AI-Augmented Proactive Cyber-Detection and Mitigation of Cybersecurity Threats in the Banking Sector

Prince Rotondwa Mulea and Dewald Blaauw
Department of Information Science, Stellenbosch University, South Africa

Princeroem@gmail.com
Dnblaauw@sun.ac.za

Abstract: The digital transformation of the financial services sector, accelerated by the emergence of neobanks and advanced online platforms, has markedly increased its exposure to sophisticated cyberthreats. High-profile incidents, such as coordinated attacks on financial institutions in Iraq, have demonstrated the severe operational, economic, and reputational consequences that can arise from delayed threat detection and inadequate mitigation. Traditional cybersecurity measures, including firewalls, antivirus software, and signature-based intrusion detection systems, remain constrained by their dependence on known attack signatures, thereby leaving financial networks susceptible to zero-day exploits, AI-driven intrusions, and complex multi-vector threats. This study proposes and evaluates a supervised machine learning intrusion detection and prevention model aimed at proactively securing financial networks at a network level. To simulate realistic network conditions and generate representative traffic data, a banking environment was constructed using GNS3. To address class imbalance within the dataset, the Synthetic Minority Oversampling Technique (SMOTE) was employed, thereby improving the detection of minority-class attack instances. Several machine learning algorithms, including Support Vector Machine, Multi-Layer Perceptron Neural Network, and Long Short-Term Memory, were assessed using key performance metrics to determine their effectiveness. The Decision Tree model demonstrated superior performance, achieving an accuracy rate of 99.98%, perfect precision and recall, zero false positives, and only thirteen false negatives. These results underscore its capacity to deliver highly accurate, real-time threat detection while minimising operational disruptions caused by false alarms. Its transparent decision-making process enhances explainability, supports regulatory compliance, and fosters institutional trust, factors that are critical in financial cybersecurity. The findings validate the viability of interpretable, high-performance machine learning models for the real-time detection and mitigation of advanced cyberthreats, including Distributed Denial-of-Service (DDoS) attack patterns. Future research should prioritise scaling the simulation framework to encompass more complex financial network topologies, integrating adaptive online learning capabilities, and incorporating explainable artificial intelligence (XAI) techniques to investigate whether enhanced model interpretability improves threat detection accuracy and analyst response times.

Keywords: Machine learning, Cybersecurity, Cyberattacks, Financial networks, Banking sector

1. Introduction

The universal banking model, encompassing institutions that provide a wide range of financial services beyond traditional lending and payments, has historically shaped the global financial sector. Over time, this model has evolved through digital-first strategies, advanced data capabilities, and new technologies that enhance service delivery and competitiveness. Traditionally, high entry barriers limited competition, reinforcing the dominance of universal banks. However, the rise of neobanks, also referred to as digital banks, lowered these barriers and disrupted the sector's competitive landscape. Unlike the traditional model, modern banking now emphasises customer engagement, personalisation, and agile core systems, shifting priorities from sales and services to consumer experience.

While the digitisation and digitalisation of the financial sector, along with the integration of neobanks, have positively impacted the sector's productivity and operations, these technological advancements have also heightened cybersecurity threats within the financial industry. Beyond traditional security risks such as financial information breaches, cyberattacks now pose systemic challenges to financial infrastructure. These cyberattacks, which are the primary focus of this study, threaten not only banking stability but also national security and economic resilience.

The increasing frequency and sophistication of cyberattacks underscore the pressing need for solutions that not only respond to incidents post-occurrence but also proactively detect and mitigate malicious activities in real time, ensuring that threats such as large-scale fraud attempts are intercepted at their earliest stages. Consequently, effective mitigation strategies must operate in tandem with proactive detection mechanisms, establishing a multi-layered defence system capable of addressing both known and emerging threats. The mitigation of these attacks involves the utilisation of artificial intelligence (AI) tools and traditional cybersecurity measures.

This study proposes a potential solution for safeguarding the financial sector at a network level against cyberthreats and cybercriminals through the utilisation of AI tools. However, the accelerating speed and increasing complexity of contemporary threats have exposed the limitations of traditional cybersecurity systems, thereby underscoring the imperative for intelligent, adaptive models that can learn from and respond to evolving attack patterns.

