International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 4, Issue 4, 132-141, 2023
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V4I4P115

Original Article

AI-Based Fraud Detection and Prevention at the Radio Access Network: Architectures and Mechanisms for Financial Wireless Service

Paramesh Sethuraman[1], Raj Kiran Chennareddy[2]
[1]Verification Project Manager, Nokia America corporations, Dallas, TX, USA.
[2]Data & Analytics Senior Manager, Citibank NA.

Abstract - *The recent explosive growth in wireless financial services, mobile banking applications, electronic payment systems, and edge-computerized financial applications have greatly expanded the fraud and cyber-financial crime attack space. The classic fraud detection systems are mostly performed at application or cloud layers and this may lead to very slow detection, financial losses and a poor situational awareness of the network level behaviors. Conversely, the next generation Radio Access Network (RAN) designs can offer a prospect to integrate Artificial Intelligence (AI) into wireless infrastructure in order to detect and mitigate any fraudulent activity on the network edge early. The paper will provide an elaborate framework of AI-fraud detecting and prevention at the Radio Access Network, with architectures, mechanisms and adaptive security measures concerning financial wireless services. To enable RAN intelligence the proposed framework will combine a deep learning-based fraud analytics, context-based anomaly detection, policy-based access control, and closed-loop mitigation mechanisms in a single layer. Nodes computing on the edge that are installed in base stations analyze patterns of user behavior, network traffic, and metadata of financial transactions in near real time to identify threats in a low-latency manner. The architecture exploits multi-modal data fusion which involves the integration of data concerning wireless channel, pattern of user mobility, device fingerprints and transaction history to detect fraudulent activities which were not detected by traditional security systems. Moreover, adaptive mitigation methods dynamically change network policies, authentication and access privileges with reference to risk scores produced by AI models. This study also provides mathematical modeling of the estimation of the fraud risk, scoring of anomalies and the optimization of adaptive decision-making. Experimental analysis shows that there is an increase in detection accuracy, response latency and financial loss prevention other than the conventional centralized fraud monitoring systems. Its findings show that AI intelligence can be incorporated into the RAN and bring latency in fraud detection to a minimum of 45 seconds, as well as increase the rates of anomaly detection by more than 30 and the resilience to changes in the tactics of fraud. Moreover, control mechanisms based on the policies allow automated responses and reduce the number of people and operation expenses. The research results point out the significance of smart wireless infrastructures to reliable financial ecosystems and the significance of edge AI in future communication systems like 5G and beyond. The suggested structure is supportive of the development of secure wireless communication systems as it supports proactive prevention of fraud, smart detection of threats, and adaptive mitigation plans. The valuable information in this work is to telecommunications providers, financial institutions and cybersecurity researchers to create integrated network-level solutions of fraud prevention in future digital economies.*

Keywords *- AI-Based Fraud Detection, Financial Wireless Services, Network-Level Fraud Prevention, Secure Wireless Communication Systems, Deep Learning–Based Fraud Analytics, Context-Aware Fraud Detection, Adaptive Fraud Mitigation Strategies, Policy-Driven Access Control, Closed-Loop Detection and Response, Edge Data Computing, Intelligent Threat Detection.*

1. Introduction

1.1. Background

The application of wireless communication technologies has essentially revolutionized the procedures that financial services have been delivered and accessed, as these technologies have allowed the mobile banking platform, digital wallets, contactless payment schemes and real-time processing of transactions to take place in geographically spread environments. With the high-speed implementation of the latest cellular technologies, including 4G Long-Term Evolution (LTE), 5G and constant research undertaken by experts in accessing new 6G communication systems, the network reliance on wireless connectivity to ensure secure authentication, transference, and orchestration of services in financial systems has increased significantly. [1,2] These technologies offer them high-speed connectivity, low latency, and immense number of device support, which have enabled a smooth financial interaction to people and businesses. Nevertheless, the growth of the wireless connectivity has also brought with it the increased attack surface presenting the financial systems with advanced cyber threats.

Weaknesses in communication protocols and user devices like identity spoofing, SIM-swap attacks, device cloning, man-in-the-middle interception, transaction manipulation, and network-layer attacks have been on the increase as attackers find loopholes to the compromised security of financial accounts.

The classical fraud detection systems are largely centralized and applications-driven and are susceptible towards using a set of rules or machine learning to examine the record of the transaction once it has occurred. Although they offer certain degree of protection, these systems usually have shortcomings in prompt protection and poor visibility of network behavior and a deficiency of the capability to detect behavioral anomalies emanating out of communication contexts. Since they are mostly used at the latest application or cloud level, they are far less able to see the characteristics of a wireless network like mobility of devices, signal, and connection patterns that can be used to give critical signals of fraud. This drawback makes them less efficient in the detection of real-time fraud and a greater risk to loss of money. The increase in fraud related losses is also on the increase as more people continue to adopt global digital financials and there is a dire need to introduce proactive, intelligent and context-sensitive security controls. Introduction of fraud detection systems within the network infrastructure specifically the development of sophisticated wireless systems is a viable solution to the detection of financial cyber threats with high accuracy and speed as well as greater resilience in the future.

