Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

AI-Driven Threat Detection In 5G Edge computing environments Post-2024 Rollout

Akinrinsola Akinseye [1,*], Mary Akinseye [2], Vincent Anyah [3] and Adewa Adeola [4]

[1] *Department of Physics, University of Ilorin, P.M.B. 1515, Ilorin, Kwara State, Nigeria.*
[2] *Levin College of Public Affairs and Education, Cleveland State University, 2121 Euclid Avenue, Cleveland, OH 44115, USA.*
[3] *Department of Computer Science, Ivan Hilton Center for Science and Technology, New Mexico Highlands University, Las Vegas, NM, USA.*
[4] *McClure School of Emerging Communication Technologies, Ohio University, Athens, OH, USA.*

Global Journal of Engineering and Technology Advances, 2024, 19(03), 164-185

Publication history: Received on 18 May 2024; revised on 24 June 2024; accepted on 28 June 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.19.3.0109

Abstract

The massive increase in the Internet of Things gadgets and the extensive implementation of fifth-generation networks have already changed the world connectivity environments radically, as well as increasing the attack surface of advanced cyber attackers. The study introduces a thorough study of artificial intelligence-based threat detection systems and is specifically modelled to train in edge computing structures and architectures of the fifth-generation network in the post-2024 rollout stage. The proposed study suggests a new hybrid deep learning intrusion detection system that will combine Convolutional neural networks, Bidirectional Long short-term memory networks and Autoencoder networks together in a federated learning process that will facilitate the training of privacy-preserving collaborative models on distributed edge devices. The investigation will have positive outcomes to such intelligent, scalable, and adaptive security solutions to heterogeneous fifth-generation Internet of Things ecosystems that can enable computational constraints, privacy preservation needs, and real-time detection functions necessary to protect critical infrastructure and support autonomous operations in next-generation wireless networks.

Keywords: Artificial Intelligence; Threat Detection; Fifth-Generation Networks; Edge Computing; Intrusion Detection Systems; Hybrid Deep Learning; Federated Learning; Autoencoder; Network Slicing; Privacy Preservation; Cybersecurity

1. Introduction

The fifth-generation wireless networks and Internet of Things convergence have become a paradigm shift in the global telecommunications infrastructure, allowing unprecedented connectivity, ultra-low latency, and the ability to place devices in a dense array that are redefining the industrial automation, healthcare delivery, autonomous city operation, and autonomous transportation system (Osseiran et al., 2014). The implementation of the fifth-generation networks is beneficial in terms of three main service types such as Enhanced Mobile Broadband to support the high-throughput applications, Ultra-Reliable Low-Latency communications to support the mission-critical services, and Massive Machine-Type communications to support the large sensor deployments.

Integration of edge computing structures in fifth generation network deployments provides the capability to perform computational processing and data analytics at points close to data generating sources, instead of having to transmit them to centralized cloud deployments, and thus reduce latency, bandwidth usage, and privacy protection (Greengard, 2015). Real-time decision-making applications at the network edge require Multi-access Edge Computing platforms, which are deployed at the network periphery and are necessary to support the need of autonomous cars, industrial

* Corresponding author: Akinrinsola Akinseye

control system, telemedicine services, and augmented reality services that demand response times in milliseconds (Roman et al., 2018).

Artificial intelligence systems, especially deep learning systems, have proven to have exceptional potential in managing high-dimensional data, extracting structured features in the form of hierarchies, and undertaking the correct classification of various application fields, such as computer vision, natural language processing, and cybersecurity analytics. Convolutional Neural Networks are effective at representing spatial patterns and local features correlation of structured data representations, Long Short-Term Memory networks are good at modeling the time dependencies and sequential relationships, and Autoencoders offer unsupervised learning features of anomalies in learning by analysing reconstruction errors (Vinayakumar et al., 2019).

1.1. Evolution of Fifth-Generation Networks and Internet of Things Integration

Architectural advancements with the fourth-generation to the fifth-generation wireless technology bring on new fundamental architectures such as network function virtualization, software-defined networking, network slicing, and cloud-core network implementations which allow dynamic resource allocation, service customization, and operational efficiency improvements (Raza et al., 2013). Network slicing functionality will divide physical infrastructure into several logical networks that best serve service needs and enable parallel support of multiple use cases with distinct performance characteristics, quality of service guarantees, and security policies to be supported by shared spectrum resources.

Decoupling network capabilities and proprietary hardware to software components that can be deployed on commercial off-the-shelf servers brings both flexibility and lower costs with it and increases attack surfaces since software vulnerabilities and configuration mistakes and coordination complexities can cause security lapses that can be exploited by advanced adversaries (Shrestha et al., 2023). Potential unauthorized access and privilege escalation targets are application programming interfaces exposures needed to facilitate inter-component communication and service orchestration and lateral movement in network infrastructure (Ali and Kumar, 2022).

1.2. Security Imperatives for Edge Computing Environments

Edge computing architecture spreads computing resources across geographically distributed locations such as base stations, aggregation points, enterprise premises, and customer premises equipment to reduce the latency between data-generation and processing and minimizes the backhaul bandwidth usage and improves responsiveness of applications (Buczak and Guven, 2016). The geographic location of edge servers with end users and devices facilitates real-time analytics, local decision-making, and less reliance on cloud connectivity which is crucial to applications with high latency constraints such as autonomous navigation, industrial process control, augmented reality, and emergency response systems (Shi et al., 2016).

This heterogeneity of edge computing infrastructure with different hardware platforms, operating systems, virtualization technologies, and management structures brings complexity and makes standardization of security more complex, management of vulnerabilities, and compliance checking activities more difficult (Satyanarayana, 2017). Uncoordinated security settings, slow patch updates, and the incomplete access control policy among distributed edge locations give attackers the chance to discover and use the most vulnerable elements within the broader attack surfaces (Debar et al., 2008).

1.3. Artificial Intelligence Applications in Cybersecurity

The technologies of machine learning and deep learning have transformed the practice of cybersecurity by allowing large volumes of data to be analysed automatically, detecting the presence of insidious attack indicators, predicting the emergence of new threats, and responding to changing adversary tactics that are beyond the ability of human analysts to analyze (Roman et al., 2018). Training the assisted learning algorithms with the labeled datasets that include the examples of benign and malicious traffic patterns can precisely classify network flows, detect intrusion attempts, and identify variants of malware with performance that is higher than the traditional signature-based tools.

Multiple layers of deep neural networks learn hierarchical feature representations of raw input data, successively transforming lower-order attributes into higher-order semantic components that support more intricate pattern recognition tasks. Convolutional Neural Networks use spatial locality and translation invariance characteristics to compute grid-structured machine-generated data such as packet headers, network flow statistics and system call sequences and extract localized patterns which give evidence on malicious behavior (Li et al., 2020).

Autoencoders with bottlenecks (dimensionality reduction) that are trained to reconstitute the input information acquire bottlenecks that learn compressed representations of critical information about the data that excludes noise and redundant features (Mirsky et al., 2018). The magnitude of reconstruction error is used as an error indicator of anomalies whereby the inputs that do not show significant variations with the training data distributions generate large reconstruction errors, indicative of induced security incidents that need to be investigated (Vinayakumar et al., 2019).