2. Literature Review

The literature review examines cybersecurity within the banking sector, highlighting the integration of AI and ML as critical tools for enhancing security.

2.1 Cybersecurity and the Presence of AI in Cybersecurity of the Banking Sector

Technological developments in computational capacity and real-time communication have financial operations, enabling intelligent data management and information sharing while exposing institutions to risks such as system compromise, data breaches, and unauthorised access (Duque & Omar, 2015). In response, financial security emphasises confidentiality, integrity, and availability of stored data. Ensuring business continuity requires resilient, affordable security systems that reduce economic and organisational impact of cyberattacks (Von Solms & Van Niekerk, 2013). One framework, the System of Systems (SoS), integrates multiple security systems to identify evolving risks and implement proactive defence mechanisms.

Traditional cybersecurity measures within the banking sector include Device management via consistent updates; Organisational risk management; and Investment in employee training. Abdulrahman (2020) notes popular strategies by financial executives to lower cyber risks mandatory awareness training and allocating sufficient funds for security. Skills shortages among cybersecurity employees, particularly in technical expertise and communication, remain a significant challenge. The incorporation of AI into cybersecurity strategies reduces errors and expenses while enhancing security. Banks employ ML, deep learning (DL), and natural language processing (NLP) to detect and prevent cyber threats (Prince et al., 2024). These tools can process vast amounts of data and identify patterns, thereby enhancing the efficiency of cyber threat detection. AI techniques facilitate rapid detection and prevention of risks, ensuring high security standards to prevent data breaches. The incorporation of AI has enhanced archaic cybersecurity techniques in banking employing encryption software to keep cybercriminals away from their confidential information and online transactions (Mhlanga, 2020). Over time, ML algorithms adapt by learning from past data, enabling them to recognise anomalies and predict attacks more effectively than static, rule-based systems.

Banks prioritise cybersecurity due to sensitive client data. Safeguards include ATM validation, OTP confirmation, and pre-enrolment with signature authorisation. AI, while beneficial for cybersecurity, introduces adversarial attacks that manipulate training data to deceive ML models (Prince et al., 2024). Despite risks, AI is significant in detecting malware and ransomware early, automating monitoring, and freeing security professionals for strategic tasks. The reliance on AI in cybersecurity fuels rapid expansion of AI-driven security markets, reflecting demand for adaptive defence systems. AI is positioned not merely as a supplementary tool but central to modern banking cybersecurity.

2.2 Overview of Machine Learning Techniques for the Financial Sector

Machine learning techniques (MLTs), illustrated in figure 1, are critical in protecting banking systems. ML is used to predict loan approvals, detect fraudulent transactions, and monitor anomalies (Nuthalapati, 2023). Financial institutions deploy ML and DL against sophisticated cyber threats, mirroring technologies used by cybercriminals.

Modern attacks demand adaptive and proactive strategies (S. Mishra, 2023). ML enables real-time threat detection through analysis of large datasets, anomaly identification as early warnings, and continuous adaptation to emerging cyber threats (Prince et al., 2024). However, ML introduces vulnerabilities. Adversarial ML can distort threat assessments, hence creating vulnerabilities in security systems. To mitigate this, institutions train ML algorithms on accumulated data to identify behavioural patterns associated with breaches, strengthening predictive accuracy. AI automates detection and response, enhancing efficiency. Subcategories include: DL uses neural networks to detect anomalous network traffic patterns and identify malware. NLP enhances threat intelligence in the deployment of self-response systems, i.e. chatbots, and text retrieval. Reinforcement learning modifies defence tactics identifying new environmental interactions and improving security measures. Behaviour analytics use User and Entity Behavioural Analytics (UEBA) identify insider threats, unauthorised account compromises, or other suspicious behaviour.