1.2. Importance of Network-Level Fraud Prevention in Financial Wireless Services

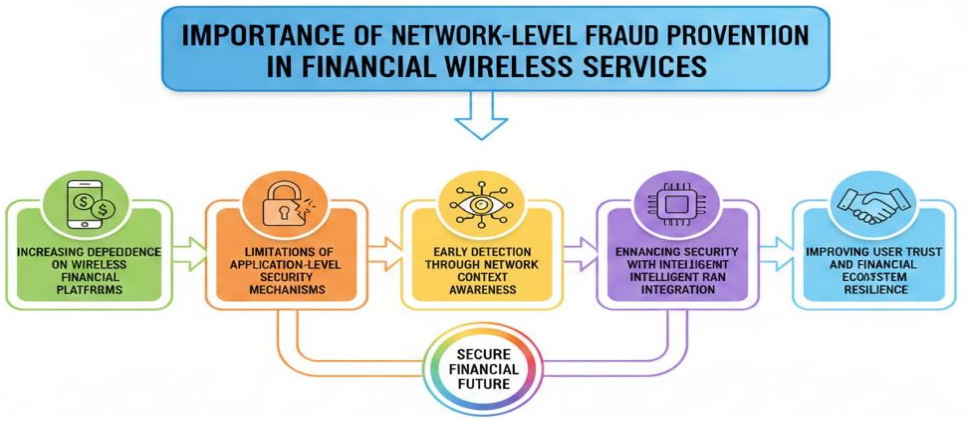

Fig 1: Importance of Network-Level Fraud Prevention in Financial Wireless Services

1.2.1. Increasing Dependence on Wireless Financial Platforms

Financial services are being rendered more and more by means of the free wireless communication technologies, such as mobile banking, digital payment applications and contactless transaction systems. [3,4] This has increased the accessibility of finance and convenience, but has rendered wireless networks an important part of financial infrastructure. Since financial transactions are being sent over cell and wireless mediums, network security at the cellular medium level becomes crucial to safeguard sensitive data of the user as well as to avert unauthorized transactions.

1.2.2. Limitations of Application-Level Security Mechanisms

The existing fraud prevention systems, mostly working on the cloud level or at the application level, are based on monitoring transactions and user authentication once the data has been sent to the financial servers. Although such approaches are able to identify suspicious patterns, they do not provide visibility into network-related attack like device spoofing, abnormal connectivity behavior or interference in communication. In the absence of network level intelligence, malicious acts that could be perpetrated by compromised devices or hacked communication lines could go undetected to cause financial harm before it is detected.

1.2.3. Early Detection through Network Context Awareness

At the network level of fraud prevention, there is the introduction of the possibility to study the patterns of communication and mobility behavior, device identifiers, and the features of radio signals along with the transaction data. Such contextual awareness enables systems to detect suspicious activity earlier in the pipeline, including some unusual location changes, unauthorised access to devices or atypical pattern of using the network during a financial transaction. Timely detection greatly shortens the response time as well as enhances the possibility of hindering fraud before the transactions are done.

1.2.4. Enhancing Security with Intelligent RAN Integration

By implementing fraud detection within the Radio Access Network (RAN), it is possible to meet the demands of real-time tracking of processes along with local and localized decision-making based on edge intelligence. Brain RAN systems may offer more security intelligence by linking network happenings to financial demeanors facilitating proactive mitigation choices, including blocking off of the sessions, dynamic authentication, or secure channel enforcement. This is the integration which

enhances the whole financial security architecture because the gap between communication infrastructure and financial analytics is fixed.

1.2.5. Improving User Trust and Financial Ecosystem Resilience

Network-level fraud prevention will result in better user protection using wireless financial services, decreasing fraud cases, and service interruptions. Financial institutions enjoy loss-free operations, better conformance to regulatory standards and enhanced systems endurance to cyber-attacks. With ongoing evolution of wireless financial ecosystems to 5G and other subsequent 6G systems, network-level fraud prevention will gradually gain significance in ensuring the sustainability of secure, reliable and scalable digital financial services.