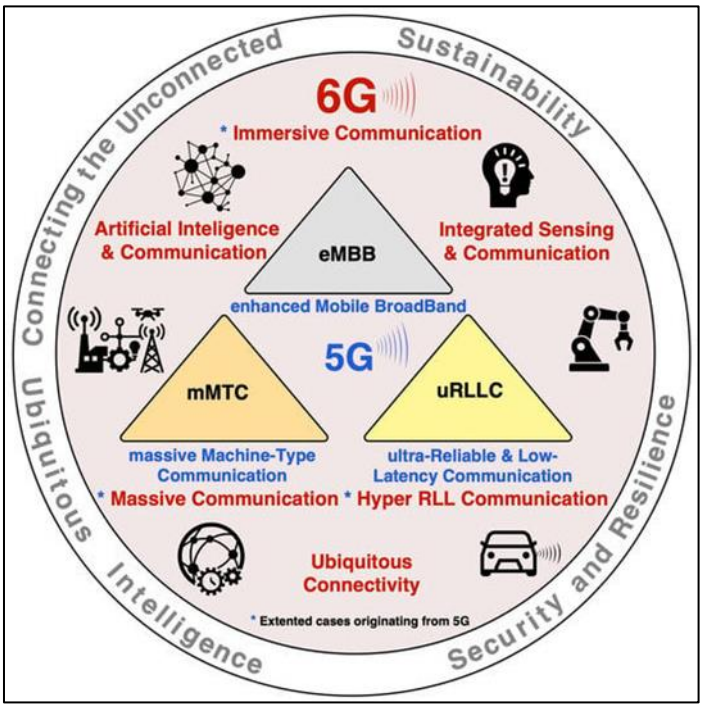

Figure 1 Evolution from Fifth-Generation to Sixth-Generation Networks and Fundamental Key Features (Source: Adapted from Osseiran et al., 2014)

The fifth to sixth-generation wireless network transition is the next generation in technological improvement which introduces artificial intelligence-native architecture, terahertz frequencies, satellite connectivity, and ubiquitous connectivity to support immersive extended reality applications (Osseiran et al., 2014). The current focus of the fifth-generation networks is on three major service categories such as the Enhanced Mobile Broadband which supports peak data rates of more than 10 gigabits per second, Ultra-Reliable Low-Latency Communications which has end-to-end latencies less than one millisecond, and the massive Machine-Type Communications which supports connection densities of more than one million devices per square kilometer (Abdulqadder et al., 2024).

The sixth-generation development considers the experience of the fifth-generation implementation in terms of security behavior, privacy, and trust provisions required to support critical infrastructure and sensitive applications (Roman et al., 2018). According to study by Nguyen and Reddi (2021), artificial intelligence and machine learning are part of the network functioning and not auxiliary, which makes autonomous management of the network possible, predictive maintenance, intelligent resource utilization, and proactive prevention of security threats. Combining sensing feature with communication feature opens new applications of high-precision localization, environmental mapping, gesture recognition, and activity monitoring and brings into view privacy concerns of pervasive sensing infrastructure (Li et al., 2020).

1.4. Research Objectives and Contributions

The study fills key gaps in the current literature as it will introduce a new hybrid deep learning architecture that is optimized precisely to perform intrusion detection in resource-constrained edge computing systems to serve the fifth-generation Internet of Things networks. The main research question is to create an integrated threat detection system, which effectively integrates Convolutional Neural Networks to extract spatial features, Bidirectional Long Short-Term Memory networks to model time dependencies, and Autoencoder models to generate anomaly sensitivity by reconstructing significant features via a single model that would be able to detect various attack types with high accuracy and low latency.

The principal contributions of this investigation encompass the following key elements:

- Novel Hybrid Architecture Design: Development of a three-branch fusion architecture integrating Autoencoder bottleneck representations with Convolutional Neural Network spatial pattern recognition and Bidirectional Long Short-Term Memory temporal context modeling, enabling comprehensive threat detection capabilities surpassing individual model performance (Goodfellow et al., 2016).
- Federated Learning Implementation: Deployment of privacy-preserving distributed training protocols allowing edge devices to collaboratively improve global model performance without sharing raw traffic data, thereby maintaining data sovereignty and regulatory compliance (Yang et al., 2019).
- Comprehensive Performance Evaluation: Rigorous experimental validation using established benchmark datasets demonstrating superior detection accuracy, balanced error rates, and inference latency compatible with Ultra-Reliable Low-Latency Communications requirements.
- Practical Deployment Considerations: Analysis of computational resource requirements, energy consumption profiles, and scalability characteristics relevant for real-world edge computing deployments across heterogeneous hardware platforms (Nasser & Hassan, 2024).
- Explainability and Interpretability: Investigation of model decision-making processes through attention mechanisms and feature importance analysis supporting security analyst understanding and regulatory compliance documentation (Raza et al., 2013).

The further parts of the paper have the following structure: Section 2 provides the system model and architecture that characterizes the fifth-generation Internet of Things network setting, edge computing infrastructure, and threat landscape description; Section 3 explores the edge computing, edge artificial intelligence implementations in the Internet of things and fifth-generation networks; Section 4 outlines the proposed hybrid deep learning methodology comprising data preprocessing, model architecture, and federated learning framework; Section 5 reports the experiment results and performance analysis, Section 6 discusses the implication, limitations, and future research directions; Section 7 concludes.

2. System model and architecture

The modern fifth-generation advanced network architecture is a combination of heterogeneous technology such as radio access networks, core network functionality, edge computing platforms, and cloud infrastructure to provide end-to-end connectivity services to a wide range of applications in the Internet of Things, based on their performance needs (Diro and Chilamkurti, 2018). The system model contains several architecture layers that include physical devices on the edges of the network, between processing tiers, and centralized orchestration and analytics which provide the fundamental capabilities necessary to achieve system functionality (Shrestha et al., 2023).

2.1. Fifth-Generation Advanced Network Infrastructure

Fifth-generation deployments are based on the principles of software-defined networking and network function virtualization technologies to break up the legacy monolithic network components into modular software units running on commercial off-the-shelf hardware platforms. The core network is the implementation of service-based architecture in which the network functions can present standardized interfaces that allow the flexible composition of services, dynamic scaling, and compatibility between vendors (Liao et al., 2013).

The radio access network consists of distributed base stations and centralized processing units that organize wireless transmissions and reception, over more than one frequency band such as sub-6 gigahertz frequencies covering with a range and millimetre-wave spectrum, with capacity (Buczak and Guven, 2016). Massive Multiple-Input Multiple-Output Massive antenna arrays with dozens or hundreds of antenna elements allow spectral efficiency, beamforming, and coverage enhancement and interference reduction methods (Shi et al., 2016).

