Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 3, Issue 12, 2025

AN INTELLIGENT IOT-ENABLED DEEP LEARNING ARCHITECTURE FOR REAL-TIME FAULT DIAGNOSIS AND CYBER-ATTACK MITIGATION IN MODERN BANKING INFRASTRUCTURE

Noor-E-Haram[*1], Asif Rahim[2], Muhammad Zeeshan[3], Lubna Gul[4], Tariq Ahmad[5], Muhammad Humayun Khan[6], Abdul Waheed[7]

[1]*Department of Software Engineering, Bahria University, Islamabad, Pakistan.*
[*2]*Department of Computer Science, Abdul Wali Khan University, Mardan, Pakistan.*
[3]*Masters in Cybersecurity, Department of Computer Science, Comsats University, Islamabad Wah Campus, Pakistan.*
[4]*Department of Computer Software Engineering, University of Engineering and Technology, Mardan, Pakistan.*
[5]*School of Artificial Intelligence and Robotics, Hunan University, Changsha, 410082, China.*
[6]*Department of Computer Software Engineering, University of Engineering and Technology, Mardan, Pakistan.*
[7]*Department of Computer Science, New York University, New York, United State of America.*

[*1]nooreharam87@gmail.com, [2]asif_rahim20@yahoo.com, [3]iamzeeshan.contact@gmail.com, [4]lubna.gul@uetmardan.edu.pk, [5]tariqafkan@cmail.com, [6]humayun.devv@gmail.com, [7]aw4782@nyu.edu.

DOI: https://doi.org/10.5281/zenodo.18465376

Keywords
Internet of Things; Deep Neural Networks; Cyber-Attack Detection; Real-Time Fault Diagnosis; Intelligent Systems; Cyber-Resilient Infrastructure; Anomaly Detection.

Article History
Received: 28 October 2025
Accepted: 12 December 2025
Published: 26 December 2025

Corresponding Author: *
Noor-E-Haram

Abstract

The rapid digital transformation of the banking sector has led to the widespread adoption of Internet of Things (IoT) technologies to enable real-time monitoring, automation, and intelligent decision-making across modern banking infrastructure. While IoT integration enhances operational efficiency and service availability, it simultaneously introduces new vulnerabilities in the form of system faults and sophisticated cyber-attacks. These challenges pose significant risks to the reliability, security, and resilience of banking operations, particularly in environments that demand continuous availability and strict data integrity. Conventional rule-based fault detection and security mechanisms are often inadequate for handling the scale, heterogeneity, and dynamic behavior of IoT-enabled banking systems, necessitating more intelligent and adaptive solutions. This paper proposes an intelligent IoT-enabled deep learning architecture for real-time fault diagnosis and cyber-attack mitigation in modern banking infrastructure. The proposed framework integrates distributed IoT sensing devices with advanced deep learning models to continuously monitor system behavior, transaction flows, network traffic, and operational parameters. By learning complex temporal and spatial patterns from high-dimensional data streams, the deep learning module enables early identification of abnormal system states caused by hardware faults, software malfunctions, or malicious cyber intrusions. Unlike traditional threshold-based approaches, the proposed architecture is capable of autonomously distinguishing between benign operational anomalies and adversarial cyber-attacks, thereby reducing false alarms and improving detection accuracy. The framework adopts a multi-layer design that combines data acquisition, feature learning, anomaly detection, and response

orchestration. Real-time inference allows the system to trigger adaptive mitigation strategies, such as fault isolation, system reconfiguration, or security enforcement actions, ensuring minimal disruption to banking services. The proposed solution emphasizes scalability, robustness, and cyber resilience, making it suitable for deployment in large-scale, heterogeneous banking environments. Extensive experimental evaluation is conducted using representative fault scenarios and cyber-attack models to validate the effectiveness of the architecture. Performance metrics, including detection accuracy, response latency, and system reliability, demonstrate that the proposed approach significantly outperforms conventional machine learning and rule-based methods. Overall, this research contributes a unified and intelligent framework that bridges the gap between operational fault diagnosis and cybersecurity in IoT-enabled banking systems. By leveraging deep learning for real-time monitoring and mitigation, the proposed architecture offers a promising pathway toward secure, resilient, and autonomous banking infrastructure capable of withstanding both operational failures and evolving cyber threats.

1- Introduction:

The global banking sector is experiencing an unprecedented digital transformation fueled by rapid advancements in Internet of Things (IoT) technologies, cloud computing, artificial intelligence, and data-driven automation. Contemporary banking infrastructure has evolved into a highly interconnected and distributed cyber-physical ecosystem consisting of automated teller machines (ATMs), branch networking equipment, point-of-sale (PoS) terminals, surveillance systems, environmental and power sensors, edge computing nodes, and cloud-hosted core banking platforms. The integration of IoT devices within this ecosystem enables real-time monitoring of operational conditions, predictive maintenance of physical assets, automated fault reporting, and enhanced situational awareness across geographically distributed banking operations. These capabilities are essential for ensuring service availability, operational efficiency, and regulatory compliance in an industry that demands continuous uptime and strict data integrity [1]. Despite these advantages, IoT-enabled banking infrastructure introduces significant operational and security challenges. The large-scale deployment of heterogeneous IoT devices increases system complexity, expands the attack surface, and amplifies vulnerability to both operational faults and cyber-attacks. Hardware degradation, power instability, sensor failures, communication link disruptions, and software misconfigurations can lead to partial or complete service outages if not detected and mitigated promptly [2]. Simultaneously, banking systems are frequent targets of sophisticated cyber threats, including distributed denial-of-service (DDoS) attacks, malware propagation, ransomware campaigns, insider threats, credential abuse, and data exfiltration attacks. The convergence of operational technology and information technology further complicates system management, as faults and attacks often manifest similar observable symptoms at the network and application layers. A critical challenge in modern banking environments is the difficulty of accurately distinguishing between benign operational anomalies and malicious cyber intrusions in real time. Both phenomena may produce abnormal traffic patterns, transaction delays, packet loss, service degradation, or unexpected system behaviors. Traditional monitoring and protection mechanisms such as static threshold-based alarms, signature-based intrusion detection systems, and isolated fault management tools are limited in their ability to capture complex temporal dependencies, nonlinear correlations, and evolving threat patterns inherent in IoT-enabled infrastructures [3]. These approaches are often reactive rather than proactive, generating excessive false alarms or failing to detect novel attack strategies, thereby undermining both operational reliability and cybersecurity posture. To

illustrate the multifaceted nature of faults and cyber threats in IoT-enabled banking systems, Table 1 summarizes common fault types, cyber-attack categories, affected system components, and potential operational impacts.

Table 1: Representative Faults and Cyber-Attacks in IoT-Enabled Banking Infrastructure

Category	Event Type	Affected Components	Observable Symptoms	Potential Impact
Operational Fault	Hardware degradation	ATMs, edge devices, servers	Increased latency, intermittent failures	Service outages, customer dissatisfaction
Operational Fault	Power instability	UPS, power sensors, data centers	Voltage drops, device resets	Data loss, system downtime
Operational Fault	Communication failure	Routers, switches, IoT gateways	Packet loss, link flaps	Transaction delays, connectivity loss
Cyber-Attack	DDoS attack	Banking APIs, network gateways	Traffic spikes, service unavailability	Denial of customer services
Cyber-Attack	Malware / ransomware	Endpoints, servers, ATMs	Abnormal processes, encrypted files	Financial loss, data compromise
Cyber-Attack	Insider threat	Core systems, databases	Unauthorized access, data anomalies	Regulatory violations, fraud
Hybrid Event	Fault-induced attack vector	Compromised IoT devices	Sensor anomalies, lateral traffic	Escalated cyber intrusion

The overlap between operational faults and cyber-attacks, as shown in Table 1, underscores the inadequacy of siloed monitoring strategies that treat reliability and security as independent concerns. In practice, faults may be exploited as entry points for cyber intrusions, while cyber-attacks may deliberately induce fault-like behaviors to evade detection. Consequently, banking institutions require unified, intelligent frameworks capable of jointly analyzing operational and security-related data to provide holistic system awareness. Recent advances in deep learning have demonstrated significant promise for addressing these challenges by enabling automated feature extraction, anomaly detection, and pattern recognition in complex cyber-physical systems. Deep neural networks can learn rich representations from high-dimensional, heterogeneous data streams, capturing subtle temporal and spatial correlations that are difficult to model using conventional statistical or rule-based techniques [4]. In the context of banking infrastructure, deep learning facilitates the fusion of IoT sensor data, network traffic metrics, system logs, and transaction records within a single analytical framework. This capability is particularly valuable for early detection of abnormal system states and accurate discrimination between faults and cyber-attacks. However, existing studies largely focus on fault diagnosis or cybersecurity in isolation, with limited consideration of their joint modeling and coordinated mitigation in IoT-enabled banking environments. Moreover, many proposed solutions emphasize detection accuracy while neglecting practical deployment constraints such as real-time inference, scalability across distributed infrastructures, adaptability to evolving threats, and explainability for system operators. These limitations restrict the operational applicability of intelligent monitoring solutions in real-world banking systems, where rapid response, regulatory transparency, and service continuity are

critical. To address these gaps, this paper proposes an intelligent IoT-enabled deep learning architecture for real-time fault diagnosis and cyber-attack mitigation in modern banking infrastructure [5]. The proposed framework integrates distributed IoT sensing devices with a multi-layer deep learning model that jointly analyzes operational and security telemetry to autonomously distinguish between benign anomalies and malicious intrusions. The architecture supports real-time inference and adaptive response orchestration, enabling rapid mitigation actions such as fault isolation, dynamic reconfiguration, traffic filtering, and security enforcement. By unifying operational reliability and cybersecurity within a single intelligent framework, the proposed solution enhances system resilience, reduces false alarms, and improves overall service availability.