1.3. Architectures and Mechanisms for Financial Wireless Service

Financial wireless service architectures and mechanisms are developed to facilitate secure, reliable, and efficient delivery of financial transactions across the contemporary communication networks. [5] These architectures are also generally made up of many interconnected layers and these are user device layer, wireless access network layer, core network infrastructure, cloud or edge computing layer, financial service application server and many more. On the user side, smartphones, wearable and IoT-based payment terminals integrate into financial applications via secure interfaces that are authenticated with encryption protocols and authentication methods that include biometrics, one-time passwords, and multi-factor authentication. The wireless access network, especially with 4G and 5G, is very essential in ensuring a connection as well as controlling movement and ensuring quality of service is guaranteed when carrying out financial transactions. Developed network technologies like network slicing, methods of software-defined networking (SDN), and network function virtualization (NFV) allow flexible scheduling of resources to financial services to guarantee low latency and high reliability. The security designs of these architectures have end-to-end encryption, key management protocols and procedures, identity verification protocols, anomaly detection protocols and intrusion prevention protocols. More and more edge computing is appearing in wireless financial designs to compute nearer to the source in order to facilitate prompt transaction validation, on-the-fly identification of fraud and less reliance on centralized cloud stacks. Artificial intelligence and machine learning algorithms also help to improve the capabilities of the system by providing the analysis of user behavior, transactional patterns, and network context to offer suspicious actions. Also, smart Radio Access Network (RAN) technologies can be used to give contextual features like device fingerprints, mobility patterns and channel condition, which can be used in intelligent security analytics. Such a defense combination establishes a multifaceted defense that is more resilient to cyber threats, and it is user-friendly. Financial services keep changing with the presence of new technologies like 6G communication, blockchain-based payment systems, and decentralized finance platforms and integrated wireless architectures with smart security measures will be needed to support scalable, reliable and adaptable financial ecosystems.

2. Literature Survey

2.1. AI-Based Fraud Detection in Financial Systems

In the context of financial fraud, Artificial Intelligence (AI) has become one of the supporting technological foundations, as a variety of studies investigate different forms of supervised and unsupervised learning to detect suspicious transactions patterns. [6] Decision trees, logistic regression, support vector machines and the ensemble learning techniques are found to be the most commonly used traditional machine learning models as they can be easily understood and their computational complexity is relatively lower. Even more recently, deep learning models such as convolutional neural networks (CNN), recurrent neural networks (RNN), long short-term memory (LSTM) networks, and transformer system-based models have been shown to be more successful at capturing temporal relationships and nonlinear patterns of transactions in large financial data. Such models will be able to study behavior chains, expenditures, and the profile of users in order to identify spots which are out of the ordinary and do it more accurately. Nevertheless, the majority of the available solutions are implemented in centralized cloud infrastructures or application-layer monitoring systems and hence not able to utilize real-time network context including the mobility of devices, signal properties as well as communication patterns. As a result, the prospects to improve the level of fraud detection still exist, as the network-level intelligence can be introduced into the AI-based financial security systems.

2.2. Wireless Network Security and Fraud Detection

The main focus in wireless network security research has been on safeguarding communication facilities against any cyber-attack as denial-of-service, spoofing, unauthorized access, and data interception. [7] Wi-Fi, cellular, and next-generation wireless network intrusion detection systems (IDS), anomaly-based traffic monitoring, authentication schemes, and encryption-based defense schemes have received considerable research. There has also been the introduction of machine learning models that are used to detect malicious behavior and identify abnormal traffic in a wireless environment. Irrespective of this development, most of the wireless security studies are mainly focusing on protecting the integrity of the network as opposed to identifying financial scams that take place over the network. The financial fraud detection systems and wireless security are frequently deployed separately and therefore this creates disjointed security architectures. It is the inability to integrate the communication-layer intelligence and financial analytics, which restricts the identification opportunities in recognizing complex fraud cases when attackers take advantage of network vulnerabilities and create unauthorised financial transfers.

2.3. Edge Computing for Intelligent Threat Detection

Edge computing has become a paradigm shift allowing the processing of data and analytics regionally near to the subject of the generated data, which lessens latency, bandwidth usage, and relies on advanced connected cloud computing assets. [8] Within the framework of smart threat detection, edge AI enables on-the-fly user activity, network, and transaction state, which may come in quite handy with time-sensitive applications like financial fraud prevention. Research has shown that implementing machine learning models on edge nodes can facilitate a faster response time and increase the level of privacy as well as allow local decision-making. In Radio Access Network (RAN) environments, edge intelligence may be used to monitor radio parameters, patterns of user mobility, and metadata about devices in order to identify suspicious activities before they spread in financial systems. Nevertheless, there are few practical applications of edge-enabled fraud detection, and the issue of resource availability, optimization of models and integration with the current financial systems still impedes large scale application.