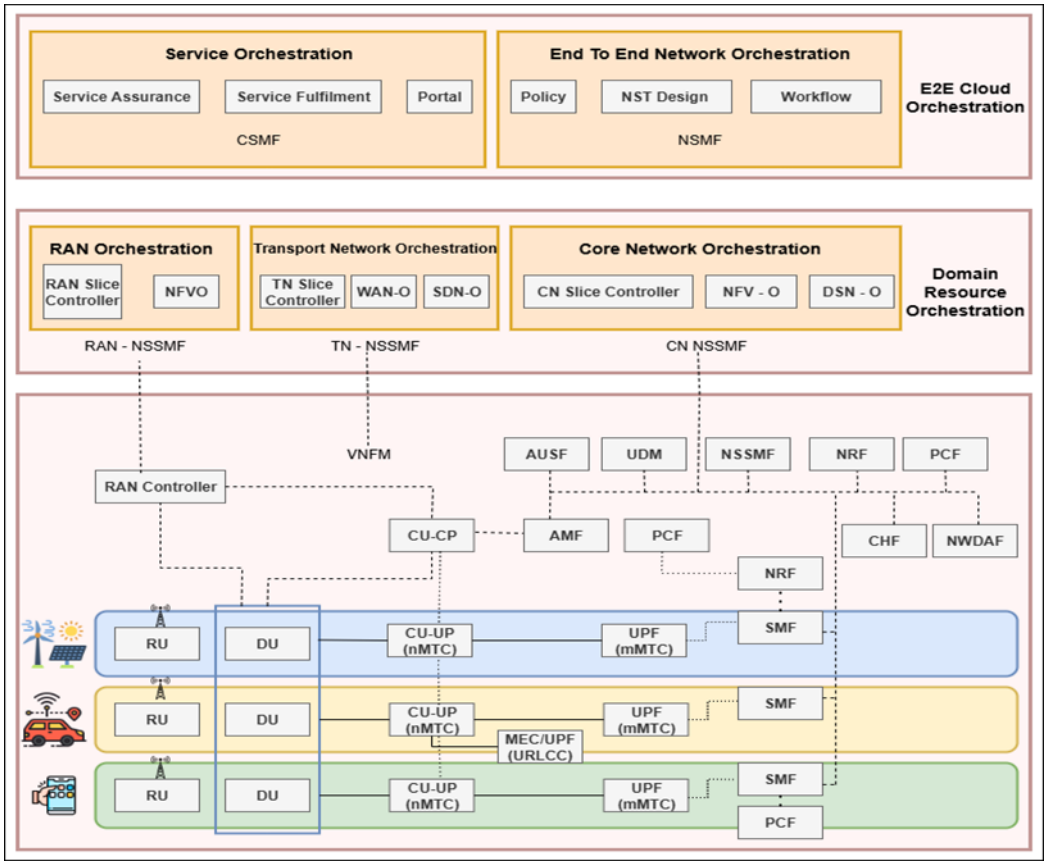

Figure 2 Internet of Things Fifth-Generation End-to-End Orchestration Architecture (Source: Adapted from Diro and Chilamkurti, 2018)

End-to-end orchestration architecture in Figure 2 shows how mobile and Internet of Things devices will be connected through radio access networks to next-generation core network infrastructure accessing internet services (Diro and Chilamkurti, 2018). The firewalls are artificial intelligence-enhanced to conduct deep packet inspection on traffic, traffic filtering, and threat detection on strategic network boundaries to protect unauthorized access and malicious traffic. The access layer consists of mobile and Internet of Things devices, which create various traffic patterns, such as periodic sensor telemetry and streaming multimedia content and interactive application sessions. Radio access networks combine traffic of wireless devices and build secure tunnels to core network functions to be authenticated, manage the session, and enforce the policy (Nguyen and Reddi, 2021).

AI-driven firewalls utilize machine learning algorithms to detect abnormal traffic patterns, malicious flows, and intrusion attacks and block them in real-time without introducing new rules to the firewall system (Liu et al., 2019). The orchestration model facilitates the distribution of resources, the creation of services and the enforcement of policies between heterogeneous components of infrastructure such as physical servers, virtual machines, and containerized microservices (Buczak and Guven, 2016). The security monitoring systems gather the telemetry of distributed network components, correlate the events of various sources, and automatically invoke response activities on recognition of threats (Buczak and Guven, 2016). With artificial intelligence integrated into every part of the network structure, autonomous optimization, predictive maintenance, and intelligent threat mitigation features allow the complexity of operations to be lowered and services to be more reliable.

2.2. Internet of Things Device Ecosystem

The Internet of Things device ecosystem has a huge heterogeneous population of connected endpoints including basic environmental sensors, advanced industrial controllers, and medical devices as well as self-driving vehicles (ITU-T, 2012). Mid-tier Internet of Things devices with reduced capability strike a cost-capability-functionality trade-off by reducing bandwidth to 20 megahertz, omitting carrier aggregation options, and using single receive antenna designs instead of multiple-antenna designs found in full fifth-generation devices. These design options make gadgets less complex and have a longer battery duration without losing connection to fifth-generation networks to implement applications that need moderate data rates and tolerable latency (Debar et al., 2008).

Many Internet of Things devices have resource constraints that prevent the possibility of implementing more secure systems that demand a high level of computational power, memory, or energy usage (Roman et al., 2018). Simple sensors with microcontrollers can have as little as kilobytes of random-access memory and megahertz clock speed that is not enough to execute cryptographic operations or elaborate security protocols (Mao et al., 2017). Devices that rely on batteries need to be particularly considerate about energy consumption to obtain operating lifespan in years, which requires lightweight security solutions reducing processing load and communication volumes.

2.3. Threat Landscape and Attack Vectors

The growing attack space posed by the deployment of fifth-generation Internet of Things applications is appealing to highly sophisticated attackers such as opportunistic script kiddie hackers, organized criminal organizations and nation-state actors with various goals such as making money, stealing intellectual property, disrupting services, and gaining a strategic edge (Li et al., 2020). DDoS attacks exploit the IoT compromised devices to create excessive traffic volumes intending to utilize computational resources, overwhelm network bandwidth, or activate the automated protection strategies that unintentionally block the legitimate users. To create coordinated attack platforms, botnet operators scan internet address spaces, find vulnerable devices, use default credentials or vulnerabilities known to them to gain unauthorized access, install malware that would allow them to be controlled remotely, and pool thousands or millions of compromised endpoints (Mirsky et al., 2018).

Internet of Things systems are targeted by data breaches to steal sensitive data such as personal identifiable information, proprietary industrial data, financial records, or healthcare information that can be sold in an underground market, used as an identity theft tool, or used as a source of competitive intelligence (Vinayakumar et al., 2019). Man-in-the-middle attacks are device to backend service communication, which may capture credentials, eavesdrop sensitive data transmissions, or inject harmful commands to control device behavior.