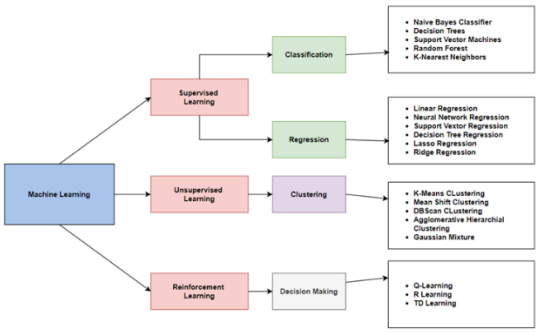

Figure 1: Machine Learning Techniques in Financial Sector

Supervised learning forecasts and categorises data, with Naïve Baye Classifier (NBC), Decision Tree (DT), Support Vector (SV), Linear Regression (LR), and K-Nearest Neighbours (KNN) as examples. Unsupervised learning techniques investigate hidden patterns in data without training datasets, labelled data, or predicted results. The main objective of this learning technique is for data clustering, often via Mean shift Clustering (MSC), and K-Means Clustering (KMC). Reinforcement learning strategies observe the system's environment, execute control, and optimise cumulative rewards. Q learning, R-Learning, and TD-Learning are instances of reinforcement learning algorithms.

ML algorithms analyse historical data to detect deviations from normal user behaviour, network traffic, or system activity patterns. ML enhances adaptability and self-learning of digital banking systems, strengthening security. Such adaptability ensures persistent protection of sensitive assets (S. Mishra, 2023). Digital banks benefit from incorporating ML into their cybersecurity protocols, enabling rapid threat response and safeguarding assets. ML-based cybersecurity solutions in digital banking should also address ethical issues that come with their use in the financial sector. MLTs in finance are applied in data collection, quality checks, cleansing, feature engineering, training and validation, monitoring, incident response, evaluation, updates, and privacy protections.

3. Method

In this section the methodology employed to conduct the study and obtain the findings is described. It provides an overview of the study's tools and research design. The choice of research approach is justified in this section. A real-world case study is incorporated to contextualize the experimental setup and validate the applicability of the proposed approach to practical financial environments. The implementation of network analysis using Wireshark and the creation of a secure cyber financial network using GNS3 are described. It presents practical work employing Kali-Linux to launch targeted network cyberattacks. Data is gathered from the network under analysis both prior to and during the attacks. The procedures used to develop the ML algorithm for identifying and preventing cyberattacks are thoroughly illustrated in this section.

3.1 Research Design

The technologies currently employed in the banking industry and cybersecurity procedures that are required are investigated in this study using both a qualitative and quantitative methodology.

Quantitative research is the methodical study of phenomena through the collection of quantifiable data and the use of statistical, mathematical, or computational methods (Recker, 2021). Researchers and statisticians employ mathematical frameworks and concepts related to the quantity under investigation in the research approach. This research will benefit from a quantitative approach, as its objective is to identify vulnerabilities and develop an algorithm for cybercrime defence within financial services systems at a network level. The study utilises Kali Linux to simulate real-world cyber threats and vulnerabilities in the banking industry. The study also utilises Kali Linux's penetration testing tools to collect data on attack vectors, analyse security gaps, and iteratively refine the algorithm based on observed patterns and insights. An actual financial network will be replicated by an emulated cyber security financial network. Graphical Network Simulator-3 (GNS3) will be used as a simulation tool or software for designing and creating the financial network. GNS3 is an open-source platform that is used to record data traffic in real time and to construct intricate networks. Wireshark, which establishes a path for the data MTL method, will be used to analyse network data flow.

Recker (2021) asserts that a qualitative approach is useful for contextualising real-life events. A qualitative methodology is applicable in this study, as its objective is to explore cybersecurity in the context of the financial services industry at a network level. This study will investigate a case study on what systems are in place to track, monitor, protect and respond to cyber threats. This approach enables the study to investigate the cybersecurity measures financial institutions have implemented on their systems at a network level, be it online or offline protocols, machines or people. The investigation aids in identifying the optimal cybersecurity measures necessary for the existing networks. The experimentation process involves simulating controlled scenarios within a standardised financial sector network to systematically collect data for ML applications. Python is utilised for data analysis, model development, and performance evaluation in ML applications. To facilitate these tasks, the open-source web-based tool Jupyter Notebook is employed, offering a comprehensive suite of libraries and frameworks specifically designed for such purposes.

This study focuses on enhancing cybersecurity within the financial sector through the application of ML algorithms. It is important to emphasise, however, that the aim is not to completely redesign or replace existing cybersecurity frameworks, nor to conduct comparative analyses. Furthermore, it should also be noted that this study did not involve actual physical penetration testing on live networks.