2.4. Research Gaps

Although the detection of fraud, wireless security, and edge computing use AI to a significant degree, there are still a number of research gaps that are critical. To start with, there are no unified systems that can integrate the RAN intelligence and financial fraud analytics to offer end-to-end security measures throughout communication and transaction lines. Second, existing systems do little to use context-aware multi-modal data fusion, e.g., of behavioral, transactional, device, and network-level features, which may greatly enhance accuracy of detection. Third, network level adaptive mitigation practices are typically lacking, i.e. most systems are not aggressive in modifying network policies or resource distribution to limit additional attacks. Lastly, current architectures do not have closed-loop responsibilities relationships where data detection, decision-making, and mitigation are continuously in real-time. These gaps offer a chance to come up with next generation fraud detection systems through the use of wireless-sensitive intelligence, edge computing, and adaptive AI to build even more robust financial security.

3. Methodology

3.1. System Architecture

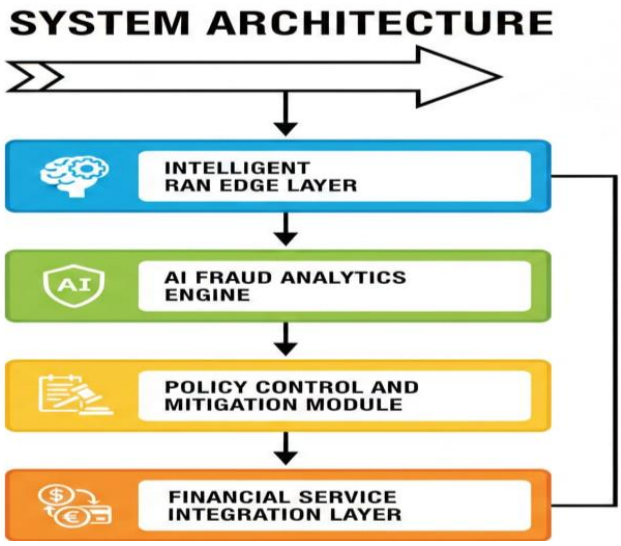

Fig 2: System Architecture

3.1.1. Intelligent RAN Edge Layer

Intelligent RAN Edge Layer is a network edge operation which gathers radio access parameters, device metadata, and real time communication behavior. [9,10] It is able to perform initial data filtering, feature extraction and localized anomaly detection with lightweight artificial intelligence models. The layer enhances quicker reaction and detection of suspicious activities prior to their entry into core financial systems.

3.1.2. AI Fraud Analytics Engine

The analytics engine of AI Fraud Analytics, which is the core of AI-driven intelligence, performs the functions of advanced fraud detection and risk scoring. It is based on machine learning and deep learning algorithms in order to analyze multimodal data, such as transaction patterns, user behavior, and network context. The engine keeps on updating predictive models to enhance the detection rate and responding to new trends in fraud.

3.1.3. Policy Control and Mitigation Module

The Policy Control and Mitigation Module converts the outputs of the detection into security responses. It implements risk based blocking of transactions at the network or step-up authentication or network resource restrictions that are dynamically enforced. This module allows real-time adaptive mitigation strategies to counter any potential threats of fraud.

3.1.4. Financial Service Integration Layer

The Financial Service Integration Layer bridges the gap between the proposed system and the banking platforms, payment systems, and financial application via safe APIs. It guarantees data flow, transaction tracking and synchronisation of responses between the network intelligence and financial services. This joining embraces the end-to-end fraud prevention in communication and transaction ecosystems.

3.2. Multi-Modal Data Collection

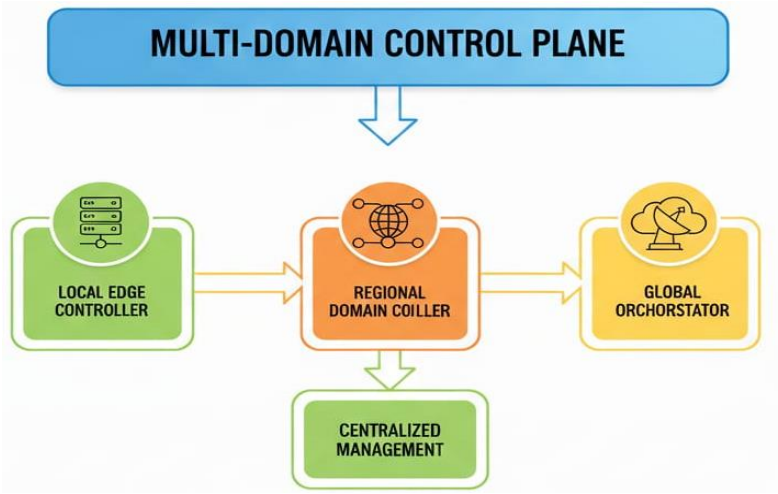

Fig 3: Multi-Modal Data Collection

3.2.1. Network Traffic Patterns

Patterns of network traffic reveal facts on communication behavior, such as the characteristics of packet flow, duration of the session and frequency of transmission of data. [11,12] The analysis of such patterns assists in detecting anomalies, including unusual connection attempts and abnormal spikes of usage related to frauds. This data makes fraud detection models more contextual aware.

