compared to Random Forest.

5. Discussion of Findings

The study examined cybersecurity threats in the financial sector between 2015 and 2024, focusing on the classification of attack types, identification of vulnerability patterns, and analysis of institutional response mechanisms across various geopolitical contexts. Using a structured dataset, multiclass classification models, random forest, and XGBoost were applied to predict attack types based on features such as country, financial loss, number of affected users, and defense strategies. The results revealed that phishing, man-in-the-middle attacks, and DDoS were the most prevalent threats, with phishing topping the list. Vulnerabilities were nearly all linked to social engineering, weak passwords, and zero-day exploits. Geopolitically, incidents were more frequent in countries with high digital exposure but relatively weaker regulatory enforcement.

Both the Random Forest and XGBoost models performed effectively in predicting attack types, with XGBoost slightly outperforming Random Forest. The tuned XGBoost model achieved an accuracy of 80.90% and a weighted F1-score of 80.98%, while Random Forest recorded 78.65% accuracy and an F1-score of 78.55%. ROC analysis further confirmed these results, with AUC values of 0.96 for Random Forest and 0.93 for XGBoost, indicating excellent discriminatory power. These outcomes suggest that ensemble-based classifiers can reliably predict attack typologies in the financial sector, especially when trained on high-quality, structured data. The improved performance of XGBoost may be attributed to its ability to handle feature interactions and weighted instances, which is advantageous in imbalanced multiclass settings. The consistent classification of attack types highlights the feasibility of developing predictive systems that can serve as early-warning tools, especially when integrated into cybersecurity operation centers in financial institutions.

Feature importance analysis revealed that both models consistently identified the number of affected users, financial loss, and incident resolution time as the most influential predictors. These features directly reflect the magnitude and institutional impact of an incident, indicating that attack severity is a strong determinant of attack typology. While Random Forest emphasized numerical predictors more heavily, XGBoost distributed importance more evenly, assigning greater weight to categorical variables such as security vulnerability type and attack source. This suggests that XGBoost may better capture nuanced patterns across diverse threat vectors. Notably, variables such as defense mechanisms used and year also contributed meaningfully, inferring temporal shifts in attack strategies and variation in institutional preparedness.

The study also provided a detailed breakdown of the types of vulnerabilities exploited and defense mechanisms employed across the financial sector. Social engineering and weak passwords were the most common vulnerabilities,

reflecting a persistent human factor in cyber risk. This finding suggests that despite technological advancements, behavioral lapses remain a major point of entry for attackers. Among defensive strategies, VPNs, antivirus tools, AI-based detection systems, and encryption were commonly used, though their effectiveness varied across regions and attack types. Institutions relying more on reactive measures, such as antivirus and firewalls, tended to experience longer resolution times.

The geopolitical context played a significant role in the nature and frequency of cybersecurity incidents observed. Financial institutions in countries with high levels of digital connectivity but low regulatory enforcement reported a higher number of breaches. This reveals a gap between digital innovation and cybersecurity governance. Countries with stringent data protection laws and cyber defense frameworks showed relatively fewer and less severe incidents, emphasizing the importance of regulatory maturity.

6. Conclusion

This study examined cybersecurity threats in the financial sector from 2015 to 2024, analyzing attack types, vulnerability patterns, and institutional response mechanisms. Using machine learning models, it identified phishing and man-in-the-middle attacks as dominant threats, with social engineering and weak passwords as key vulnerabilities. Both Random Forest and XGBoost models demonstrated strong predictive capabilities, with XGBoost slightly outperforming. The findings highlight the importance of data-driven risk modeling, proactive defense strategies, and policy reforms. Mitigating cyber threats in finance requires not only technical innovation but also coordinated action across institutional, technological, and geopolitical boundaries.

Recommendations

- Implement AI-driven threat detection systems to proactively identify and classify potential cyberattacks in real time.
- Mandate regular cybersecurity awareness training for all financial sector employees to reduce social engineering risks.
- Adopt and enforce multi-factor authentication (MFA) and strong password policies to combat credential-based attacks.
- Invest in cross-border cyber intelligence sharing platforms to enhance regional and global incident response coordination.
- Integrate predictive machine learning models into institutional cybersecurity workflows for dynamic threat monitoring and early warning alerts.

Compliance with ethical standards

Disclosure of conflict of interest

The authors disclose that there is no conflict of interest to be disclosed.

References

[1] Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. . Information, 15(11), 682.

[2] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning. Journal of Cybersecurity and Privacy, 2(3), 527-555.

[3] Alavi, S. (2023). The Evolution of Cyber Conflicts and its Impact on International Security: A Comprehensive analysis.

[4] Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications, 14(7), 1185-1191.