3.2 Case Study: Cyber-Attacks and Cybersecurity Readiness of Iraqi Private Banks

The increasing digitisation of financial services has brought unprecedented convenience to consumers while simultaneously exposing financial institutions to escalating cybersecurity threats. According to the World Bank's Global Findex Database, global account ownership rose from 51% in 2011 to 76% in 2021, with digital payments usage in emerging economies increasing from 35% to 57% over the same period (World Bank Group, 2022). Iraq, as part of this global trend, has witnessed a growing reliance on digital financial services, making its banking infrastructure a target for cybercriminals. Against this backdrop, (Hasan et al., 2021) investigated the cybersecurity readiness of Iraqi private banks, providing a representative case of the challenges faced by financial institutions in emerging economies.

The study adopted a questionnaire-based methodology to compensate for the limited availability of official data on cyber incidents within Iraq's banking sector. A total of 51 responses were collected from clients residing in Baghdad, Karbala, Babel, and Najaf, thereby reflecting perspectives from central regions of the country. The demographic profile of respondents indicated a male majority, 62.7%, with the largest age group being 36-45 years, 51%. Furthermore, more than half of participants reported four to six years of technology use, suggesting a reasonably experienced user base. The investigation focused on five primary categories of cyber threats: cyberstalking, hacking, phishing, cross-site scripting (XSS), and DDoS attacks. Cybersecurity readiness was conceptualised as the dependent variable, measured through eight questionnaire items, while each cyber threat represented an independent variable. Findings revealed that cyberstalking was a recurring issue, with consumers reporting experiences of harassment, blackmail, and extortion attempts while accessing banking services. Hacking was also perceived as a major risk, particularly in relation to the use of insecure applications and public Wi-Fi, though actual instances of credential theft were less frequent. Phishing emerged as one of the most significant concerns, with participants highlighting exposure to fraudulent links, deceptive emails, and counterfeit websites designed to harvest sensitive information. Similarly, XSS vulnerabilities were evident, with users frequently redirected to malicious websites through misleading content, while DDoS attacks reflected customer fears regarding the capacity of banks to ensure data protection and service continuity.

Statistical analysis, however, indicated no significant relationship between cybersecurity readiness and the independent variables, with hacking even demonstrating a negative correlation. This suggests that, despite growing awareness of cyber threats, Iraqi banks' defensive strategies have not instilled sufficient consumer confidence. Respondents consistently expressed scepticism regarding the sector's ability to secure online transactions, citing the prevalence of insecure public internet connections and the frequency of cyberattacks as key factors undermining trust.

The study's conclusions are prominent in the post-pandemic context, as financial pressures and increased digital reliance have amplified cybercrime globally. Iraqi banks, while actively working to improve their cybersecurity infrastructure, remain constrained by persistent vulnerabilities and a gap between perceived risks and actual preparedness. The case study underscores the pressing need for enhanced technical support, robust frameworks, and proactive strategies to address the evolving threat landscape. Through situating Iraq's experience within the broader discourse on cybersecurity in financial institutions, this case study highlights both the localised challenges of emerging economies and the universal need for adaptive, technology-driven solutions. Building on these findings, subsequent research proposes an AI-based cybersecurity framework

designed to strengthen detection and mitigation capabilities, thereby bridging the gap between institutional readiness and the sophistication of modern cyberattacks.

3.3 Research Instruments

This study employed a suite of simulation, virtualisation, penetration testing, and data analysis tools to design, evaluate, and secure a financial network environment. The primary setup comprised GNS3 and VMware, integrated with Kali Linux, supported by an 11th Gen Intel Core i7 processor, 8 GB RAM, Windows 11 (64-bit) operating system. GNS3 served as the main platform for emulating a financial network. It enabled the design and testing of complex topologies using virtual and physical devices. GNS3 is valued for its flexibility, scalability, and cost-effectiveness, supporting devices from Cisco, Juniper, MikroTik, and others. For this study, GNS3 version 3.0.5 was used in conjunction with VMware for improved performance. VMware Workstation Player (v17.6.3) was employed as the preferred virtualisation tool due to its efficiency and support for multiple operating systems. Its compatibility with GNS3 and free availability made it optimal for the study's requirements.