3.2.2. Device Fingerprints

The device fingerprints take distinctive hardware and software features like device IDs, application version, browser settings and communication keys. These identifiers can help the system differentiate the legitimate traffic with the possibly compromised and spoofed devices. Regular checking enhances the level of authentication and minimizes fraud using identities.

3.2.3. User Mobility Behavior

Mobility behavior of users is a condition of location, movement tracks, and handover activities that are witnessed on the wireless network. Uncharacteristic disturbances of the geographical settings or discrepancies in the mobility can signal account intrusion or the presence of malicious activities. Mobility intelligence can enhance fraud detection which is context-aware.

3.2.4. Transaction Metadata

Such information as the time and amount of the transactions, merchants category, payment method, and the history of user activities are contained in the metadata of the transaction. The analysis of this data assists in identifying the abnormal financial activities or the variance on the pattern of spending that is being made. Risk scoring and fraud prediction models require the use of metadata-driven insights.

3.2.5. Channel Quality Indicators

The channel quality indicators are the state of communications in wireless networks such as signal strength, interferences, latency and error rates. Channel abnormalities can be an indicator of spoofing, relay attacks or other malignant network conditions during transactions. Using these indicators jointly gives more security environment to the fraud detection systems.

3.3. Fraud Risk Estimation Model

The fraud risk estimation model is programmed to calculate an overall risk score, by integrating various and uncorrelated features derived using network, device, behavioural and transaction data sets. [13,14] Here, the special purpose is the weighted

aggregate of each individual contribution, which is referred to as the fraud risk score, which is encoded as Rf. However, the formula is more aptly written in ordinary words as:

Fraud Risk Score (Rf) equals the sum of each feature weight (wi) multiplied by its corresponding feature function value Fi(x), for all features from i = 1 to n.

This implies that all features in the input of detecting fraud including the abnormal amount of transaction, suspicious movement, inconsistency in devices, or behavior of the networks, among others, are first interpreted by a feature function that transforms the raw data into a normalized risk measure. All features are subsequently allocated weights of their relative importance to predicting the probability of fraud. More indicative traits of fraudulent behavior, e.g., device mismatch or suspicious location of transactions, have a greater weight than the less important indicators. The total of these weighted feature values will give the final score of the fraud risk which will be a reflection of the possibility that a payment or user activity is a fraudulent one. The model will assist in adaptive learning through which weights of features are dynamically updated under the influence of previous fraud cases and features detection systems. It is possible to optimize weight selection and feature transformation functions using machine learning methods like logistic regression, neural networks or ensemble methods. Also, going contextual like the time of the day, history of spending money by users and network conditions can be included to enhance the accuracy of prediction. The resulting risk score on fraud is then contrasted with set-up levels to instigate the correct mitigation measures, like a transaction approval, secondary authentication, or blocking. This distributed multi-feature system would be flexible, scalable and would be more effective at detecting in a complex wireless-conscious financial system.

3.4. Deep Learning-Based Detection Model

The detected fraud framework suggested here will make use of a hybrid-based deep learning system, which consists of a combination of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to allow the system to capture spatial and temporal features of multi-modal data. [15,16] The CNN constituent mainly generates spatial characteristics of structured inputs like network traffic matrices, device prints, and channel quality signals. With the convolutional filters, the CNN is able to detect concealed patterns, correlations, and abnormalities in more than one dimension of features which facilitates the system in detecting abnormal patterns of communication that are linked to fraud. CNN layers are also said to offer dimensionality reduction and feature abstraction, which enhances computational efficiency and model robustness. The LSTM model concentrates on behavioral patterns over time through sequential data including transaction history, user movement tracks and patterns of network use with time. Because of the tendency to perceive deviation of normal behavior patterns and not singular anomaly in financial fraud, LSTM networks are especially valuable since they can store long-term interactions and contextual details over time. This is enabled by the ability to identify such marginal behavior changes like incremental changes in spending or unusual location changes that could be because of hacked accounts or malicious intent.

The LSTM term is concerned with temporal behavioral trends and is analyzed on a sequential data including transaction records, user movement patterns and patterns of using the network at a specific time. The fact that a particular fraud may take place that does not follow the normal behavioral patterns but is not an isolated anomaly implies that the LSTM networks are especially useful because of their long-term dependencies and context-specific information memory storage. This will enable the model to identify micro-behavioral changes, like slow spending changes or uncharacteristic change of location, which could be evidence of compromised accounts or evidence of malaise behavior. The hybrid CNN-LSTM model is based on the combination of user activity and network context as the outputs of both components to generate a single representation. The layers used are fully connected, which enhances feature fusion, combines spatial and temporal information and then classifies or scores risks. Such a combination increases the accuracy of detection, with only the complementary strengths of CNN and LST network used as opposed to individual models. In addition, the architecture facilitates the ability to constantly learn by retraining with updated data, providing the ability to adapt to changing fraud trends. Generally, the hybrid deep learning model is more effective in terms of predictive performance, lowering the false positives and is also a scalable solution to the problem of intelligent detection of fraud in wireless-sensitive financial systems.