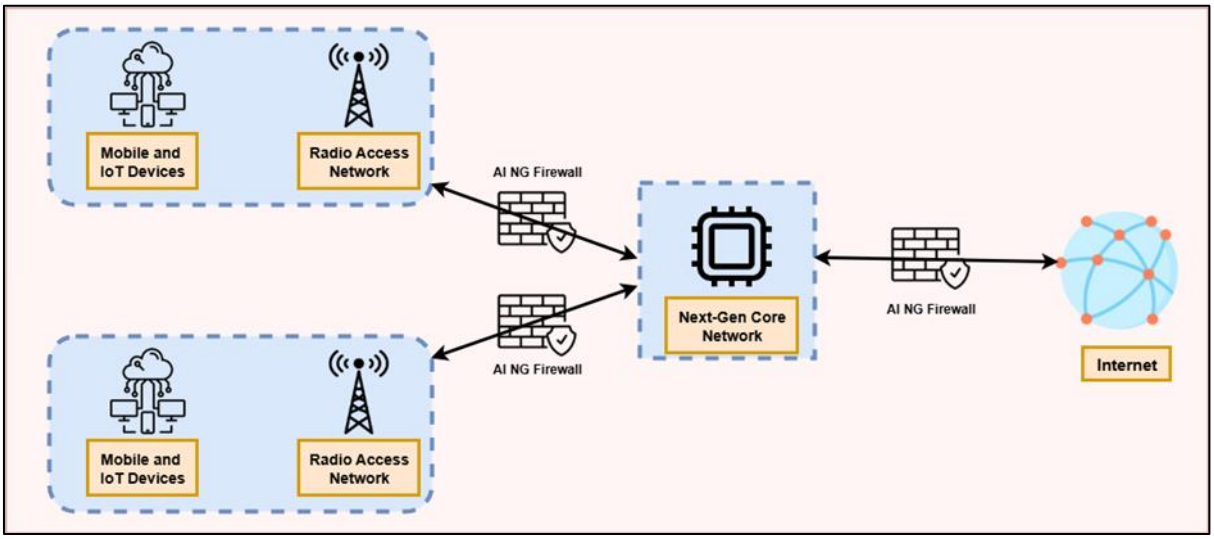

Figure 3 Common Data Transport Links and Associated Threat Vectors (Source: Adapted from Xiao et al., 2019)

The network diagram in Figure 3 shows typical data transportation connections between mobile and Internet of Things gadgets via radio access network to next-generation core network structure and internet services in addition to the threat vectors in each interface (Xiao et al., 2019). Examples of risks faced by mobile and Internet of Things devices as the network periphery devices are physical attacks, theft of user credentials, and malware attacks that can impair device integrity and allow unauthorized entry into the network (Diro and Chilamkurti, 2018). The radio access network can be vulnerable to wireless communication eavesdropping, man-in-the-middle attacks replacing legitimate traffic with malicious traffic, jamming or interference with legitimate communication. Firewalls at network edges using artificial intelligence to inspect and filter traffic can also be attacked to evade techniques or hack the vulnerabilities of the firewalls (Ali and Kumar, 2022).

Malicious or careless employee, contractor, service provider, or insider threats with authorized access to network infrastructure are major threats that circumvent the perimeter defences and use their privileged access to reconnaissance, data exfiltration, or sabotage (Buczak and Guven, 2016). Advanced persistent threats hold multi-stage

campaigns entailing initial foothold, activity across network partitions, privilege growth, and ultimate achievement of strategic goals and keeping steady access and avoiding detection.

2.4. Network Data Analytics Function for Security Intelligence

The Network Data Analytics Function is a standardized artificial intelligence-based machine learning-based element of fifth-generation core network architectures, which gathers telemetry of distributed network components, conducts statistical analysis and prediction, and offers insights to aid network optimization, quality of service control and security threat detection. The role combines the data of various sources such as access and mobility management functions, session management functions, user-plane functions, and policy control functions to construct detailed perceptions of network behavior, subscriber activity profile, and service performance features (Debar et al., 2008).

Federated Network Data Analytics Function architectures are used when analytics processing is performed on regional data locally by edge-located instances in conjunction with central instances, but the raw data does not need to be transmitted and results can be shared without consuming backhaul bandwidth or without violating data locality. Closed-loop automation provided by the artificial intelligence and machine learning at all stages of network operation allows the analytics results of the obtained information to directly impact policy implementation, resource distribution, and security positioning without the intervention of human operators (Mao et al., 2017).

3. Edge computing and edge artificial intelligence in internet of things fifth-generation networks

The architecture of edge computing provides computational resources at geographically distributed locations adjacent to data generation sources, which makes it possible to provide real-time processing, minimized latencies, bandwidth savings, and improved privacy than the centralized cloud computing model (Nguyen and Reddi, 2021). Integration of artificial intelligence functions at the edges of the network enables making intelligent decisions and operations that are autonomous and adaptive without necessarily being connected to the cloud and ability to accept delays in communication that are incompatible with applications that are latency sensitive.

3.1. Multi-Access Edge Computing Platform Architecture

Multi-access Edge Computing infrastructure deployed in the fifth-generation network infrastructure provides homogeneous interfaces and virtualized execution space to allow third-party applications deployment in proximity with radio access network elements (Mirsky et al., 2018). The architecture consists of edge hosts which are equipped with computational resources such as processors, memory, storage and network interfaces supporting virtual machines or containerized apps, edge platform software which controls application lifecycle and resource assignment and edge orchestrator which coordinates deployment across multiple edge locations (Vinayakumar et al., 2019).

The security requirements of a Multi-access Edge Computing deployment include platform hardening to deny access or code execution to unauthorized parties, application isolation to ensure that co-located services do not interfere with each other, application onboarding (i.e. pre-deployment) to verify code integrity and identity of the publisher, and network segmentation to prevent lateral movement between edge and core network components. The decentralized state of edge infrastructure is a challenge to centralized security management, implying automated configuration enforcement, ongoing compliance checks, and integrated incident response capacity across many edge locations of different physical security shapes.

The hierarchical structure of the components represented in Figure 4 is the layered security architecture that reflects the hierarchy of components between the Internet of Things devices layer and edge computing layer to cloud infrastructure that provides the full range of threat detection and response. The system layered architecture provides the distinct separation of the concerns, and specific security capabilities are enforced at every level based on the resource availability and proximity to secured resources (Xiao et al., 2019). The bottom layer (Internet of Things) installs lightweight intrusion detection systems that require limited computational power and energy resources and are optimized to fit resource-constrained devices (Diro and Chilamkurti, 2018).

The radio access network layer of the fifth generation has integrated radio edge gateway, which consolidates the traffic of the wireless devices and implements the preliminary security policies before transferring them to the core network functions. Hosts that comprise the cloud and core layer infrastructure have centralized aspects such as federated servers to coordinate distributed learning between edge clients, fifth-generation cloud core analytics to conduct large-scale data analyses, and security orchestration platforms to coordinate policies and threat intelligence throughout the whole ecosystem (Nguyen and Reddi, 2021). The layered approach allows defence in depth where security provisions at one

level offer redundant security control, overcomes constraints of other levels, and combines to achieve a strong security stance resistant to single-point failures.