Kali Linux, an open-source Debian-based operating system, provided penetration testing capabilities to simulate cyberattacks. Its suite of tools, such as Yersinia, Ettercap, hping3, Nmap (network mapping), Netcat (port scanning), Scapy (packet manipulation), and Ping was used to exploit vulnerabilities in the emulated network. Wireshark, a packet analyser, captured and analysed traffic within the simulated network, exporting data for pre-processing and further analysis. For data processing and machine learning, Python was selected due to its readability and extensive libraries. Key modules included NumPy, SciPy, Pandas, Scikit-learn, Seaborn, and Logging, enabling statistical computation, data transformation, model development, and visualisation. Jupyter Notebook facilitated implementation, combining live code, analysis, and documentation. Collectively, these instruments ensured a robust experimental environment for simulating, analysing, and mitigating cybersecurity threats in financial systems at a network level.

3.4 Bank Architecture

Modern banking architecture is essential for cross-enterprise intelligence, analytics, compliance, and security (Keen et al., 2018). The rise of smartphones, blockchain, cloud computing, AI, Internet of Things (IoT), and open APIs has driven intelligent digital banking, enabling customer-centric, technology-driven services. The financial sector now extends beyond traditional lending to include investments, portfolio management, and lifestyle services. Emerging technologies such as AI-powered chatbots, robot-advisors, fraud detection, automation, and gamification enhance personalisation and risk management. Big Data supports smart banking, segmentation, and churn analysis, while IoT enables account automation and real-time services. Blockchain applications include open banking APIs, digital wallets, smart contracts, and central bank digital currencies. Biometrics and cloud computing further strengthen authentication and core banking flexibility.

The study adopts a Service-Oriented Architecture (SOA), depicted in figure 2, enabling interoperability and integration across distributed systems. SOA's modular, reusable, and open-standards-based design overcomes the rigidity of legacy ICT infrastructures, facilitating adaptability, seamless application integration, and strategic enterprise value (Meredith & Bjorg, 2003).

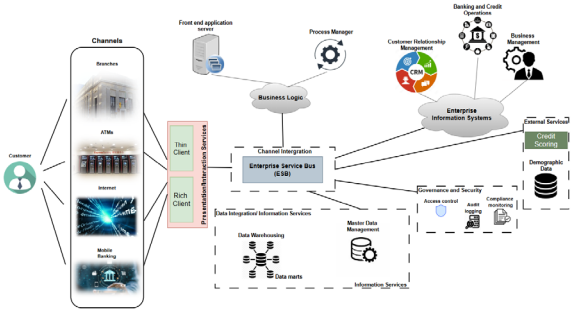

Figure 2: Bank Architecture

3.5 Cybersecurity of Bank Architectures and AI Integration

Cybercrime in banking encompasses identity theft, fraud, malware, and intrusions aimed at disrupting operations or stealing sensitive data (S. Mishra, 2023). Traditional security strategies often struggle with scalability and advanced threats, highlighting the need for comprehensive cyber-risk management. Banks rely on encryption, firewalls, intrusion detection systems (IDS), and mobile security to safeguard customer data and

maintain trust. A robust security program integrates policies, protocols, and tools to ensure confidentiality, integrity, and availability while complying with financial regulations. The components of the financial sector cybersecurity, include secure payments, data protection, and mobile safeguards. AI enhances these frameworks by automating repetitive tasks, providing real-time threat detection, and strengthening predictive capabilities. Applications include spam filtering, fraud detection, biometric authentication, and behavioural analytics.

3.6 Security Concerns in Financial Networks

Financial networks face increasing cyber threats targeting both institutional IT infrastructure and customers, often compromising transaction data or monitoring systems. Among the most prevalent are DDoS attacks, which overwhelm servers with malicious traffic, disrupting core banking, payment processing, and ATM services. Man-in-the-Middle (MitM) attacks intercept and alter communication channels, enabling attackers to reroute funds, inflate credit limits, or suppress compliance alerts, thereby undermining operational integrity. Cryptojacking exploits institutional computing resources for unauthorised cryptocurrency mining, degrading system performance, increasing costs, and impacting transaction and payment systems. Credential stuffing uses automated tools and stolen login data to infiltrate financial systems, facilitating fraud, data theft, and reputational damage. To mitigate these risks, institutions emphasise unique credentials, anomaly monitoring, and multi-factor authentication (MFA).