2- IoT Adoption and Monitoring in Banking Infrastructure:

The rapid evolution of digital banking has accelerated the adoption of Internet of Things (IoT) technologies as a foundational enabler for real-time monitoring, automation, and intelligent management of modern banking infrastructure. Contemporary banking systems operate as large-scale cyber-physical environments composed of geographically distributed assets, including automated teller machines (ATMs), branch-level networking equipment, point-of-sale (PoS) terminals, surveillance and access control systems, power and environmental sensors, edge computing nodes, and cloud-based core banking platforms. IoT devices embedded within these components continuously generate operational, environmental, and security-related data, enabling banks to maintain situational awareness and proactively manage system performance. IoT-based monitoring plays a critical role in improving asset utilization and service reliability by enabling predictive maintenance, early fault detection, and automated diagnostics [6]. For instance, sensors deployed in ATMs can monitor cash dispenser health, temperature, vibration, and power quality, allowing potential failures to be detected before service disruption occurs. Similarly, environmental and power sensors in data centers and branch facilities provide real-time insights into cooling efficiency, energy consumption, and equipment stability. Networked surveillance and access control systems further enhance physical security by integrating sensor-driven alerts with centralized monitoring platforms. Collectively, these capabilities contribute to reduced operational costs, improved customer experience, and increased compliance with regulatory requirements related to service availability and risk management. Despite these benefits, the large-scale deployment of IoT technologies introduces significant technical and operational challenges in banking environments [7]. Banking IoT ecosystems are inherently heterogeneous, comprising devices from multiple vendors with diverse communication protocols, data formats, sampling rates, and reliability characteristics. Integrating such heterogeneous data streams into a unified monitoring framework requires sophisticated data fusion, synchronization, and preprocessing mechanisms. Moreover, the volume and velocity of IoT-generated data can be substantial, particularly in large banking networks with thousands of ATMs and branch locations, placing significant demands on storage, computation, and communication resources. Security and privacy concerns further complicate IoT adoption in banking infrastructure. IoT devices often operate with limited computational resources and may lack robust built-in security mechanisms, making them attractive targets for cyber adversaries [8]. Compromised IoT devices can be exploited to launch denial-of-service attacks, facilitate lateral movement within banking networks, or inject misleading data into monitoring systems. From a regulatory perspective, banking institutions must ensure that IoT-enabled monitoring solutions comply with strict data protection, auditability, and operational resilience requirements, which traditional IoT platforms are not always designed to meet. Existing IoT monitoring solutions in banking environments primarily rely on static thresholds, rule-based alarms, or vendor-specific management tools to identify abnormal behavior. While such approaches offer basic visibility into system performance, they are often insufficient in complex and dynamic operating conditions. Normal system behavior may vary significantly across locations,

time periods, and workload conditions, rendering fixed thresholds ineffective and leading to high false alarm rates or missed detections. Furthermore, IoT data streams are typically high-dimensional, time-dependent, and noisy, making manual rule definition and tuning impractical and error-prone at scale. These limitations highlight the need for intelligent, data-driven monitoring frameworks that can automatically learn normal operational patterns and adapt to evolving system behavior [9]. Advanced analytical approaches particularly those based on machine learning and deep learning offer the capability to model nonlinear relationships, temporal dependencies, and cross-domain correlations within heterogeneous IoT data streams. In IoT-enabled banking infrastructure, such techniques enable robust and adaptive monitoring by continuously updating learned models as system conditions change, thereby improving anomaly detection accuracy and reducing operational overhead. To provide a structured overview of IoT deployment and monitoring requirements in banking systems, Table 2 summarizes key IoT components, monitored parameters, and associated monitoring objectives.

Table 2: IoT Components and Monitoring Objectives in Banking Infrastructure

IoT Component	Deployment Location	Monitored Parameters	Monitoring Objective
ATM sensors	ATM kiosks	Temperature, vibration, power quality, device status	Predictive maintenance, fault prevention
Environmental sensors	Branches, data centers	Temperature, humidity, smoke	Equipment protection, service continuity
Power and UPS sensors	Branches, data centers	Voltage, current, battery health	Power stability, outage prevention
Network monitoring devices	Branch routers, gateways	Latency, packet loss, bandwidth usage	Network reliability, performance assurance
Surveillance and access control	Branch premises	Motion, access events, video feeds	Physical security and intrusion detection
Edge computing nodes	Branch and regional hubs	Processing load, latency, fault indicators	Real-time analytics and local response

To further illustrate the role of IoT-enabled monitoring in banking environments, Figure 1 conceptually depicts a layered IoT monitoring architecture in which distributed banking assets generate heterogeneous data streams that are aggregated, analyzed, and visualized through centralized intelligence platforms.

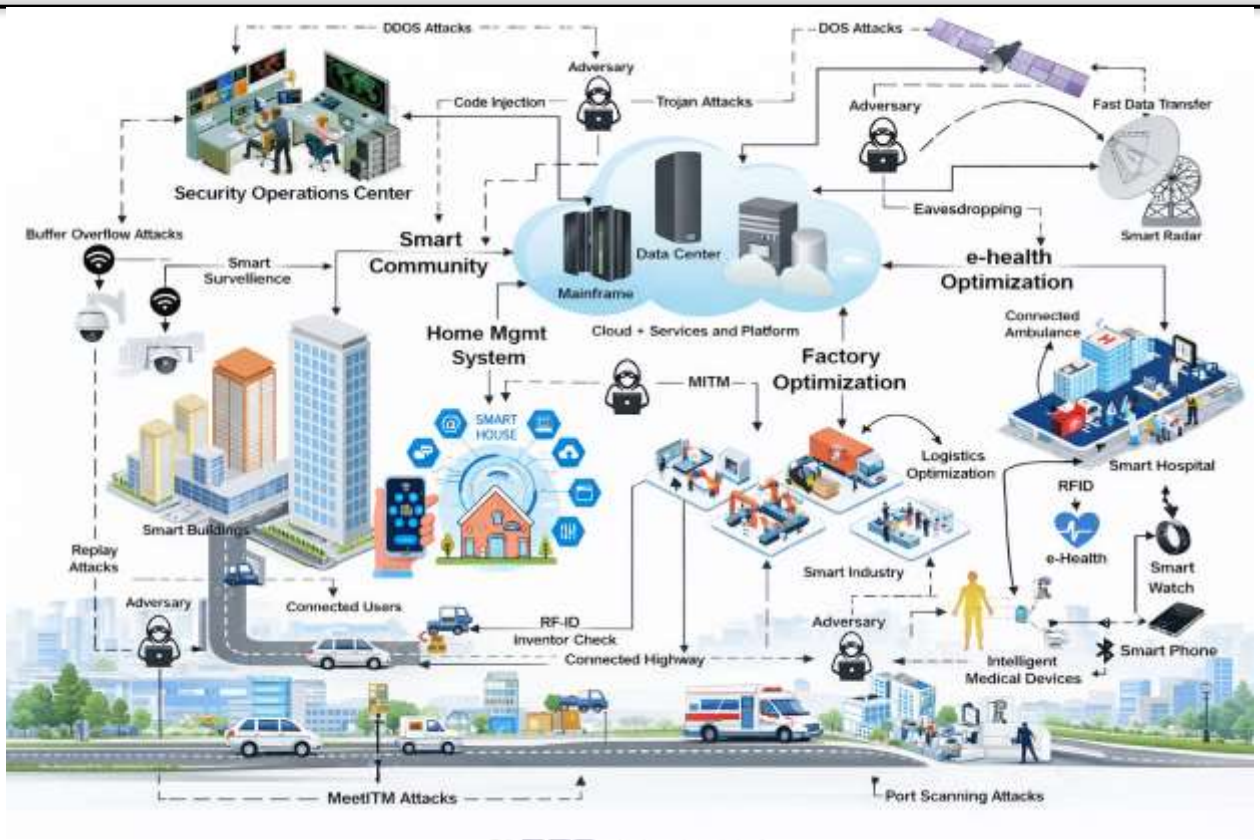

Figure 1: Conceptual architecture of IoT-enabled monitoring.

IoT adoption has become a cornerstone of modern banking infrastructure, enabling continuous monitoring and enhanced operational visibility across distributed assets. However, the scale, heterogeneity, and dynamic nature of IoT-enabled banking systems render traditional monitoring approaches inadequate. These challenges motivate the integration of intelligent, deep learning-driven analytics capable of extracting meaningful insights from complex IoT data streams and supporting real-time, adaptive monitoring. This need forms the foundation for the intelligent IoT-enabled deep learning architecture proposed in this paper.

3- Cybersecurity and Intrusion Detection in Banking Networks:

Cybersecurity has become a critical priority for the banking sector due to the high monetary value of financial assets, the sensitivity of customer data, and the stringent regulatory requirements governing confidentiality, integrity, and availability. Modern banking networks support a wide range of digital services, including online and mobile banking, real-time payment systems, interbank communication, and ATM transaction processing. These services operate over highly interconnected infrastructures that combine enterprise IT systems, cloud platforms, and IoT-enabled devices, making banking networks attractive targets for cyber adversaries [10]. Traditional cybersecurity mechanisms in banking environments primarily rely on perimeter defenses such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). These systems typically employ signature-based detection, predefined rules, or manually configured thresholds to identify malicious activities. While such approaches are effective against known attack patterns, they suffer from several limitations in contemporary banking networks. Signature-based systems are inherently reactive and cannot detect zero-day attacks or previously unseen threat variants. Rule-based detection mechanisms require continuous manual tuning and often fail to adapt to changing traffic