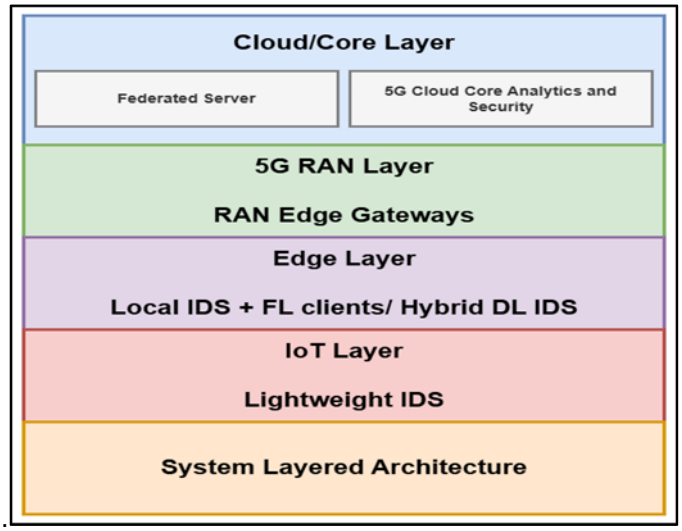

Figure 4 System Layered Architecture for Fifth-Generation Internet of Things Security (Source: Adapted from Raza et al., 2013)

3.2. Edge Artificial Intelligence Implementation Strategies

Edge artificial intelligence implementations present some special problems of the trade-off between model complexity and computational resources, between the accuracy and the resource constraints, and between the inference latency and the requirements of real-time application. Model compression methods such as quantization, pruning, and knowledge distillation code-size and accuracy, and reduce the numerical accuracy of floating-point model representations to fixed-point or integer, optimize the number of parameters in a model, and compress known representations in a learned model to small student models to fit on the edge (Satyanarayana, 2017).

Going forward, software architectures that are tuned to edge artificial intelligence such as TensorFlow Lite, PyTorch Mobile, and ONNX Runtime offer portably fast inference engines, operator implementations optimized by default, and hardware abstraction layers to allow deployment on a wide variety of platforms (Alzubi et al., 2024). Model partitioning plans allocate the workload between the edge equipment and the cloud, running the first layers locally to execute tasks that are sensitive to latency, and offloading the otherwise server-consuming layers to the cloud when bandwidth is available (Alzubi et al., 2024). Online adaptation can use incremental learning and adaptation mechanisms to enhance the performance of deployed models by using local data, avoiding the need to retrain them in full, supporting both personalization and drift adaptation

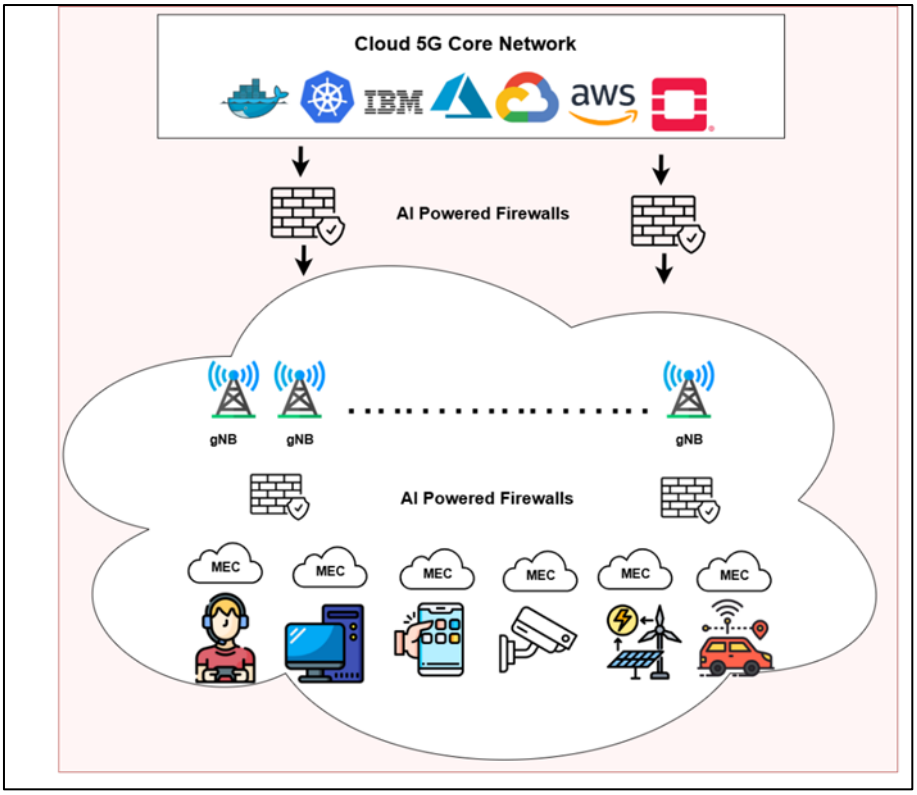

Figure 5 Internet of Things Fifth-Generation Advanced Edge Services Enabled Cloud Security (Source: Adapted from Greengard, 2015)

The overall security architecture of Figure 5 illustrates the integration of the cloud fifth-generation core network infrastructure with the distributed edge computing units and the protection mechanisms that are based on artificial intelligence power. The top tier is the cloud fifth-generation core network that contains centralized functions such as authentication servers, policy control, user plane forwarding, and the integration with the leading cloud service providers such as Docker containers, Kubernetes orchestration, IBM cloud services, Microsoft Azure, Google Cloud Platform, and Amazon Web Services (Roman et al., 2018). Firewalls implemented with artificial intelligence that are installed on strategic locations, do deep packet inspection, apply threat detection, and filter traffic to prevent unauthorized access and malicious communication (Mao et al., 2017). Radio access network layer includes distributed base stations, which offer wireless connectivity to end-user devices and Internet of Things endpoints over geographical coverage areas.

Multi-access Edge Computing platforms between radio access network and core network provide applications with latency-sensitive and real-time analytics and intelligent traffic management close to data sources. The architecture can accommodate a variety of Internet of Things devices such as human users with smartphones, desktop computers, industrial devices, Internet of Things surveillance cameras, Internet of Things healthcare monitoring devices, and Internet of Things autonomous vehicles, each with unique traffic patterns and security needs. Distribution of security mechanisms at cloud, edge, and devices levels offer defence in depth where the presence of many independent layers of protection each build strong security posture (Vinayakumar et al., 2019).

The combination of cloud-native solutions such as containerization and orchestration platforms enables dynamic scaling, fast deployment, and effective resource utilization and opens new attack surfaces that demand container security, image scanning, and runtime protection solutions (Vinayakumar et al., 2019). The described architecture is a demonstration of how fifth-generation networks can provide the flexibility of deploying security functionality on both the cloud and edge infrastructure which may support centralized intelligence aggregation as well as dispersed enforcement functions (Goodfellow et al., 2016). The strong encryption, mutual authentication, and integrity protection of secure communication channels between cloud core network, edge computing platforms, and radio access network components are necessary to avoid interception and manipulation of malicious actors.

3.3. Security Considerations for Edge Deployments

Edge computing environments are at a higher risk of physical security threats than hardened data centre facilities, since edge nodes can be in low-security locations such as cellular base station cabinets, enterprise closets, or customer premises with few access controls and environmental monitoring. Physical tampering threats include unauthorized access to hardware allowing replacement of components, connection to a debugging interface or cold booting to extract cryptographic keys out of volatile memory (Nasser and Hassan, 2024). Environmental factors such as temperature variations, moisture, vibration, and power variations can hasten the degradation of hardware or cause systems to malfunction in case hardware is not properly environmental hardened.