3.7 Machine Learning Process

The proposed methodology is illustrated in Figure 3. Three datasets were prepared. Each processed into thirteen features and divided into training (70%), validation (30%), and a separate testing set. The model was trained and refined through hyperparameter tuning, with its primary function to classify network traffic and detect cyberattacks, and its secondary role to enforce firewall rules by blocking suspicious packets while permitting legitimate ones.

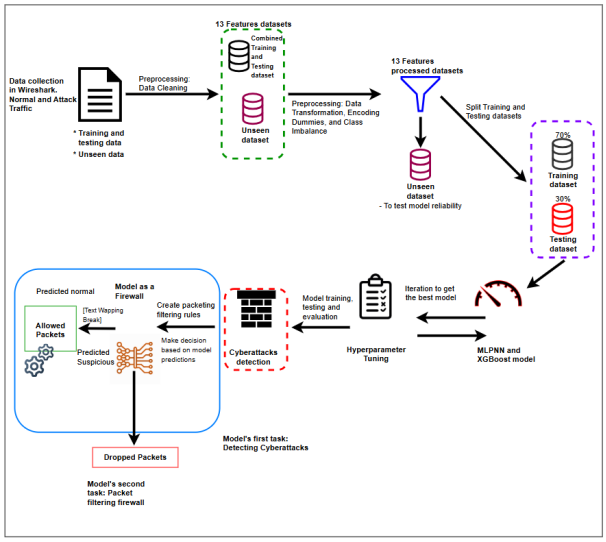

Figure 3: Model Architecture and Methodology

Data acquisition was central to the process. Real-time network traffic was recorded before and during simulated cyberattacks, including DDoS, MitM, False Data Injection Attacks (FDIA), and Credential stuffing. Wireshark was used to capture traffic, evident in figure 4, given its accuracy in packet analysis. Extracted features included IP and MAC addresses, ports, TTL values, protocol flags, and ICMP codes. Normal traffic was also recorded to establish baseline behaviour. Activities performed during acquisition included generating audit and transaction logs, data transfers, file uploads, file relocation, server access, and network reachability checks. This structured dataset enabled the model to learn patterns of normal versus malicious activity, ensuring robust evaluation across unseen scenarios.

Time	Src_IP	Dst_IP	Protocol	Src_Port	Dst_Port	Src_MAC	Dst_MAC	Time_to_Live	Flag	ICMP_Type	ICMP_Code	Packet_Cate
42292	10.10.10.100	10.10.10.15	HTTP	45378.0	8080.0	PCSSystemtec_b4a1:05	0cb1:3d:44:00:00	64	0x018	NaN	NaN	Mali
61375	10.10.10.15	10.10.10.100	HTTP	8080.0	45378.0	0cb1:3d:44:00:00	PCSSystemtec_b4a1:05	64	0x019	NaN	NaN	Mali
74663	10.10.10.100	10.10.10.15	HTTP	45388.0	8080.0	PCSSystemtec_b4a1:05	0cb1:3d:44:00:00	64	0x018	NaN	NaN	Mali
79185	10.10.10.15	10.10.10.100	HTTP	8080.0	45388.0	0cb1:3d:44:00:00	PCSSystemtec_b4a1:05	64	0x019	NaN	NaN	Mali
94515	10.10.10.100	10.10.10.15	HTTP	45392.0	8080.0	PCSSystemtec_b4a1:05	0cb1:3d:44:00:00	64	0x018	NaN	NaN	Mali
96714	10.10.10.15	10.10.10.100	HTTP	8080.0	45392.0	0cb1:3d:44:00:00	PCSSystemtec_b4a1:05	64	0x019	NaN	NaN	Mali
04574	10.10.10.100	10.10.10.15	HTTP	45404.0	8080.0	PCSSystemtec_b4a1:05	0cb1:3d:44:00:00	64	0x018	NaN	NaN	Mali

Figure 4: Sample of Dataset

3.7.1 Data preprocessing

Preprocessing was the foundational step, ensuring raw network traffic data was systematically organised, transformed, and cleansed for machine learning. This phase addressed issues such as noise, incompleteness, high dimensionality, and class imbalance to enhance model accuracy and reliability.