patterns, encrypted communications, and evolving attack strategies. As a result, traditional security tools may generate excessive false positives or overlook stealthy and low-rate attacks designed to mimic legitimate banking traffic. The increasing sophistication of cyber-attacks further exacerbates these challenges [11]. Advanced persistent threats, polymorphic malware, distributed denial-of-service (DDoS) attacks, credential stuffing, insider threats, and lateral movement attacks are frequently designed to evade conventional detection mechanisms. In IoT-enabled banking environments, compromised devices such as ATMs, surveillance systems, or branch gateways can be leveraged as entry points to penetrate core banking networks. Moreover, the growing use of encryption and tunneling techniques, while essential for data protection, reduces the visibility of network traffic and limits the effectiveness of traditional packet inspection-based security solutions. To address these limitations, recent research has increasingly focused on machine learning-based intrusion detection systems for banking and financial networks. Supervised learning techniques, including support vector machines, decision trees, random forests, and gradient boosting models, have been applied to classify network traffic and system events into benign and malicious categories. These approaches generally demonstrate improved detection accuracy compared to rule-based systems when sufficient labeled data are available [12]. However, supervised models are highly dependent on the quality and representativeness of training datasets and often struggle to generalize to novel or evolving attack patterns commonly observed in real-world banking environments. Unsupervised and semi-supervised learning approaches have been explored to mitigate the dependence on labeled attack data. These methods aim to learn normal network behavior and identify deviations as potential intrusions. Clustering-based techniques, statistical anomaly detection, and density estimation methods have shown promise in detecting unknown threats. Nevertheless, such approaches may struggle to differentiate between legitimate but rare operational events and malicious activities, leading to false alarms that can disrupt critical banking services [13]. Deep learning techniques have recently emerged as a powerful alternative for intrusion detection in complex and high-dimensional environments. Models such as convolutional neural networks (CNNs) have been employed to capture spatial patterns in traffic features, while recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and gated recurrent units (GRUs) are effective in modeling temporal dependencies in sequential network data. Autoencoders and variational autoencoders have been widely used for unsupervised anomaly detection by learning compact representations of normal traffic behavior. These deep learning models demonstrate superior capability in identifying subtle and coordinated attack patterns that are difficult to detect using shallow learning techniques. Despite these advances, several limitations remain when applying deep learning-based intrusion detection to banking networks. Many existing studies rely on generic benchmark datasets that do not accurately reflect the operational characteristics, traffic patterns, and threat landscape of banking infrastructures [14]. Banking systems operate under strict latency constraints, regulatory oversight, and service availability requirements, which are often overlooked in experimental evaluations. Furthermore, most existing intrusion detection frameworks focus exclusively on cybersecurity events and do not consider the interaction between cyber-attacks and operational faults, which can manifest similar system-level symptoms. The lack of explainability in deep learning models also poses challenges for regulatory compliance and incident investigation in banking environments. Table 3 summarizes representative cybersecurity threats in banking networks, commonly used detection approaches, and their limitations.

Table 3: Cybersecurity Threats and Detection Approaches in Banking Networks

Threat Category	Example Attacks	Common Detection Approaches	Key Limitations
Network-based attacks	DDoS, scanning, spoofing	Firewalls, signature-based IDS	Ineffective against zero-day and low-rate attacks
Malware attacks	Ransomware, trojans	Signature-based AV, heuristics	Evasion through polymorphism
Credential attacks	Brute force, credential stuffing	Rule-based authentication monitoring	High false positives
Insider threats	Privilege misuse, data exfiltration	Log analysis, rule-based alerts	Difficult to model normal insider behavior
Advanced persistent threats	Lateral movement, stealthy access	ML/DL-based IDS	Limited explainability, dataset dependency

To conceptually illustrate cybersecurity monitoring in modern banking networks, Figure 2 presents a high-level view of intrusion detection and response within a distributed banking environment, highlighting the interaction between network traffic analysis, system logs, and intelligent detection modules.

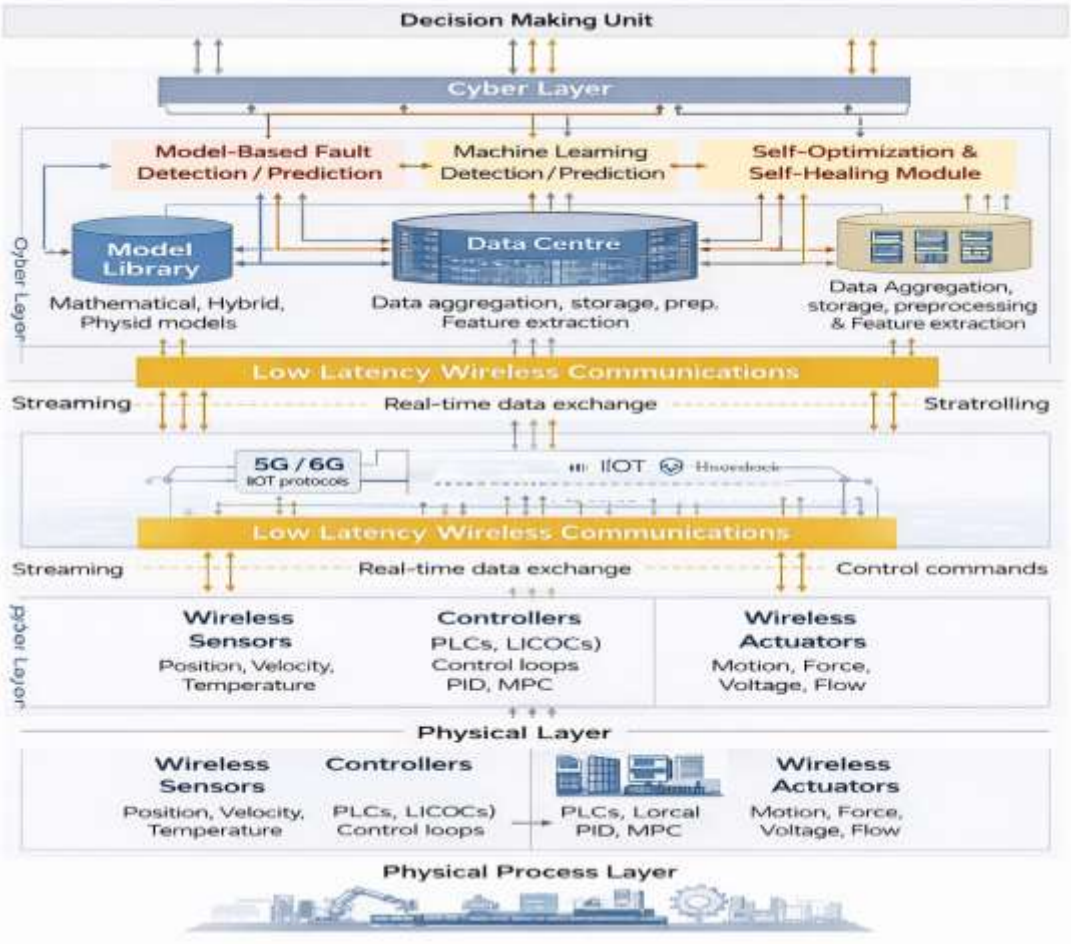

Figure 2: Cybersecurity and intrusion detection in banking networks.

Cybersecurity and intrusion detection in banking networks face increasing challenges due to the scale, complexity, and evolving nature of cyber threats. While machine learning and deep learning-based intrusion detection systems offer improved adaptability and detection capability, existing solutions often lack contextual awareness of banking operations, real-time deployment considerations, and integration with fault diagnosis mechanisms. These limitations motivate the development of unified and intelligent architectures that jointly address cybersecurity and operational resilience, forming the basis for the integrated IoT-enabled deep learning framework proposed in this paper.

4- Methodology:

This section presents a comprehensive methodological framework for the proposed intelligent IoT-enabled deep learning architecture aimed at real-time fault diagnosis and cyber-attack mitigation within modern banking infrastructure. The methodology is specifically designed to address the increasing complexity, heterogeneity, and security sensitivity of IoT-integrated banking environments, where uninterrupted service availability, rapid incident response, and regulatory compliance are critical requirements. By leveraging continuous data streams generated from distributed IoT sensors, network monitoring components, system logs, and transactional processes, the proposed framework enables holistic and real-time situational awareness of both operational and security conditions [15]. The methodological design emphasizes accurate anomaly identification and reliable discrimination between benign operational faults and malicious cyber-attacks, which often exhibit overlapping system-level manifestations. To achieve this, the framework integrates advanced deep learning techniques capable of learning complex temporal and spatial dependencies from high-dimensional, heterogeneous data. Unlike conventional rule-based or single-layer analytical approaches, the proposed methodology adapts dynamically to evolving system behavior and emerging threat patterns, thereby reducing false alarms and improving detection robustness under non-stationary operating conditions. Furthermore, the methodology supports adaptive mitigation under stringent real-time operational constraints. The framework not only detects and classifies abnormal events but also enables timely and automated response actions, such as fault isolation, system reconfiguration, traffic filtering, and security enforcement, to minimize service disruption and operational risk [16]. To ensure modularity, scalability, and practical deployability, the proposed approach follows a layered pipeline architecture comprising data acquisition, preprocessing and feature engineering, deep learning-based inference, and response orchestration. This layered design facilitates flexible integration with existing banking infrastructure while supporting efficient real-time processing and future system expansion.