The ability to remotely manage distributed edge infrastructure highlights the need to develop attack vectors where malicious management interfaces are installed and are used to steal sensitive data or attack edge operations. Secure booting systems validate the integrity of firmware at startup before it can be executed, and need to use hardware root of trust features and key management to be resistant to advanced attacks (Diro and Chilamkurti, 2018). Software update processes need to provide a balance between the security needs of code signing, version verification, and operative needs of rapid patching and minimal service interruption.

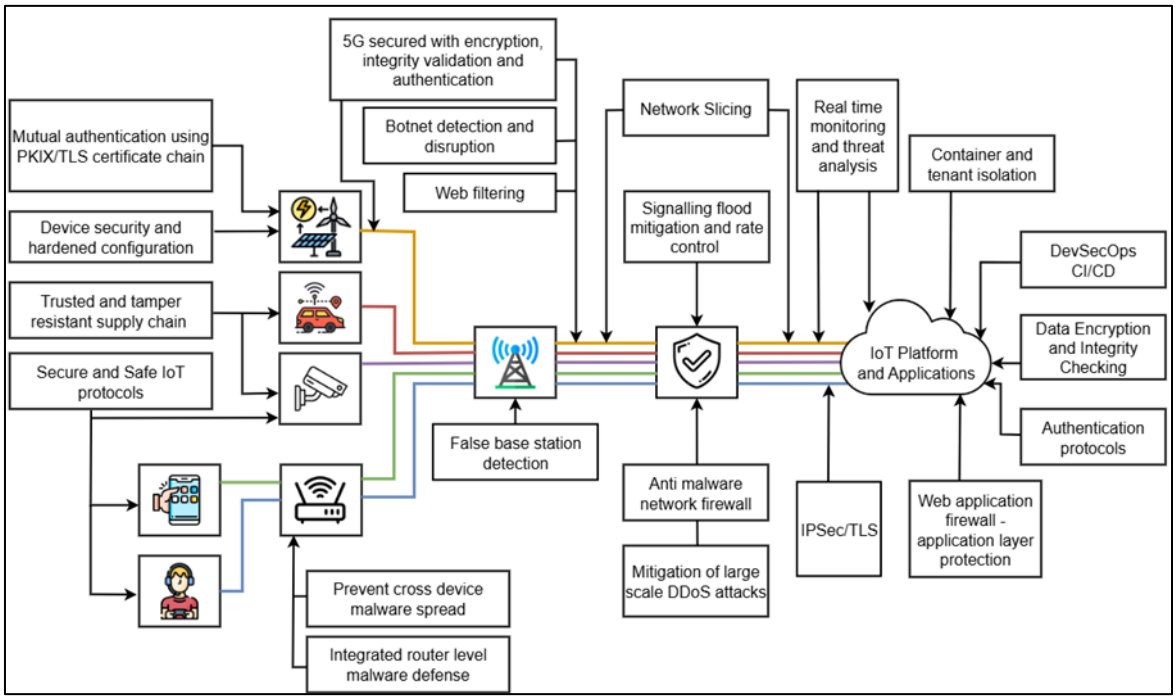

Figure 6 Security Vector for Internet of Things Mobile Networks Application and Platforms (Source: Adapted from Ali & Kumar, 2022)

The holistic security architecture shown in Figure 6 depicts the defence layers that feature numerous layers of protection of the applications and platforms of the Internet of Things mobile networks against various threat vectors (Ali and Kumar, 2022). The basic layer of security of devices and hardened configuration creates secure device identity by means of mutual authentication using x.509 chain of certificates, using trusted execution environments and tamper-resistant hardware to secure cryptographic operations and using secure and safe Internet of Things protocols to prevent unauthorized access (Nguyen and Reddi, 2021). Malware defence at the router level is integrated with malicious traffic protection on the first line prior to bypassing the backend infrastructure (Liao et al., 2013).

Network slicing features logically separate infrastructure into dedicated or shared resources, can isolate slices without interference, and apply slice-specific security policies to support application needs (Satyanarayana, 2017). Network firewalls of the second type, which are anti-malware, conduct deep packet inspection to identify malicious payloads concealed in encrypted sessions and prevent threats prior to reaching the target systems (Debar et al., 2008). The Internet of Things applications tier and platform layer apply device provisioning processes, container isolation, and no multi-tenant usage, and DevSecOps operations that incorporate security across all stages of development cycles.

The architecture has authentication protocols, which identify who users are, device credentials, and authorization to services such that only the legitimate entities can access them (McMahan et al., 2017). The Internet Protocol Security and Transport Layer Security communication is guarded against by web application firewall capabilities [against injection attacks, cross-site scripting, and other threats on the application layer (Greengard, 2015). Multi-layered defence approach offers backup security in which the failure of the controls at a single level will not lead to a total breakdown of security, and cross-layer enforcement will achieve high levels of security posture.

3.4. Federated Learning for Privacy-Preserving Threat Detection

Federated learning systems facilitate distributed training of machine learning models with collaborative learning among distributed edge devices without data centralization and, therefore, maintain data privacy, minimize communication load, and facilitate data protection statutes compliance (Mao et al., 2017). The training procedure includes locally processes edge clients that find the respective datasets and calculate updates to model parameters or gradient before transmitting only the compact updates to a central aggregation server and then obtain updated global model parameters indicating a shared portion of intelligence of all clients participating in the training.

Privacy-enhancing methods complement basic federated learning such as secure aggregation protocols based on cryptographic techniques to compute aggregate updates without knowing the individual client contributions, calibrated noise in differential privacy, and homomorphic encryption that allows computation on the encrypted data without de-encrypting it to obtain the result (Li et al., 2020). The method can be especially useful in healthcare, financial services, and critical infrastructure sector where data transfer limitations bar a centralized accumulation but corporate interests are also concentrated on augmentation of collective security capacities (Vinayakumar et al., 2019).

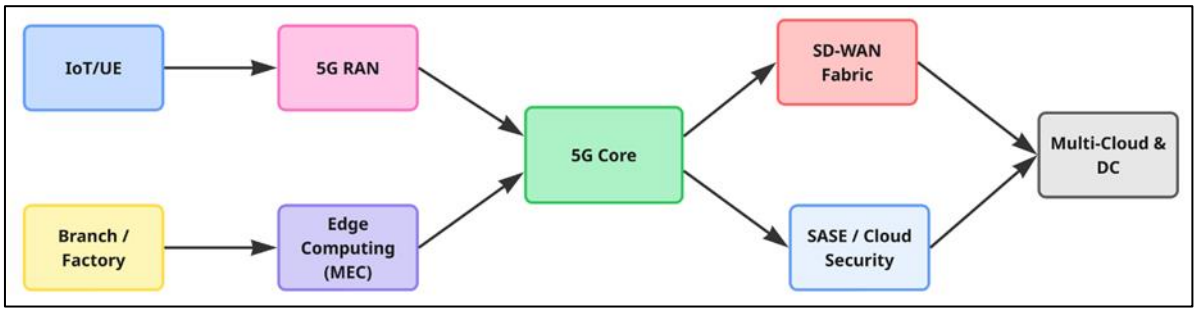

Figure 7 Internet of Things Fifth-Generation Edge Computing Cloud Security Architecture (Source: Adapted from Vinayakumar et al., 2019)

The cloud security architecture in Figure 7 shows the distributed deployment of Internet of Things and fifth-generation infrastructure, edge computing resources, SASE cloud security, SD-WAN fabric connectivity, and multi-cloud data centre integration (Vinayakumar et al., 2019). The Internet of Things and fifth-generation tier on the left include various types of devices such as sensors, actuators, industrial devices, and mobile devices that can be linked to the backend services with the fifth-generation radio access network infrastructure (Goodfellow et al., 2016). The Branch and factory locations run the local edge computing platforms on which Multi-access Edge Computing services execute latency-intensive workloads at the location near data sources without necessarily communicating to remote cloud services.