3.7.2 Data cleaning

Missing or incomplete values, particularly across protocol-specific fields, were handled without discarding rows. Instead, missing entries were substituted with zeros, retaining critical records while ensuring dataset consistency.

3.7.3 Data transformation

The dataset was split into training (70%) and validation (30%) subsets and transformed through feature engineering, normalisation, and encoding. IP and MAC addresses were hash-encoded, protocols one-hot encoded, and Boolean values converted to integers. A critical step was addressing the pronounced class imbalance in Packet_Category using SMOTE. Unlike random oversampling, SMOTE generated synthetic minority-class samples by interpolating between nearest neighbours, enhancing diversity and reducing overfitting risks. Stratified sampling, maintained class proportions across all subsets, ensuring robust and generalisable evaluation.

3.7.4 Model selection

The study evaluated four models: Decision Tree, Support Vector Machine (SVM), Multilayer Perceptron Neural Network (MLPNN), and Long Short-Term Memory (LSTM), to determine the most effective approach for detecting financial network cyberattacks. Given the dataset's complexity, the chosen model needed to handle heterogeneous variables, capture non-linear relationships, and deliver high interpretability for real-world cybersecurity.

The Decision Tree classifier emerged as the strongest performer, achieving 99.98% accuracy with precision, recall, and F1 scores all exceeding 99.97%. Its confusion matrix showed zero false positives and only 13 false negatives out of nearly 60,000 samples, minimising risks of undetected threats or false alarms. Beyond its accuracy, the model's interpretability was pivotal: top features such as Flag, IP/MAC addresses, ports, and TTL values provided transparent insights into malicious traffic patterns. The tree's structure illustrated clear, low-impurity decision paths, reinforcing analyst trust and supporting timely, accountable threat response. SVM, MLPNN, and LSTM also delivered strong performance, with accuracies ranging from 98.99% to 99.92%. However, SVM produced higher false positives, MLPNN slightly increased misclassifications, and LSTM, though accurate, lacked the Decision Tree's interpretability. Performance evaluation confirmed the Decision Tree's reliability, generalisation, and operational suitability. Its combination of accuracy, zero false positives, and transparent decision-making established it as the optimal model for financial cybersecurity at a network level.

4. Findings and Analysis

This section presents the findings derived from the previous sections. The section contains documentation of the analysis of the findings. The performance evaluation of the proposed machine learning algorithm in detecting and mitigating cyberattacks within financial systems at a network level and visual representations. It reviews datasets, pre-processing methods, literature insights, and model performance.

The literature revealed that the financial sector faces distinct and complex cybersecurity challenges at a network level, as it manages sensitive data and high-value transactions. Traditional, rule-based measures are increasingly inadequate against evolving threats, while AI and ML have become essential for real-time detection and response. However, challenges such as adversarial AI, a shortage of skilled personnel, and reliance on reactive strategies persist. Simulated environments like GNS3 offer controlled conditions for training AI models, underscoring the importance of predictive and proactive approaches.

The case study of private banks in Iraq highlighted weak institutional readiness despite growing awareness of cyber risks. Frequent threats, including phishing, DDoS, and hacking, were reported, yet responses remained ad hoc, lacking structured strategies. Respondents also identified unsecured networks, poor data confidentiality, and insufficient user training as major concerns, revealing a disconnect between policy and implementation.

The datasets were generated in a simulated financial network, illustrated in figure 5, using Wireshark, capturing attributes such as IP and MAC addresses, ports, flags, protocols, and ICMP codes. These were divided into

training, validation, and testing subsets to ensure reliable performance evaluation. Data pre-processing included cleaning and encoding, while SMOTE was applied to address class imbalance. By generating synthetic samples, SMOTE reduced overfitting and enhanced generalisation, contributing significantly to model robustness.