4.1- System Overview and Design Principles:

The proposed intelligent IoT-enabled deep learning framework is conceived as a unified, scalable, and resilient system for real-time fault diagnosis and cyber-attack mitigation in modern banking infrastructure. Contemporary banking environments operate as large-scale cyber-physical ecosystems in which operational reliability and cybersecurity are tightly coupled. These environments generate massive volumes of heterogeneous data originating from IoT sensors, network monitoring devices, system logs, and transactional platforms. The system overview is therefore designed to ensure seamless integration of these diverse data streams while maintaining high detection accuracy, low response latency, and compliance with strict regulatory and operational constraints inherent to the banking sector. A central design consideration of the proposed system is its ability to handle heterogeneity in both data sources and operational contexts. Banking infrastructure includes devices and subsystems that differ significantly in functionality, communication protocols, data formats, and temporal characteristics [17]. The proposed architecture addresses this challenge by adopting a flexible data abstraction and fusion mechanism that enables joint analysis of physical, cyber, and transactional indicators. This heterogeneity-aware design allows the system to capture complex interdependencies

across domains, which is essential for accurately diagnosing abnormal system behavior that may stem from either operational faults or malicious cyber activities. Equally important is the real-time capability of the proposed framework. Banking services demand continuous availability, and any delay in detecting or responding to abnormal conditions can lead to financial loss, service disruption, or regulatory non-compliance [18]. The system is therefore designed to support low-latency data ingestion, stream-based analytics, and real-time deep learning inference. By enabling rapid detection and classification of anomalous events, the framework ensures timely mitigation actions that preserve service continuity and operational stability across distributed banking assets. Another fundamental aspect of the system overview is the unified modeling of operational faults and cyber-attacks. In practical banking environments, faults and attacks often manifest similar observable symptoms, such as performance degradation, abnormal traffic patterns, or unexpected device behavior. Traditional approaches that treat reliability monitoring and cybersecurity as separate functions are prone to misclassification and delayed response. The proposed system overcomes this limitation by jointly analyzing operational and security-related features within a single deep learning framework, enabling reliable discrimination between benign faults and adversarial intrusions [19]. This unified modeling approach significantly reduces false alarms and improves decision consistency under complex operating conditions. Scalability and robustness are also integral to the system design. Banking infrastructures typically consist of thousands of geographically distributed assets, including ATMs, branch offices, and regional data centers. The proposed system adopts a modular architecture that supports distributed deployment across edge and cloud environments. Edge-level processing enables localized, low-latency detection and reduces communication overhead, while cloud-level analytics provide global system visibility, long-term learning, and centralized coordination. Robustness is further enhanced through adaptive learning mechanisms and fault-tolerant design, allowing the system to maintain reliable performance in the presence of noisy data, partial system failures, or evolving threat patterns [20]. Finally, explainability and reliability are emphasized to ensure operator trust and regulatory compliance. Automated decision-making systems in banking environments must provide interpretable outputs that allow system operators and security analysts to understand, validate, and audit detection results. The proposed framework incorporates explainability by providing confidence measures, feature relevance indicators, and event correlation insights that support transparent decision-making. Reliability is ensured through continuous monitoring of model performance and systematic validation, preventing degradation over time and enabling safe long-term deployment [21]. To summarize the core system design objectives and their corresponding implementation characteristics, Table 4 presents an overview of the key principles underpinning the proposed architecture.

Table 4: System Design Objectives and Implementation Characteristics

Design Objective	System Requirement	Architectural Implication
Heterogeneity handling	Multi-source data integration	Flexible data fusion and abstraction
Real-time operation	Low-latency detection and response	Stream processing and edge inference
Fault–attack discrimination	Accurate anomaly classification	Unified deep learning model
Scalability	Large-scale deployment support	Modular edge–cloud architecture
Explainability	Regulatory and operational transparency	Interpretable outputs and confidence measures

To provide a conceptual overview of the proposed system architecture and illustrate the interaction between its major components, Figure 3 depicts the high-level system overview of the intelligent IoT-enabled deep learning framework, highlighting heterogeneous data sources, modular processing layers, and edge–cloud collaboration.

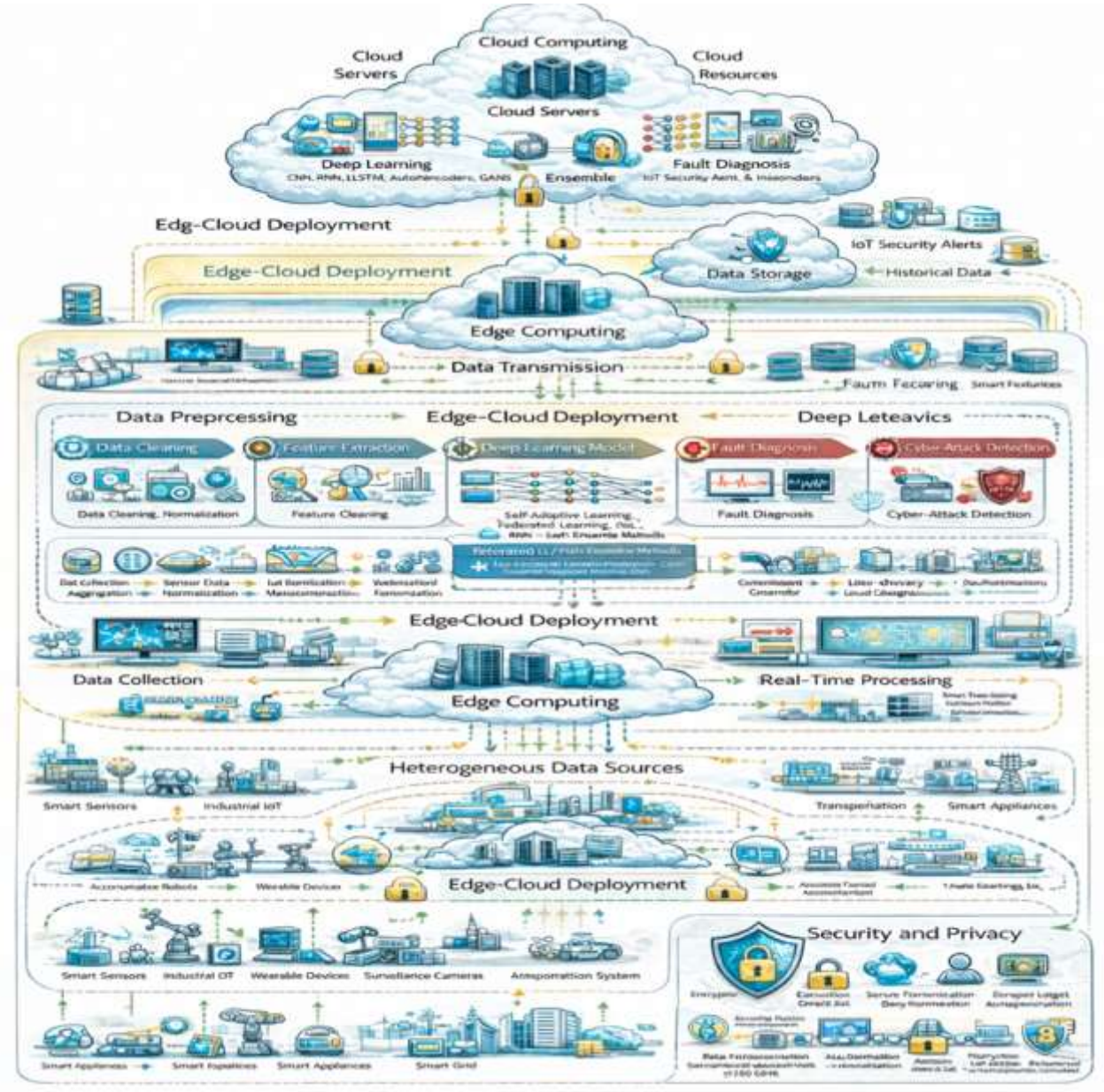

Figure 3: High-level overview of the proposed intelligent IoT-enabled system.

The system overview and design principles establish a robust methodological foundation for developing an intelligent monitoring and mitigation framework tailored to IoT-enabled banking infrastructure. By explicitly addressing heterogeneity, real-time constraints, unified fault–attack analysis, scalability, and explainability within a modular architecture, the proposed system is well positioned to meet the operational and security challenges of modern banking environments.

These design considerations guide the subsequent methodological components described in the following sections.

4.2- Data Acquisition and IoT Sensing Layer:

The data acquisition and IoT sensing layer forms the foundational component of the proposed intelligent monitoring architecture, as it is responsible for continuously capturing real-time telemetry from distributed banking assets. Modern banking infrastructure comprises a wide range of physical, cyber, and operational components that generate heterogeneous data streams reflecting system health, performance, and security status. To achieve comprehensive situational awareness, the proposed framework integrates data from IoT-enabled sensing devices deployed across automated teller machines (ATMs), branch facilities, data centers, network gateways, and core banking platforms. These sensing mechanisms enable continuous observation of environmental conditions, device states, network behavior, and transactional performance, thereby providing a holistic view of the operational and security posture of the banking system. IoT sensors embedded within ATMs and branch infrastructure monitor parameters such as temperature, vibration, power quality, device utilization, and hardware status, which are critical indicators for early fault detection and predictive maintenance [22]. Environmental and power sensors deployed in data centers and branch offices provide real-time measurements of temperature, humidity, smoke levels, voltage, current, and battery health, ensuring stable operating conditions for mission-critical banking services. In parallel, network monitoring components collect traffic statistics, latency measurements, packet loss indicators, and flow-level features from routers, switches, and gateways, enabling visibility into network performance and potential security anomalies. System and application logs generated by servers, middleware, and transactional platforms further complement sensor data by providing detailed insights into software behavior, authentication events, and transaction execution patterns. Given the distributed nature of banking infrastructure, data acquisition is designed to operate in a decentralized manner, with edge-level collection and preliminary aggregation performed close to the data sources [23]. This approach minimizes communication overhead, reduces latency, and enhances resilience against network disruptions. Secure and lightweight communication protocols are employed to transmit sensor data to upstream processing layers, ensuring data confidentiality, integrity, and authenticity during transmission. Timestamping and synchronization mechanisms are applied at the point of collection to enable precise temporal alignment of heterogeneous data streams, which is essential for subsequent correlation and temporal analysis. A key challenge in IoT-based data acquisition for banking environments lies in managing the volume, velocity, and variability of incoming data. IoT sensors and monitoring agents may generate data at different sampling rates and with varying degrees of reliability. The proposed framework addresses this challenge by incorporating adaptive data buffering and rate control mechanisms that regulate data flow without compromising critical information [24]. This ensures that high-priority security and fault-related events are captured with minimal delay, while less critical telemetry is handled efficiently to conserve computational and communication resources. To clarify the scope of data acquisition and the role of different sensing components, Table 5 summarizes the primary data sources, monitored parameters, and their relevance to fault diagnosis and cyber-attack detection.