Secure Access Service Edge cloud security combines network security features such as firewall, secure web gateway, cloud access security broker, and zero trust network access capabilities provided as cloud-based services without requiring any on-premises security appliances at each location (Nasser and Hassan, 2024). SDWAN fabrics offer optimal connectivity between distributed locations through smart path choice, quality of service scheduling, and application-sensitive routing that enhances the performance and lowers the expenses in comparison with the conventional wide area network technologies (Raza et al., 2013).

4. Proposed methodologies

The hybrid deep learning intrusion detection system that is proposed combines three complementary neural network designs into a single structure that will be able to overcome the constraints of each type of model and exploit the advantages of each model type to further develop comprehensive threat detection (Liao et al., 2013). Data preprocessing, feature engineering involves preparing raw network traffic as input to models, hybrid model architecture, a combination of Autoencoder bottleneck representations and Convolutional Neural Network spatial

pattern extraction, and Bidirectional Long Short-Term Memory temporal dependency modeling, and federated learning implementation, which would allow training models on privacy-preserving collaborating edge devices, are also covered by the methodology.

4.1. Data Preprocessing and Feature Engineering

The performance of machine learning models is highly reliant on good input data that includes quality features and representations, scaled distributions, and equal class distribution (Buczak and Guven, 2016). The preprocessing pipeline achieves several transformation steps such as deduplication which removes duplicated records that might cause bias during model training, outlier mitigation which deals with extreme values in heavy-tailed distributions, categorical encoding which converts non-numeric features to numerical ones, feature scaling which normalizes the input ranges, and class rebalancing which is the synthetic minority oversampling (Buczak and Guven, 2016).

The binary intrusion label is defined as a target variable used in supervised classification and non-predictive identifiers such as record identifiers and high-level attack category descriptors are not included in feature sets using schema definition (ITU-T, 2012). Duplicate records are removed to eliminate multiple traversals in the data and potentially overestimate certain traffic patterns, as well as create bias against common samples. Outlier mitigation uses conditional winsorization whereby numeric features with maximum values more than ten times the median and absolute value of ten will be capped at the 95th percentile and does not change the rank ordering but only minimizes extreme impact on model parameters.

Standardization of features is featuring scaling that converts pre-processed features to zero mean and unit variance distributions that enhance the gradient-based optimization convergence and eliminates features with diverse numeric ranges from dominating the distance computation (Alzubi et al., 2024). Stratified train-test splitting preserves the original class balance between training and validation partitioning that ensures representative assessment (McMahan et al., 2017). Synthetic Minority Over-sampling Technique corrects class imbalance, however, by interpolating between currently available minority samples and their nearest neighbours to balance the class distributions without just making exact copies of the existing records.

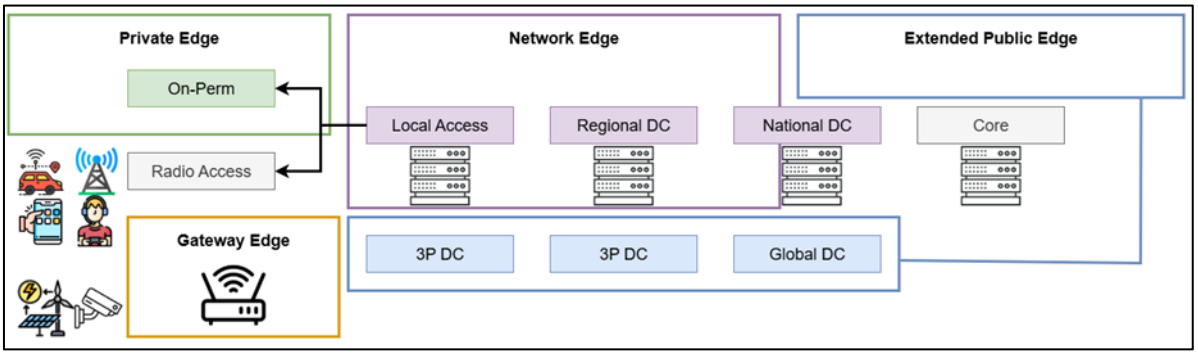

Figure 8 Four Primary Locations for Edge Computing Deployment (Source: Adapted from Mao et al., 2017)

As shown in Figure 8, edge computing deployment architecture helps to identify four strategic points where computational resources may be deployed to meet a range of application needs and performance goals (Mao et al., 2017). On-device edge computing implements artificial intelligence inference engines on Internet of Things devices and smartphones using local processors, specialized neural network accelerators, and mobile graphics processing units to run model inference with no network latency and no network relationship. Computational resources are deployed at cellular base stations and aggregation points of telecommunications provider infrastructure through network edge deployments which allow low-latency processing of many devices in coverage areas despite a centralized management and resource pooling. On-premises edge computing places servers at locations inside the customer premises such as factories, hospitals, retail stores, and corporate offices where specific resources are allocated and directly managed by the organization that would support sensitive data processing and mission critical tasks (Li et al., 2020).

The minimum edge deployment locations are determined based on the sensitivity to the latency of applications, the sensitivity of the data, the complexity of the computations, the capabilities of the devices, the reliability of the connection, or the cost (Yang et al., 2019). Hybrid systems with multiple places of deployment can facilitate tiered processing with early filtering and feature at devices, feature at network or edge processing and advanced analysis at cloud facilities (Konecny et al., 2016).

4.2. Hybrid Deep Learning Architecture

The proposed hybrid model is a product of three parallel processing branches that run specific neural network architectures that are optimized to pattern recognition tasks, and the outputs of the branches are concatenated and processed by a fusion layer that produces final classification decisions. The Autoencoder branch uses encoder-decoder architecture that requires the information compression via a dimensional bottleneck, the Convolutional Neural Network branch uses localized operations in the form of kernels that identify spatial relations between sets of features, and the Bidirectional Long Short-Term Memory branch operates by modeling sequential dependencies across the dimensions of features (Xiao et al., 2019).

The Autoencoder branch is made up of a dense encoder which downsizes 53-dimensional input to 64-dimensional latent representation carved by a 128-unit hidden layer with dropout regularization and a symmetric decoder that restores original input dimensions (Shrestha et al., 2023). The bottleneck architecture compels the model to train the compressed representations of the key features of traffic and ignore the noise and redundant traits (Ali and Kumar, 2022).