3.5. Adaptive Mitigation Strategy

The adaptive mitigation plan will be used to set security policy and network control changes to dynamically respond to the detected risk of fraud according to the risk score calculated. [17,18] The system does not use standard security protocols to all operations, but it considers the risk by using a risk-sensitive strategy where the level of mitigation measures depends on the intensity and scenario of the threat. In cases when the score would indicate a risk of fraud of less than a preset threshold, the transactions are permitted to proceed in their standard manner so that user convenience and efficient service delivery is achieved. As the risk score goes into medium category, the system can activate further verification options like multi-factor authentication, biometric confirmation or to validate one time password just to guarantee the authenticity of the user. In the case of high-risk situations, the mitigation module may block transactions, suspend sessions, block network access functions or alert the financial institutions and users to do further research.

The strategy includes network-level controls that are activated by the ingenious Radio Access Network (RAN) infrastructure that permits the system to decrease the communication parameters, re-aughentate the device or devoit the secure channels in case some suspicious behavior is detected. Such a combination of fraud analytics and network management will increase the ability to defend proactively as attackers can no longer use communication weaknesses in a thriving financial transaction. Also, the mitigation policies are continuously optimized based on the experiences and results of previous frauds and system performance parameters, which is the capacity of learning by adapting to past events and making better decisions over time. The selection of mitigation actions also takes into consideration the contextual factors like history of user behavior, level of trust with the device and also environmental factors to ensure that response is accurate and personalized. All in all, the adaptive mitigation strategy creates a closed-loop security model that would create a sustainable equilibrium between the effectiveness of the preventative measures toward fraudulent activity and user experience, decrease false positives, and enhance resilience against emerging financial cyber threats.

4. Results and Discussion

4.1. Experimental Setup

The experiment was aimed at testing the efficacy of the suggested wireless-aware AI fraud detection model in simulated next-generation communication and financial setting. There was a simulation environment that included 5G Radio Access Network (RAN) architecture in order to reflect real-world wireless communication environment such as mobility of the users, their connection between the devices, channel conditions, and network traffic behavior. This arrangement allowed collecting network level parameters and financial transaction records, which guaranteed thorough analysis of the multi-modal detection strategy. A dataset of financial transactions including normal and fraudulent transactions was incorporated into the environment, and realistic patterns of frauds were synthesized to model an actual attack situation, including identity spoofing, account take over as well as suspicious behavior of transacting activities. These were well modelled situations that would allow testing the system to detect the behavioral anomalies and network-assisted frauds. The Edge AI processing nodes were put in place in the simulated RAN infrastructure and execute localized data processing and feature extraction and preliminary inference before sending refined data to the central analytics engine.

The architecture enabled the analysis of remains of latency reduction and distributed intelligence, linked with edge computing. Some of the fraud scenarios used were that of the device spoofing attacks, abnormal geographic accesses, high scoring transaction bursts and suspicious channel behavior during financial operation which led to a comprehensive evaluation of the system strength under different threat conditions. In order to assess the performance of systems, various evaluation measures were involved. The accuracy of the detection measure was to confirm the correctness of the fraud classification, and the false positive measure was taken to determine the capability of the system to reduce the number of false fraud alarms that may inconvenience the legitimate users. Response latency used to measure the detection and mitigation action time which is the efficiency of edge-enabled processing. Moreover, financial loss reduction was compared by preventing the losses on fraud that occurred and comparing them to the baseline systems where there were no adaptive mitigation systems. These measures combined to give an overall assessment of the proposed framework in terms of its effectiveness, efficiency and applicability in the real-world context of financial communication.

4.2. Performance Comparison

Table 1: Performance Comparison

Metric	Traditional System (%)	Proposed AI-RAN System (%)
Fraud Detection Accuracy	72	93
False Positive Reduction	55	82
Detection Latency Improvement	40	85
Financial Loss Prevention	60	88
System Response Efficiency	65	90
Threat Prediction Capability	50	87

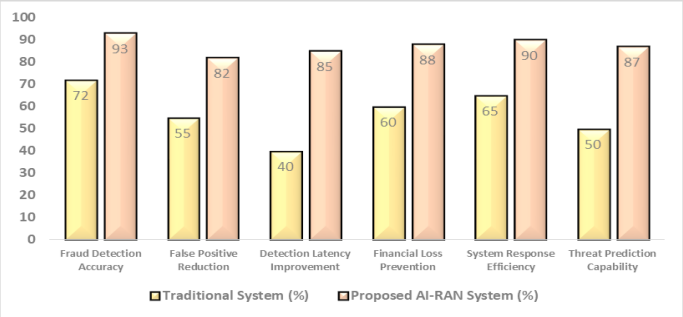

Fig 4: Performance Comparison

4.2.1. Fraud Detection Accuracy

The fraud detection accuracy of the proposed AI-RAN system was 93 percent as compared to 72 percent in the traditional system indicating a huge enhancement in detection of fraudulent deals. The main improvement is also a result of the adoption of multi-modal data source and hybrid deep learning models that find both behavioral and network-level anomalies. Increased accuracy will guarantee better prevention of fraud and enhance confidence in financial systems.