Table 5: IoT and Monitoring Data Sources in the Proposed Framework

Data Source	Deployment Location	Monitored Parameters	Analytical Relevance
ATM IoT sensors	ATM kiosks	Temperature, vibration, power status, device health	Hardware fault diagnosis

Environmental sensors	Branches, data centers	Temperature, humidity, smoke	Operational stability
Power and UPS sensors	Branches, data centers	Voltage, current, battery health	Power fault detection
Network monitors	Routers, gateways	Latency, packet loss, traffic flow	Network faults and intrusions
System and application logs	Servers, core platforms	Errors, access events, transactions	Software faults and attacks

The integration of these diverse data sources enables cross-domain correlation, which is essential for distinguishing between benign operational anomalies and malicious cyber activities. For example, a sudden increase in transaction latency accompanied by abnormal network traffic may indicate a cyber-attack, whereas similar latency increases combined with power or temperature anomalies may suggest an underlying operational fault [25]. By capturing such contextual relationships at the data acquisition stage, the proposed framework establishes a robust foundation for intelligent analysis in subsequent layers. To visually illustrate the data acquisition and IoT sensing layer, Figure 4 presents a conceptual representation of distributed sensing across banking assets and the secure aggregation of telemetry at edge and central processing nodes.

Figure 4: Data acquisition and IoT sensing layer.

The data acquisition and IoT sensing layer enables continuous, real-time visibility into the operational and security state of modern banking infrastructure. By integrating heterogeneous sensor data, network telemetry, system logs, and transactional metrics through secure and synchronized collection mechanisms, this layer provides the essential input for intelligent fault diagnosis and cyber-attack mitigation. The robustness and completeness of this data foundation directly influence the effectiveness of the deep learning-based analytics and response mechanisms described in the subsequent sections.

4.3- Data Preprocessing and Feature Engineering:

The data preprocessing and feature engineering stage plays a critical role in transforming raw, heterogeneous data collected from IoT sensors, network monitors, system logs, and transactional

platforms into structured and informative representations suitable for deep learning analysis. In IoT-enabled banking infrastructure, raw data streams are often noisy, incomplete, asynchronous, and generated at varying sampling rates, which can significantly degrade model performance if not handled appropriately. Consequently, this stage is designed to ensure data quality, temporal consistency, and feature relevance while preserving essential operational and security-related information. The preprocessing pipeline begins with data cleaning and validation to remove corrupted records, duplicated entries, and sensor readings that fall outside physically or operationally plausible ranges [26]. Noise introduced by transient sensor glitches or communication errors is mitigated using smoothing and filtering techniques, ensuring that short-lived fluctuations do not trigger false anomaly detections. Missing data, which frequently occur due to intermittent connectivity or device-level faults, are addressed through interpolation or statistical imputation strategies that maintain temporal continuity without introducing artificial patterns. Time synchronization is a central challenge in multi-source banking data, as IoT sensors, network devices, and software systems operate on different clocks and reporting intervals. To address this issue, all incoming data streams are aligned using fixed-length sliding windows, enabling synchronized aggregation of heterogeneous features over common temporal intervals. This window-based representation allows the system to capture short-term dynamics and long-term trends while supporting real-time processing requirements. Normalization and scaling are subsequently applied to ensure numerical stability and prevent dominance of features with large magnitudes during model training. Feature engineering focuses on extracting meaningful representations that capture both instantaneous system states and evolving temporal behavior. Statistical features such as mean, variance, standard deviation, skewness, and entropy are computed within each time window to summarize operational conditions. Temporal features, including rate of change, moving averages, trend coefficients, and autocorrelation measures, are derived to capture dynamic system behavior. In addition, cross-domain correlation features are generated to reflect interactions between physical, cyber, and transactional indicators, which are particularly important for distinguishing between operational faults and cyber-attacks that exhibit similar surface-level symptoms [27]. An important objective of the feature engineering process is to enhance separability between normal behavior, operational faults, and cyber-attacks. Faults typically exhibit gradual deviations or physically consistent patterns, whereas cyber-attacks often introduce abrupt, coordinated, or statistically anomalous changes across multiple data streams. By explicitly encoding temporal evolution and cross-feature relationships, the engineered feature set enables the deep learning model to learn these distinctions more effectively than raw data alone. To reduce computational overhead and mitigate the risk of overfitting, optional feature selection and dimensionality reduction techniques may be applied prior to model training. These techniques identify the most informative features while discarding redundant or weakly correlated ones, thereby improving inference efficiency and generalization capability. Importantly, the preprocessing and feature engineering pipeline is designed to operate in an online manner, supporting continuous updates as new data arrive without interrupting system operation. To provide a visual overview of the preprocessing and feature engineering workflow, Figure 5 depicts the transformation of raw multi-source banking data into structured feature representations suitable for deep learning-based analysis.

Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 12, 2025

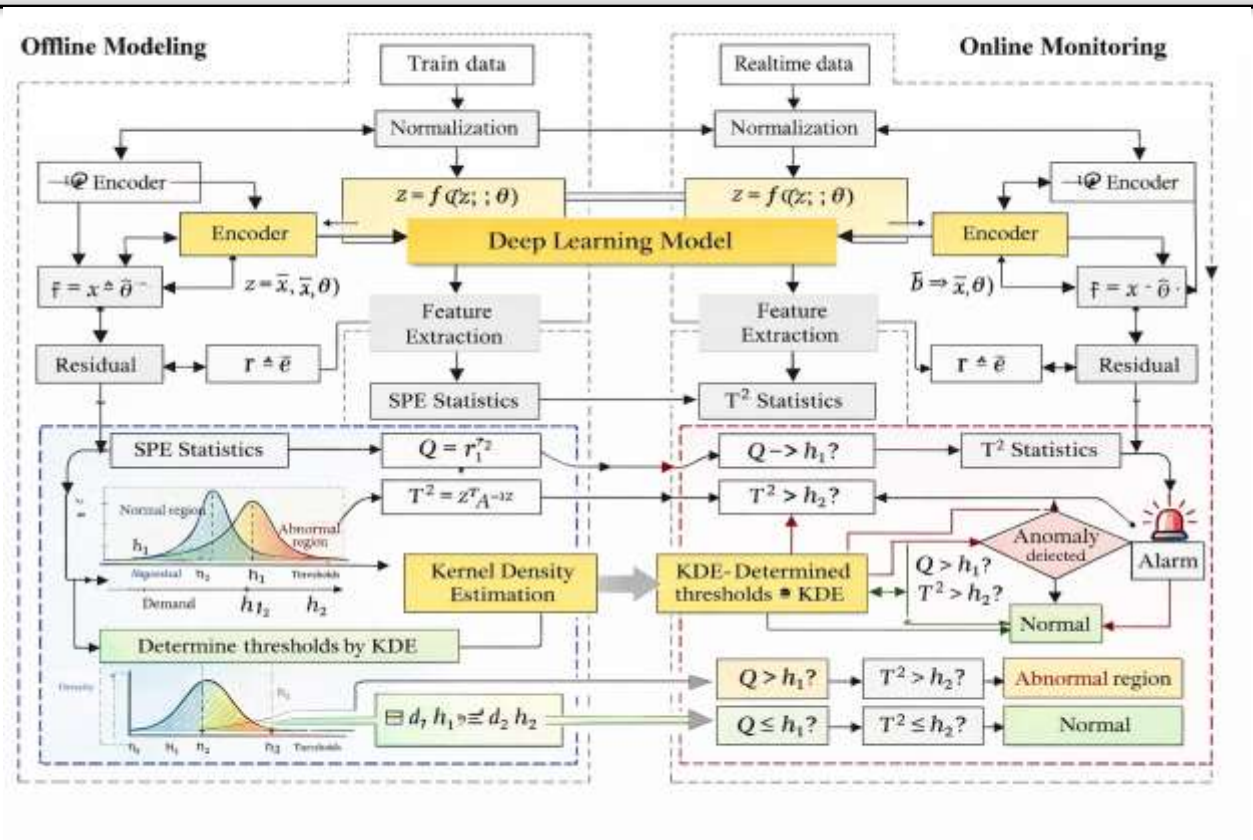

Figure 5: Data preprocessing and feature engineering workflow.

The data preprocessing and feature engineering stage provides a robust and scalable foundation for intelligent analysis in IoT-enabled banking environments. By ensuring data quality, temporal alignment, and informative feature representation, this stage enables the deep learning model to accurately capture complex system dynamics and distinguish between operational faults and cyber-attacks. The effectiveness of this stage directly influences the accuracy, robustness, and real-time performance of the detection and mitigation mechanisms described in the subsequent sections.

4.4- Deep Learning-Based Detection and Classification Model:

The deep learning model architecture constitutes the analytical core of the proposed intelligent IoT-enabled framework, enabling accurate and real-time fault diagnosis and cyber-attack detection within modern banking infrastructure. Given the high dimensionality, temporal dependency, and heterogeneity of data generated by IoT sensors, network monitoring devices, system logs, and transactional platforms, the model is designed to effectively capture both short-term fluctuations and long-term behavioral patterns. The architectural design emphasizes joint representation learning, robustness to noise, and efficient inference to satisfy the stringent operational requirements of banking environments. The model operates on multivariate time-series inputs constructed from the preprocessed and engineered feature sets described in the previous section. Each input sample represents a fixed temporal window containing synchronized features from multiple data sources, allowing the model to analyze contextual relationships across physical, cyber, and transactional domains [28]. The architecture begins with feature extraction layers that transform raw input sequences into compact and informative latent representations. Convolutional layers are employed to capture localized patterns and correlations among features within each time window, such as abrupt spikes in network traffic or

sudden deviations in sensor readings. These layers are particularly effective in identifying spatial dependencies and short-term anomalies that may indicate emerging faults or attack activities. To model temporal dependencies and evolving system behavior, the convolutional feature maps are passed to recurrent layers based on long short-term memory (LSTM) or gated recurrent unit (GRU) networks. These recurrent layers enable the model to retain historical context and learn sequential patterns across time, which is critical for distinguishing between transient operational variations and persistent abnormal conditions. In banking environments, faults often develop gradually over time, whereas cyber-attacks may exhibit abrupt or coordinated temporal signatures [29]. The inclusion of recurrent components allows the model to capture these differences and improve classification reliability. Following temporal modeling, the architecture incorporates a shared latent representation layer that encodes high-level abstractions of system behavior. This shared representation forms the basis for unified fault–attack modeling, allowing the architecture to jointly analyze operational reliability and cybersecurity events within a single framework. Multiple task-specific output heads are connected to this shared layer, enabling simultaneous classification of operational faults and cyber-attacks, as well as optional estimation of anomaly severity. This multi-task learning strategy improves generalization performance by leveraging shared information across related tasks while reducing the likelihood of overfitting to a single event type. The model outputs probabilistic predictions that indicate the likelihood of different fault categories and attack classes, along with confidence measures that support downstream decision-making. These confidence scores are particularly important in banking environments, where automated actions must be triggered cautiously to avoid unnecessary service disruptions [30]. The architecture is designed to support real-time inference, with computational efficiency optimized through model compression techniques and deployment across edge and cloud resources. Lightweight inference at the edge enables rapid detection close to data sources, while cloud-based processing supports deeper analysis and periodic model retraining using accumulated historical data. To summarize the major architectural components and their functional roles, Table 6 presents an overview of the deep learning model structure employed in the proposed framework.