[5] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics. 11(20), 3330.

[6] Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. International Journal of Science and Research Archive, 11(1), 1304-1310.

[7] Azubuike, C. F. (2023). Cyber security and international conflicts: An analysis of state-sponsored cyber attacks. Nnamdi Azikiwe Journal of Political Science, 8(3), 101-114.

[8] Boysen, S., Hewitt, B., Gibbs, D., & McLeod, A. (2019). Refining the threat calculus of technology threat avoidance theory. Communications of the Association for Information Systems, 45(1), 5.

[9] Cappa, F., Oriani, R., Peruffo, E., & McCarthy, I. (2021). Big data for creating and capturing value in the digitalized environment: unpacking the effects of volume, variety, and veracity on firm performance. . Journal of Product Innovation Management, 38(1), 49-67.

[10] Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. . Communications of the Association for Information Systems, 44.

[11] Cavelty, M. D. (2024). The politics of cyber-security. Taylor & Francis.

[12] Chen, D. Q., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. IEEE Transactions on Engineering Management, 66(4), 552-567.

[13] Galushchenko, O., Pidbereznykh, I., Piroh, O., Khrapach, D., & Tolmachov, O. (2024). Cybersecurity and geopolitical dimensions of external information interventions in Ukraine: Analysis of current trends.

[14] George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51-75.

[15] Gillam, A. R., & Waite, A. M. (2021). Gender differences in predictors of technology threat avoidance. Information & Computer Security, 29(3), 393-412.

[16] Górnicka, L., Ogawa, S., & Xu, T. (2023). Addressing Corporate Sector Vulnerabilities. In India's Financial System. International Monetary Fund.

[17] Gul, S., & Malik, W. (2024). Cyber Conflict and International Security: Legal Challenges and Strategic Solutions in Cyberspace. The Journal of Research Review, 1(4), 305-314.

[18] Hong, J. H. (2021). AI-Driven Threat Detection and Response Systems for Cybersecurity: A Comprehensive Approach to Modern Threats. Journal of Computing and Information Technology, 1(1).

[19] Ibekwe, K. I., Nwokediegwu, Z. Q., Umoh, A. A., Adefemi, A., & Ilojianya, V. I. (2024). Energy security in the global context: A comprehensive review of geopolitical dynamics and policies. . Engineering Science & Technology Journal, 5(1), 152-168.

[20] Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Computer Science.

[21] Jeyaraj, A., Zadeh, A., & Sethi, V. (2021). Cybersecurity threats and organisational response: textual analysis and panel regression. Journal of Business Analytics, 4(1), 26-39.

[22] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 564-74.

[23] Khan, A. W., Saeed, S., & Kakar, M. S. (2024). Cybersecurity As A Geopolitical Tool: The Growing Influence Of Digital Warfare In Statecraft. International Research Journal of Social Sciences and Humanities, 3(2), 345-357.

[24] Kundavaram, R. R., Onteddu, A. R., Nizamuddin, M., & Devarapu, K. (2023). Cybersecurity Risks in Financial Transactions: Implications for Global Trade and Economic Development. Global Disclosure of Economics and Business, 12(2), 53-66.

[25] Meiqi, G. (2024). Infrastructure security and cyber resilience in the context of geopolitical tensions: new challenges and coping strategies (Master's thesis, NTNU).

[26] Montasari, R. (2024). Introduction: Cyberspace, cyberterrorism and the international security in the fourth industrial revolution: Threats, assessment and responses. . In In Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses (pp. 1-15). Cham: Springer International Publishing.

[27] Mwangi, P. (2024). Cybersecurity Threats and National Security in the Digital Age. American Journal of International Relations, 9(1), 26-35.

[28] Naseeb, J., & Tariq, A. (2024). Impact of cyber-attacks on national security and international relations. . International Journal for Conventional and Non-Conventional Warfare, 1(1), 86-96.

[29] Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286-2295.

[30] Rugina, J. M. (2023). Through the eyes of attackers: A comprehensive analysis of cybersecurity strategies in international relations. Afro Eurasian Studies, 12(1), 40-57.

[31] Saaida, M. (2023). The Use of Cyber Warfare and its Impact on International Security.

[32] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369.

[33] Sankaram, M., Roopesh, M., Rasetti, S., & Nishat, N. (2024). A Comprehensive Review Of Artificial Intelligence Applications In Enhancing Cybersecurity Threat Detection And Response Mechanisms. Management, 3(5).

[34] Umar, S., & Butler, J. (2021). AI in Cybersecurity: Transforming Threat Detection and Response Mechanisms.

[35] Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. International Journal of Science and Research Archive, 11(1), 1810-1817.