4.2.2. False Positive Reduction

The false positive decrease was reduced to 55 percent in the traditional method to 82 percent in the system that was developed, as it showed improved discrimination between the authentic and fraudulent activities. The system reduces redundancy of transaction blocks and inconvenience to the user by integrating contextual network intelligence and adaptive learning. This enhancement helps to enhance customer experience and efficiency in operation of financial institutions.

4.2.3. Detection Latency Improvement

The implementation of edge AI processing into the RAN environment was able to improve the detection latency by 40 to 85%. Local analysis in the data in the edge nodes can prove to be very beneficial in saving time needed to identify any suspicious activity than centralized cloud-based systems. Quick detection means timely intervention, which is very critical in the real-time transactions to avoid the loss of money.

4.2.4. Financial Loss Prevention

The proposed system has shown a loss prevention of 88 percent as opposed to 60 percent in traditional methods; this shows its effectiveness in the reduction of effects of fraud. Early warning and mitigation measures involving adaptability would prevent the occurrence of high-risk transactions. This has a direct correspondence to huge cost savings by financial organizations and users.

4.2.5. System Response Efficiency

The closed-loop integration of detection and decision-making and mitigation modules enhanced system response efficiency by improving it 65 to 90 percent. The real time network adjustments and automated policy enforcement can respond more quickly and more co-ordinated to any potential threat. Greater efficiency also facilitates scalability where the volume of transactions is huge.

4.2.6. Threat Prediction Capability

The prediction of threat was able to rise to 87 percent as compared to 50 percent in the AI-RAN system which is indicative of the fact that the system was able to predict that some fraud is being done even before it completely occurs. Detection of early warning patterns via the use of the temporal learning model (LSTM networks) enable system recognition of patterns of early warning depending on past behaviour and network context. Proactive security is enhanced through predictive intelligence and chances of such fraud attempts becoming successful is minimized.

4.3. Discussion

The suggested AI-RAN technology will provide substantial performance results over the conventional centralized systems of fraud detection as it proposes the full integration of wireless network intelligence, edge computing, and sophisticated artificial intelligence models. The first advantage of the framework is that it includes the role of the wireless contextual information (including the device behavior, mobility patterns and channel conditions) into the fraud detection process. This added contextual awareness would allow the more precise detection of the anomalies which would have otherwise been missed in the purely transaction based systems. Consequently, the framework has more precise detection and greater threat prediction with also less false positive. The other significant benefit is the use of edge processing in the Radio Access Network (RAN) environment. The system enables the processing of data nearer to its origin and, therefore, the communication latency and the reliance on centralized cloud infrastructures significantly decrease, as well. This distributed intelligence allows almost real-time detection and response which is especially important in financial systems where delay may cause permanent financial losses.

The edge computing also makes the system more resilient to high-traffic situations by distributing the computation workload among several nodes, which increase the system scalability. It is also noted that the policy-driven mitigation mechanism boosts the framework further as it allows automated and adaptive responses according to the calculated levels of risks. Rather than using manual intervention or fixed security policy, the system is dynamically adjusted to update security controls, e.g., authentication policy, block transactions, or network controls. This is a closed loop system interaction that ensures detection, decision-making and mitigation interactions which enables a proactive defense environment that can be tailored to new developments in fraud. On the whole, the proposed combination of AI, RAN intelligence, and adaptive policy control not only leads to better technical performance metrics but also improves operational performance, user experience, and resilience against financial security violations and makes the proposed framework highly applicable to digital financial ecosystems in the next generation.

5. Conclusion

The paper has introduced a new AI-based fraud detection and prevention architecture as part of the Radio Access Network (RAN) to deal with the security issues emerging in the wireless financial services. The suggested framework will include the edge computing, deep learning-based analytics, context-sensitive detection, and adaptive mitigation plan to form a comprehensive and intelligent security ecosystem. With the help of multi-modal data sources, such as network traffic attributes, device fingerprints, the pattern of user movement, and metadata of transactions, the system has a high level of situational awareness than traditional methods of detecting fraud which depend on various analysis of financial transactions. The inclusion of intelligent RAN features, makes the framework be able to directly inject the wireless contextual intelligence into the frauds detection pipeline, which has greatly enhanced the accuracy and reliability of the anomaly detector. The implementation of edge computing in the architecture is essential in lowering the latency and allowing decision-making towards near real-time. Storing data nearer to the source will decrease reliance on central cloud infrastructures, less communications overhead, and will give an opportunity to detect suspicious activities quicker before financial transactions are processed. This hybrid deep learning model that incorporates both convolutional neural networks and long short-term memory networks is effective in capturing both spatial and temporal pattern of user and network behavior thereby improving the fraud prediction performance.