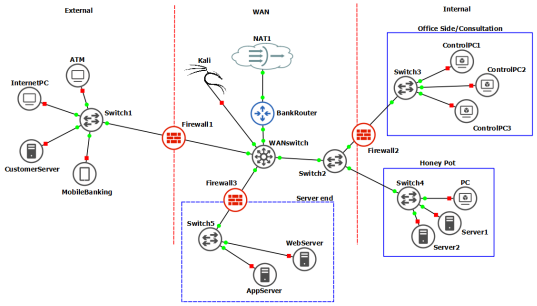

Figure 5: Hypothetical Bank network in GNS3

Among the tested algorithms, the Decision Tree proved most effective, achieving 99.98% accuracy with zero false positives and only 13 false negatives. Compared with SVM, MLPNN, and LSTM, it offered superior interpretability, efficiency, and compliance readiness. Feature importance analysis identified the Flag attribute as most critical, while the confusion matrix confirmed strong precision, recall, and balanced classification. These results establish the Decision Tree as the most suitable model for deployment in financial cybersecurity systems at a network level.

5. Conclusion

This study, supported by a real-world case of cyberattacks on Iraqi banks, developed a supervised machine learning model for proactive intrusion detection and prevention in financial networks. Using GNS3-simulated environments, Wireshark-captured traffic, and SMOTE pre-processed datasets, a Decision Tree algorithm achieved exceptional accuracy (99.98%), precision, and recall, outperforming SVM, MLPNN, and LSTM. The model's transparency ensures regulatory compliance while minimising false alarms. Key findings emphasise the need for proactive detection, AI integration, and resilience against threats such as phishing, ransomware, and DDoS. The research demonstrates AI's potential for real-time cyber defence, bridging theoretical innovation with practical financial security applications.

6. Recommendations

The proposed model should be tested in real-world financial networks through collaboration with industry stakeholders. Integrating real-time data analysis and continuous monitoring would enhance threat detection and response. Adaptive learning strategies should allow the model to update based on new data, addressing evolving cyber threats. Future work includes developing autonomous, real-time models acting as intelligent firewalls, incorporating reinforcement or online learning, and expanding simulations to address stealthy attacks and larger network topologies. Assessing performance under varying loads and applying explainable AI may help improve robustness, scalability, and transparency, supporting regulatory compliance and trust in automated financial cybersecurity systems.

AI Declaration: This study was independently prepared, authored, and compiled in its entirety without the use of any automated systems or artificial intelligence technologies.

Ethics declaration: The utilisation of the virtual simulation of a financial system was driven by its non-invasive nature, ensuring the safety of existing systems, human users, and security protocols. The study adhered to publicly available data and research for analysis and reporting, safeguarding the confidentiality of financial system security. This cautious approach ensured that the current cybersecurity operations of the financial system were not compromised. Consequently, all research methods and data incorporated in this study were conducted with the utmost objective and careful consideration of the subject matter.

References

Abdulrahman, S. (2020). 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

Duque, S., & Omar, M. N. Bin. (2015). Using Data Mining Algorithms for Developing a Model for Intrusion Detection System (IDS). *Procedia Computer Science*, *61*, 46–51. https://doi.org/10.1016/j.procs.2015.09.145

Hasan, M. F., Alramadan, N. S., Al-Ramadan, N. S., & Professor, A. (2021). Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. *Social Science and Humanities Journal*, *05*. https://doi.org/10.6084/m9.figshare.15190185.v2

Keen, M., Kaushik, R., Singh Bhogal, K., Aghara, A., Simmons, S., Dulaney, R., Dube, S., & Allison, A. (2018). *Case Study: SOA Banking Business Pattern*.

Meredith, L. G., & Bjorg, S. (2003). Contracts and types. *Communications of the ACM*, *46*(10), 41–47.

Mhlanga, D. (2020). Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion. *International Journal of Financial Studies*, *8*(3), 1–14. https://doi.org/10.3390/ijfs8030045

Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences*, *13*(10), 5875. https://doi.org/10.3390/app13105875

Nuthalapati, S. babu. (2023). AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking. *Educational Administration: Theory and Practice*, 357–368. https://doi.org/10.53555/kuey.v29i1.6908

Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Uddin Prince, N., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). *AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction Nanotechnology Perceptions AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction*. https://doi.org/10.13140/RG.2.2.22975.52644

Recker, J. (2021). *Scientific Research in Information Systems*. Springer International Publishing. https://doi.org/10.1007/978-3-030-85436-2

neu Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

World Bank Group. (2022). *The Little Data Book on Financial Inclusion*. www.worldbank.org