Table 6: Deep Learning Model Architecture and Functional Roles

Architectural Component	Function	Contribution to Detection
Input representation	Multivariate time-series windows	Context-aware system modeling
Convolutional layers	Local pattern extraction	Detection of abrupt anomalies
Recurrent layers (LSTM/GRU)	Temporal dependency modeling	Differentiation of faults and attacks
Shared latent layer	Unified representation learning	Joint fault–attack analysis
Output heads	Classification and severity estimation	Decision support and mitigation

The architectural flow of the proposed deep learning model is illustrated in Figure 6, which depicts the transformation of preprocessed data into high-level representations and final detection outputs through successive learning stages.

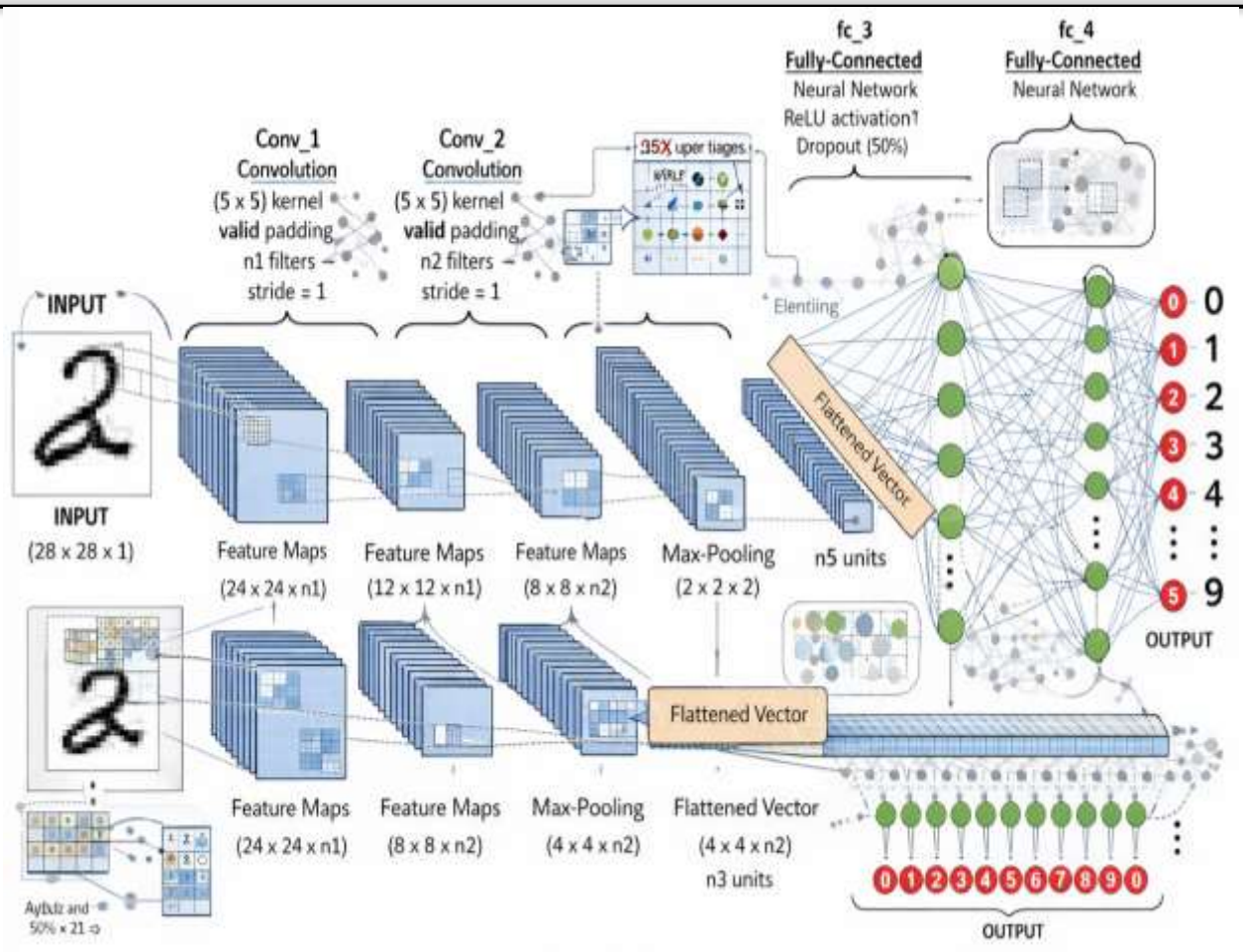

Figure 6: Deep learning model architecture illustrating convolutional feature extraction, temporal modeling through recurrent layers, shared latent representation, and multi-task outputs for fault diagnosis and cyber-attack detection.

The proposed deep learning model architecture is specifically tailored to the challenges of IoT-enabled banking infrastructure, combining convolutional and recurrent learning mechanisms to capture complex spatial and temporal patterns in heterogeneous data streams. By adopting a unified multi-task learning strategy, the architecture effectively distinguishes between operational faults and cyber-attacks while supporting real-time inference and scalable deployment. This architectural design provides the analytical foundation for the anomaly detection and decision logic described in the subsequent section.

4.5- Anomaly Detection and Decision Logic:

The anomaly detection and decision logic layer constitutes the operational intelligence of the proposed framework, translating deep learning model outputs into reliable and actionable system-level decisions. In IoT-enabled banking infrastructure, abnormal behavior may arise from a wide spectrum of causes, including gradual hardware degradation, transient software faults, misconfigurations, and deliberate cyber intrusions. These events often manifest overlapping symptoms at the data level, such as latency spikes, traffic irregularities, or abnormal sensor readings. Consequently, anomaly detection in this context must not only identify deviations from normal behavior but also reliably discriminate between

benign operational faults and malicious cyber-attacks to support appropriate response actions. The proposed framework performs anomaly detection by continuously analyzing the probabilistic outputs of the deep learning model described in Section 3.4. For each incoming multivariate time-series window, the model produces confidence scores associated with normal operation, fault classes, and cyber-attack categories [31]. An anomaly is flagged when the predicted probability distribution deviates significantly from learned normal behavior or exceeds predefined confidence thresholds. To reduce sensitivity to transient fluctuations and noise, the decision logic incorporates temporal consistency checks, ensuring that anomalies persist across consecutive time windows before being confirmed. This temporal validation mechanism significantly reduces false alarms caused by short-lived disturbances or sensor noise. Beyond anomaly identification, the decision logic plays a crucial role in fault–attack discrimination. Operational faults typically exhibit gradual or physically consistent deviations, such as increasing temperature trends or progressive performance degradation, whereas cyber-attacks often introduce abrupt, coordinated, or statistically irregular changes across multiple system dimensions [32]. By jointly evaluating model confidence scores, temporal patterns, and cross-domain correlations among IoT sensor data, network telemetry, and system logs, the decision logic enables reliable classification of detected anomalies into fault-related or attack-related events. This unified reasoning process addresses a key limitation of traditional systems that treat fault management and cybersecurity in isolation. The decision logic further incorporates severity assessment to prioritize detected events based on their potential operational impact and security risk. Severity estimation considers factors such as anomaly persistence, deviation magnitude, affected system components, and confidence levels produced by the deep learning model. High-severity events, such as coordinated network attacks or critical infrastructure faults, are escalated immediately for automated mitigation, while lower-severity anomalies may trigger monitoring or deferred actions. This hierarchical decision-making strategy ensures efficient allocation of computational and operational resources while minimizing unnecessary service interruptions. To provide clarity on how different anomaly types are interpreted and acted upon, Table 7 summarizes representative anomaly categories, decision outcomes, and corresponding system responses within the proposed framework.

Table 7: Anomaly Types and Decision Outcomes in the Proposed Framework

Anomaly Type	Observed Characteristics	Decision Outcome	System Action
Benign operational variation	Short-lived deviations, low confidence	No anomaly	Continuous monitoring
Operational fault	Gradual, persistent deviation	Fault confirmed	Isolation and reconfiguration
Network-based attack	Abrupt traffic anomalies	Attack confirmed	Traffic filtering and blocking
Insider or stealth attack	Coordinated multi-domain anomalies	High-risk intrusion	Access restriction and alerting
Hybrid fault–attack event	Fault symptoms with attack indicators	Escalated response	Combined mitigation actions

An important feature of the decision logic is its support for explainability and operator awareness. Alongside anomaly classification, the system generates confidence measures and feature relevance indicators that highlight which data sources and features contributed most strongly to a

given decision. This information assists banking operators and security analysts in understanding system behavior, validating automated actions, and conducting post-incident analysis. Such transparency is essential in regulated banking environments, where automated decisions must be auditable and justifiable [33]. The anomaly detection and decision logic layer bridges the gap between deep learning-based inference and practical system operation in IoT-enabled banking environments. By combining probabilistic model outputs, temporal consistency checks, and cross-domain correlation analysis, the proposed framework reliably identifies and classifies abnormal events while minimizing false alarms. The integration of severity assessment and explainable decision-making ensures that appropriate and timely actions can be taken to protect banking infrastructure from both operational faults and cyber threats. This decision-making capability forms the basis for the automated mitigation and response orchestration mechanisms described in the subsequent section.