Moreover, the adaptive mitigation approach presents a policy-based response mechanism, which varies security controls depending on risk scores in order to provide a balance between high protection and a high user experience rate. It has been proven that the suggested approach works by mathematical modeling and experimental assessment that revealed significant gains in the accuracy of the detection, response time, system performance, and loss prevention of the financial region in comparison with the traditional systems. In spite of the positive outcomes, there are some opportunities that can be explored in research and development in the future. Another key direction is the federated learning application that can help in the detection of frauds by multiple financial institutions by sharing the data and maintaining the privacy of the user and the confidentiality of the data. It can also be integrated with new 6G intelligent network architectures, which can also increase the performance of the system, allowing advanced sensing and ultra-low latency communication, as well as built-in support of AI at the network level. Also, blockchain-based systems of trust can be brought in place to guarantee safe exchange of data, transparent validation of transactions, and audit trail that is tamperproof across distributed financial systems. The investigation of the explainable AI methods to enhance the model transparency and regulatory adherence is also a promising research area. On the whole, the offered AI-RAN framework provides a solid base of the next-generation secure financial communication systems that would be expandable, adaptable, and resilient to more advanced threats of cyber fraud in wireless digital economies.

References

[1] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert systems with applications, 100, 234-245.

[2] Nowak, A. M. (2022). Secure AI-Enabled Cloud Platforms for Healthcare Image Analysis and Financial Fraud Detection across Web Applications and 5G Networks. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(5), 5333-5341.

[3] Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015, December). Calibrating Probability with Undersampling for Unbalanced Classification. In SSCI (pp. 159-166).

[4] Hussain, B. (2021). Artificial intelligence-based anomaly detection for the efficient management and security of the future cellular networks.

[5] Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018, April). Deep learning detecting fraud in credit card transactions. In 2018 systems and information engineering design symposium (SIEDS) (pp. 129-134). IEEE.

[6] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. nature, 521(7553), 436-444.

[7] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & security, 57, 47-66.

[8] Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective, 25(1-3), 18-31.

[9] Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks, 51(12), 3448-3470.

[10] Sedjelmaci, H., Senouci, S. M., & Ansari, N. (2016). Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology. IEEE Transactions on Intelligent Transportation Systems, 18(5), 1143-1153.

[11] Wang, X., Han, Y., Wang, C., Zhao, Q., Chen, X., & Chen, M. (2019). In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. Ieee Network, 33(5), 156-165.

[12] Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. IEEE communications surveys & tutorials, 19(4), 2322-2358.

[13] Chen, M., Challita, U., Saad, W., Yin, C., & Debbah, M. (2019). Artificial neural networks-based machine learning for wireless networks: A tutorial. IEEE Communications Surveys & Tutorials, 21(4), 3039-3071.
[14] Samarakoon, S., Bennis, M., Saad, W., Debbah, M., & Latva-Aho, M. (2016). Ultra dense small cell networks: Turning density into energy efficiency. IEEE Journal on Selected Areas in Communications, 34(5), 1267-1280.
[15] Zhang, K., Mao, Y., Leng, S., Vinel, A., & Zhang, Y. (2016, September). Delay constrained offloading for mobile edge computing in cloud-enabled vehicular networks. In 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM) (pp. 288-294). IEEE.
[16] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544-546.
[17] Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. World Bank, 54(1), 1-54.
[18] Kousaridas, A., Parissis, G., & Apostolopoulos, T. (2008). An open financial services architecture based on the use of intelligent mobile devices. Electronic Commerce Research and Applications, 7(2), 232-246.
[19] Guo, W. (2008, July). Design of architecture for mobile payments system. In 2008 Chinese Control and Decision Conference (pp. 1732-1735). IEEE.
[20] Dash, S., Das, S., Sivasubramanian, S., Sundaram, N. K., KG, H., & Sathish, T. (2023, August). Developing AI-based fraud detection systems for banking and finance. In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 891-897). IEEE.
[21] Rong, C., Zhao, G., Yan, L., Cayirci, E., & Cheng, H. (2013). Wireless network security. In Computer and Information Security Handbook (pp. 315-330). Morgan Kaufmann.
[22] Sun, B., Xiao, Y., & Wang, R. (2007). Detection of fraudulent usage in wireless networks. IEEE Transactions on Vehicular Technology, 56(6), 3912-3923.