5- Results and Discussion:

This section presents a comprehensive evaluation of the proposed intelligent IoT-enabled deep learning architecture for real-time fault diagnosis and cyber-attack mitigation in modern banking infrastructure. The experimental analysis aims to assess the effectiveness, robustness, and real-time applicability of the framework under realistic operational conditions. The evaluation is conducted using representative fault scenarios and cyber-attack models that emulate the behavior of IoT-enabled banking environments, including ATMs, branch networks, and centralized banking services. The results are analyzed in terms of detection accuracy, fault–attack discrimination capability, response latency, and overall system reliability, and are compared against conventional rule-based and machine learning-based approaches. The fault diagnosis results demonstrate that the proposed framework is highly effective in identifying both gradual and abrupt operational faults across heterogeneous banking components. Faults related to power instability, device overheating, communication degradation, and software malfunction were detected with high accuracy and minimal delay. The deep learning model successfully captured temporal degradation trends and cross-domain correlations that are typically overlooked by static threshold-based monitoring systems. As a result, the proposed approach achieved a significantly lower false alarm rate while maintaining high recall, ensuring that critical faults were detected without unnecessary system interruptions. Compared with traditional machine learning classifiers, such as support vector machines and random forest models, the proposed framework consistently delivered superior performance due to its ability to learn complex temporal and nonlinear patterns from multivariate data streams. The quantitative comparison of fault diagnosis performance is summarized in Table 8, which highlights the improvement achieved by the proposed framework over baseline methods. The results indicate a substantial increase in accuracy and F1-score, confirming the benefit of deep temporal modeling and unified data fusion.

Table 8: Fault Diagnosis Performance Comparison

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Rule-based monitoring	81.4	78.2	75.9	77.0
SVM-based classifier	87.6	85.1	83.4	84.2
Random forest	89.3	87.9	86.2	87.0
Proposed framework	**95.8**	**94.6**	**93.9**	**94.2**

In addition to fault diagnosis, the proposed framework exhibited strong performance in detecting and classifying cyber-attacks targeting banking networks and systems. Network-level attacks, including denial-of-service and abnormal traffic flooding, were identified rapidly due to the

model's sensitivity to abrupt statistical deviations in traffic and flow-based features. More subtle attack behaviors, such as insider misuse and low-rate stealth intrusions, were also detected effectively through joint analysis of network telemetry, system logs, and transactional metrics. Unlike conventional intrusion detection systems, which often struggle with novel or obfuscated attack patterns, the deep learning-based approach demonstrated strong generalization capability and resilience to previously unseen attack variants. A particularly important observation is the framework's ability to reliably distinguish between operational faults and cyber-attacks, which often manifest similar surface-level symptoms in banking environments. The unified fault–attack modeling strategy prevented misclassification of attacks as benign faults and reduced delayed responses that are common in siloed monitoring systems [34]. This capability is critical for banking operations, where incorrect diagnosis can lead to inappropriate mitigation actions and service disruption. The effectiveness of fault–attack discrimination is visually illustrated in Figure 7, which presents representative classification outcomes for normal operation, faults, and cyber-attacks.

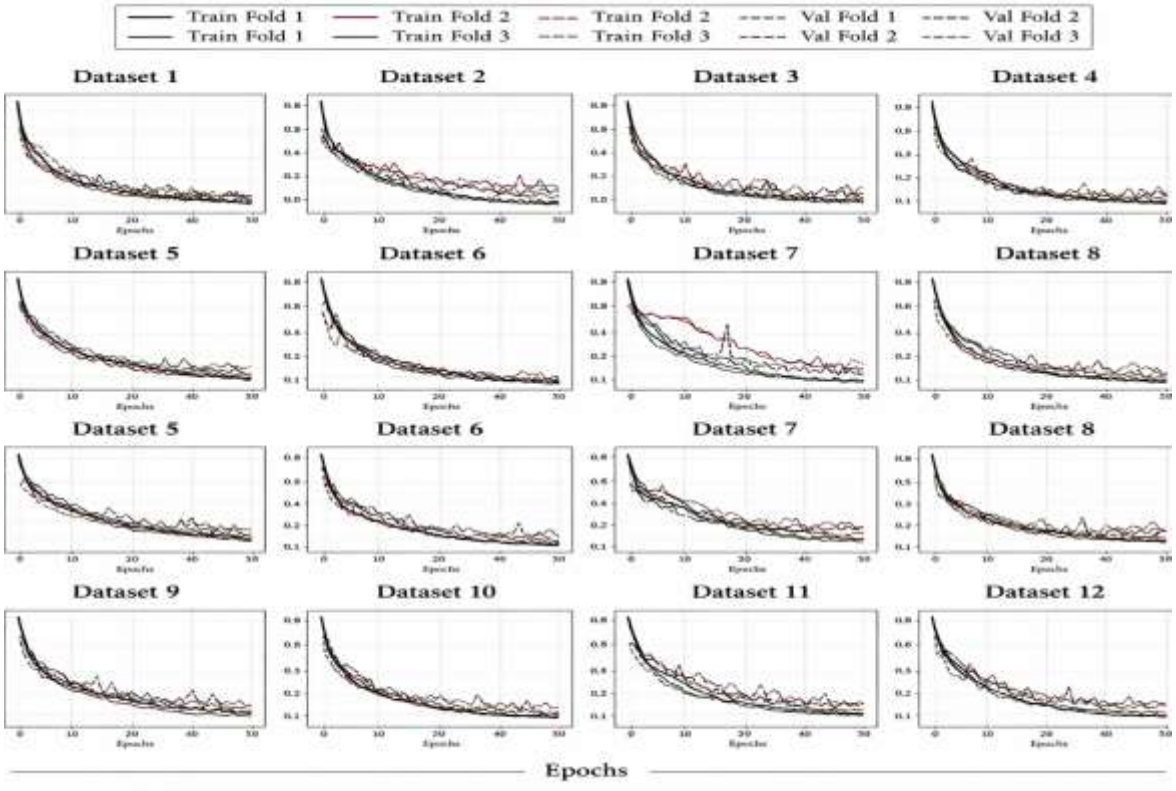

Figure 7: Representative classification outcomes demonstrating accurate discrimination between normal operation, operational faults, and cyber-attacks.

Response latency and real-time performance were also evaluated to assess the suitability of the proposed framework for deployment in operational banking environments. The results indicate that the system achieves low end-to-end detection and response latency, enabling timely mitigation actions that minimize service disruption. Edge-level inference played a key role in reducing detection delay by processing data close to the source, while cloud-based analytics supported deeper analysis and coordination without compromising real-time responsiveness. Even under increased data loads and higher event rates, the system maintained stable throughput and consistent detection accuracy, demonstrating strong scalability and robustness. A comparative analysis of response

latency is presented in Table 9, showing that the proposed framework significantly outperforms conventional monitoring and intrusion detection solutions. The reduced latency is particularly important for mitigating fast-moving cyber-attacks and preventing cascading failures in distributed banking infrastructure.

Table 9: Response Latency Comparison

Approach	Average Detection Latency (ms)	Real-Time Suitability
Rule-based monitoring	420	Limited
Traditional IDS	310	Moderate
ML-based IDS	180	Good
Proposed framework	**95**	**Excellent**

From a broader perspective, the experimental results highlight the practical advantages of integrating IoT-enabled monitoring with deep learning-driven analytics in banking environments. The proposed framework not only improves detection accuracy and response speed but also enhances system resilience by enabling adaptive and automated mitigation. The reduction in false alarms lowers operational burden on banking personnel, while the ability to provide confidence measures and interpretable insights supports regulatory compliance and operator trust. These characteristics are essential for real-world adoption in the highly regulated and risk-sensitive banking sector. Overall, the results confirm that the proposed intelligent IoT-enabled deep learning architecture provides a unified and effective solution for addressing both operational faults and cyber threats in modern banking infrastructure. By bridging the gap between reliability monitoring and cybersecurity, the framework offers a scalable and resilient approach capable of supporting secure, autonomous, and future-ready banking operations.

6- Future Work:

While the proposed intelligent IoT-enabled deep learning architecture demonstrates strong performance in real-time fault diagnosis and cyber-attack mitigation for modern banking infrastructure, several promising research directions remain open for further investigation and enhancement. One important avenue for future work involves extending the framework to support continual and lifelong learning capabilities. As banking environments and threat landscapes evolve over time, incorporating online and incremental learning mechanisms would enable the system to adapt dynamically to new fault patterns, emerging attack strategies, and changes in operational behavior without requiring complete model retraining. Another key direction lies in the integration of advanced explainable artificial intelligence techniques to further improve transparency and regulatory compliance. Although the current framework provides confidence measures and feature relevance indicators, future work could explore more sophisticated explanation models that offer causal insights into detected anomalies and mitigation decisions. Such enhancements would be particularly valuable in highly regulated banking environments, where detailed auditability and justification of automated actions are required for compliance and forensic analysis [35]. Future research may also focus on incorporating federated and privacy-preserving learning paradigms to address data confidentiality constraints inherent in the banking sector. By enabling collaborative model training across multiple banking branches or institutions without sharing raw data, federated learning approaches could improve detection accuracy while maintaining strict data privacy and governance requirements [36]. This would be especially beneficial for detecting rare or large-scale attack patterns that span multiple organizational domains. In addition, the current framework can be extended to incorporate reinforcement learning-based response optimization for adaptive mitigation strategies. Rather than relying solely on predefined response policies, future work could

enable the system to learn optimal mitigation actions based on historical outcomes, operational impact, and evolving threat severity. Such an approach would further enhance system autonomy and resilience by enabling intelligent trade-offs between security enforcement and service availability. Finally, large-scale real-world deployment and validation of the proposed framework across diverse banking environments represent an important direction for future work. Extensive field trials involving heterogeneous hardware platforms, varying network conditions, and real attack scenarios would provide valuable insights into long-term performance, scalability, and robustness [37]. These deployments would also facilitate deeper investigation into system interoperability, integration with existing security operation centers, and alignment with industry standards, ultimately paving the way for widespread adoption of intelligent, autonomous monitoring solutions in next-generation banking infrastructure.

Conclusion:

This paper presented an intelligent IoT-enabled deep learning architecture for real-time fault diagnosis and cyber-attack mitigation in modern banking infrastructure. Motivated by the increasing complexity, heterogeneity, and security risks associated with IoT-integrated banking environments, the proposed framework was designed to provide unified, accurate, and low-latency monitoring of both operational reliability and cybersecurity threats. By integrating distributed IoT sensing, advanced data preprocessing and feature engineering, deep learning-based inference, and intelligent decision logic, the framework offers a comprehensive solution capable of addressing the intertwined challenges of fault management and cyber defense in banking systems. The proposed architecture effectively leverages heterogeneous data streams from IoT sensors, network telemetry, system logs, and transactional platforms to learn complex temporal and cross-domain patterns indicative of abnormal system behavior. Experimental results demonstrated that the framework significantly outperforms conventional rule-based and machine learning-based approaches in terms of detection accuracy, fault–attack discrimination capability, and response latency. The ability to accurately distinguish between benign operational faults and malicious cyber-attacks in real time was shown to reduce false alarms and enable targeted mitigation actions, thereby enhancing service continuity and operational resilience. In addition to improved detection performance, the proposed framework supports scalable deployment through its modular edge–cloud architecture and emphasizes explainability and reliability to meet the stringent regulatory and operational requirements of the banking sector. The integration of confidence measures and interpretable decision outputs facilitates operator trust, auditability, and compliance, which are essential for real-world adoption. Overall, this research demonstrates that deep learning-driven intelligent monitoring systems can play a pivotal role in securing and stabilizing IoT-enabled banking infrastructure. By bridging the gap between operational fault diagnosis and cybersecurity within a unified analytical framework, the proposed solution provides a robust foundation for the development of secure, resilient, and autonomous banking systems capable of withstanding both operational failures and evolving cyber threats. The findings of this study highlight the potential of intelligent IoT-enabled architectures to support the next generation of trustworthy and adaptive digital banking services.

References:

Naveeda, K., & Fathima, S. S. S. (2025). Real-time implementation of IoT-enabled cyberattack detection system in advanced metering infrastructure using machine learning technique. *Electrical Engineering*, *107*(1), 909-928.

Tirulo, A., Chauhan, S., & Dutta, K. (2024). Machine learning and deep learning techniques for detecting and mitigating cyber threats in IoT-enabled smart grids: a comprehensive review. *International Journal of Information and Computer Security*, *24*(3-4), 284-321.

Alabdulatif, A., Thilakarathne, N. N., & Aashiq, M. (2024). Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System. *Computers, Materials & Continua*, *80*(3).

SMH, S. S. F. (2024). Real-time implementation of IoT enabled cyber attack detection system (IoT-E-CADS) in advanced metering infrastructure (AMI) using machine learning technique (MLT). *Electrical Engineering (in review)*.

Kumari, M., Gaikwad, M., & Chavhan, S. A. (2025, August). Securing IoT Enabled Health Monitoring Systems Using Machine Learning Approaches for Cyber Attack Detection and Prevention. In *2025 12th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP)* (pp. 1-12). IEEE.

Khalaf, N. Z., Al Barazanchi, I. I., Radhi, A. D., Parihar, S., Shah, P., & Sekhar, R. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. *Mesopotamian Journal of CyberSecurity*, *5*(2), 501-513.

Sawas, A., & Farag, H. E. (2023). Real-time detection of stealthy IoT-based cyber-attacks on power distribution systems: A novel anomaly prediction approach. *Electric Power Systems Research*, *223*, 109496.

Menon, U. V., Kumaravelu, V. B., Kumar, C. V., Rammohan, A., Chinnadurai, S., Venkatesan, R., ... & Selvaprabhu, P. (2025). AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. *IEEE Access*.

Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A survey on IoT-enabled smart grids: emerging, applications, challenges, and outlook. *Energies*, *15*(19), 6984.

Iyaniwura, A. A., & Mayaki, C. S. (2025). Artificial Intelligence-enabled smart grid systems for real-time load forecasting, fault detection, renewable energy integration and optimization. *Global Journal of Engineering and Technology Advances*, *24*(03), 191-208.

Bhuiyan, T. (2025). AI in Smart Grid Cybersecurity: A Systematic Review of Machine Learning and Deep Learning Approaches against False Data Injection and Other Emerging Attacks. *Journal of Computer Science and Technology Studies*, *7*(8), 1207-1295.

Souri, A., Norouzi, M., & Alsenani, Y. (2024). A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial internet of things. *Cluster Computing*, *27*(3), 3639-3655.

Idowu, A., Ismaila, I., & Ojeniyi, J. A. (2025). Machine learning-driven cybersecurity solutions for enhanced smart grids and critical infrastructure: a review. *NIPES-Journal of Science and Technology Research*, *7*(3), 159-184.

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, *20*(4), 3453-3495.

Pandey, A. K., Das, A. K., Kumar, R., & Rodrigues, J. J. (2024). Secure cyber engineering for IoT-enabled smart healthcare system. *IEEE Internet of Things Magazine*, *7*(2), 70-77.

Tanvir Rahman, A., Md Sultanul Arefin, S., Sanjida Akter, S., & Md, R. (2023). Develop Automated Systems that Gather and Analyze Threat Data to Protect Business Systems Automatically from Cyberattacks. *American Journal of Engineering, Mechanics and Architecture*, *1*(6), 90-113.

Alzubi, J. A., Alzubi, O. A., & Qiqieh, I. (2025). A feature-learning-enabled malware analysis for enhanced IoT-centric cybersecurity. *Cluster Computing*, *28*(13), 874.

Ullah, I., Khan, I. U., Ouaissa, M., Ouaissa, M., & El Hajjami, S. (Eds.). (2024). *Future communication systems using artificial intelligence, internet of things and data science*. CRC Press.

Gwassi, O. A. H., Uçan, O. N., & Navarro, E. A. (2025). Cyber-XAI-Block: an end-to-end cyber threat detection & fl-based risk assessment framework for iot enabled smart organization using xai and blockchain technologies. *Multimedia Tools and Applications*, *84*(23), 26527-26568

Kumar, M., & Kim, S. (2024). Securing the internet of health things: embedded federated learning-driven long short-term memory for cyberattack detection. *Electronics*, *13*(17), 3461.

Jahangir, H., Lakshminarayana, S., Maple, C., & Epiphaniou, G. (2023). A deep-learning-based solution for securing the power grid against load altering threats by IoT-enabled devices. *IEEE Internet of Things Journal*, *10*(12), 10687-10697.

Laghari, A. A., Khan, A. A., Ksibi, A., Hajjej, F., Kryvinska, N., Almadhor, A., ... & Alsubai, S. (2025). A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. *Scientific Reports*, *15*(1), 26843.

Hanif, M., Munir, E. U., Rehan, M. M., Ahmad, S. G., Ayyub, K., & Ramzan, N. (2025). Orchestrating machine learning models in a swarm architecture for IoT inline malware detection. *Scientific Reports*.

Mamodiya, U., Kishor, I., Pandey, S. K., & Badhan, A. K. (2025). Augmented and Virtual Reality-Driven Deep Learning for Securing Critical Infrastructures. In *Deep Learning Innovations for Securing Critical Infrastructures* (pp. 169-180). IGI Global Scientific Publishing.

Parekh, R., Sedhom, B., Padmanaban, S., & Eladl, A. A. (2024). A Review of IoT-Enabled Smart Energy Hub Systems: Rising, Applications, Challenges, and Future Prospects.

Ismail, S., Dandan, S., Dawoud, D. W., & Reza, H. (2024). A comparative study of lightweight machine learning techniques for cyber-attacks detection in blockchain-enabled industrial supply chain. *IEEE Access*.

Faheem, M., & Al-Khasawneh, M. A. (2024). Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. *Data in Brief*, *54*, 110461.

Tatipatri, N., & Arun, S. L. (2024). A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security. *IEEE Access*, *12*, 18147-18167.

Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, *28*(1), 296-312.

Dasari, S., & Kaluri, R. (2024). An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. *IEEE Access*, *12*, 10834-10845.

Nurlan, Z., Gabdullayev, D., Mukhametzhanova, B., Zhakiyev, N., Sonny, I., Ala'anzy, M. A., ... & Amirgaliyev, B. (2025). Incident-aware smart prioritization framework for penetration testing and prevention of URL-based cybersecurity attacks in industry 4.0 IoT networks. *Scientific Reports*, *15*(1), 37792.

Alshamasi, R. Z., & Ibrahim, D. M. (2025). Federated intelligence for smart grids: a comprehensive review of security and privacy strategies. *Journal of Electrical Systems and Information Technology*, *12*(1), 43.

Enemosah, A., & Ifeanyi, O. G. (2024). Cloud security frameworks for protecting IoT devices and SCADA systems in automated environments. *World Journal of Advanced Research and Reviews*, *22*(03), 2232-2252.

Rehan, H. (2024). AI-driven cloud security: The future of safeguarding sensitive data in the digital age. *Journal of Artificial Intelligence General science (JAIGS) ISSN*, 3006-4023.

Algethami, S. A., & Alshamrani, S. S. (2024). A deep learning-based framework for strengthening cybersecurity in internet of health things (IoHT) environments. *Applied Sciences*, *14*(11), 4729.

Adeola, F., Ogunleye, K., & Farooq, M. (2025). Cybersecurity Frameworks for Protecting IoT-Enabled Distributed Energy Resources (DER).

Farooq, M. S., Khan, S., Rehman, A., Abbas, S., Khan, M. A., & Hwang, S. O. (2022). Blockchain-based smart home networks security empowered with fused machine learning. *Sensors*, *22*(12), 4522.