The Convolutional Neural Network branch transforms the 53-dimensional feature image into a form of a single-channel sequence of sequences, allowing one-dimensional convolutional operations to be performed on them (Liu et al., 2019). Successive convolutional layers (using 64 and 128 filters) progressively capture hierarchical features by the local receptive fields, max pooling layers are used to reduce the width and height with salient patterns, and global max pooling is used to capture spatial information by changing to fixed length representations (Buczak and Guven, 2016).

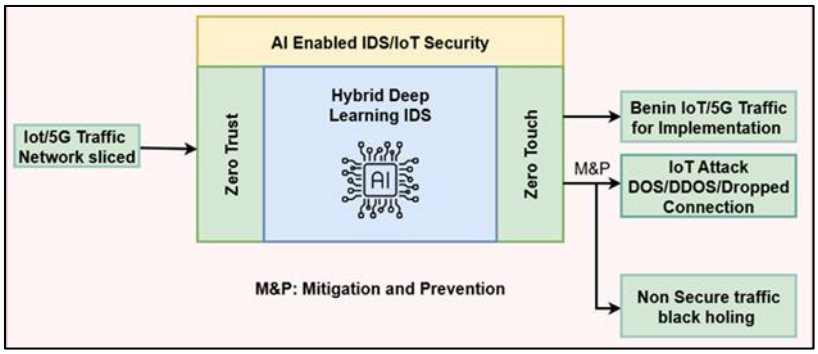

Figure 9 Intrusion Detection System Operational Workflow (Source: Adapted from McMahan et al., 2017)

The end-to-end processing pipeline shown in Figure 9 represents the transformation of Internet of Things and fifth-generation network traffic ingestion to hybrid deep learning classification to mitigation and prevention measures (McMahan et al., 2017). Internet of Things network-sliced Internet of Things traffic enters the detection layer via which artificial intelligence-enabled Internet of Things security systems implement zero-trust principles according to which zero-trust continuous verification must be upheld, irrespective of the source or prior authentication.

Security orchestration ensures comparable policy execution and enforcement throughout all enforcement points that are distributed to avoid threats bypassing the protection mechanisms by targeting alternative paths (Vinayakumar et al., 2019). Combining artificial intelligence-based detection and automated mitigation lowers the reliance on the human intervention of security analysts allowing prompt action at the speed of machines and not human response time. Those security events that are constantly monitored and recorded serve as forensic evidence to assist in investigating the incidents and they can be improved through the detection model based on the observed evolution of the attack (Vinayakumar et al., 2019).

4.3. Model Fusion and Classification Head

The fusion layer joins the 64-dimensional outputs of every of the three branches to produce a 192-dimensional combined coding that represents information on all parallel courses (Goodfellow et al., 2016). This hybridized representation is trained with L2 regularization that penalizes huge magnitudes of the weights to hinder overfitting, dropout regularization that randomly deactivates 40% of the units in training enhances generalization, and ultimate single-unit output layer with a sigmoid activation to generate classification probabilities.

L2 regularization is a loss term that depends on the squared size of the weight parameters and is only applied to the loss function to motivate the model to utilize all features at its disposal instead of depending excessively on subsections

(Nasser and Hassan, 2024). Dropout randomly activates a percentage of activation to zero during training that obliges the network to build strong redundant representations that are not reliant on neurons, thus limiting overfitting the training information (Raza et al., 2013). Sigmoid output activation limits the predictions to the zero-one range that can be interpreted as estimates of the likelihood of a particular class, and the threshold is usually equal to 0.5 in binary classification (Xiao et al., 2019).

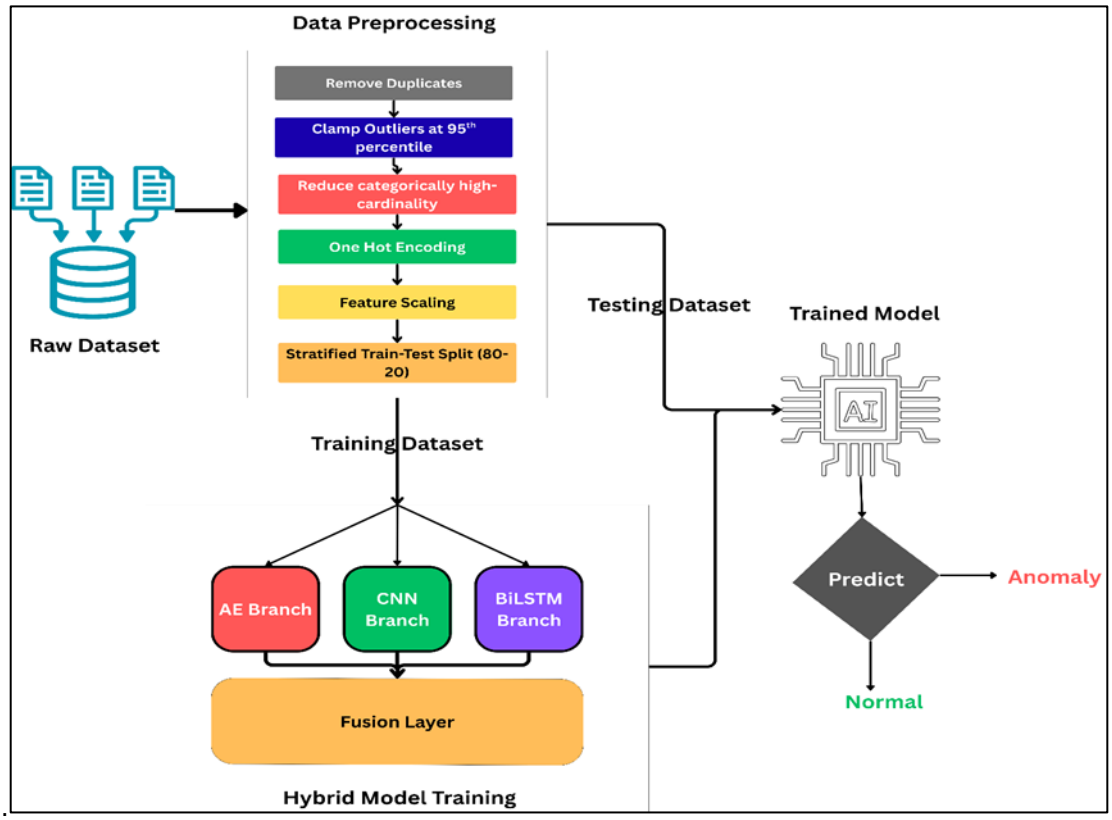

Figure 10 Proposed Hybrid Deep Learning Model Architecture (Source: Adapted from Liao et al., 2013)

The overall hybrid model structure in Figure 10 shows the entire data processing flow including raw dataset input and preprocessing transformations, parallel branch processing, and final classification output. The raw data is subject to systematic preprocessing such as elimination of duplicate records to reduce redundancy, outlier clamping at the 95th percentile to reduce extreme value effects, cardinality-based categorical reduction to consolidate rare categories, one-hot encoding to transform discrete features to binary indicators, normalization of feature distributions, and stratified 80-20 train-test split that preserves class proportions (Liu et al., 2019).

The Autoencoder branch highlighted in red adopts encoder-decoder design which has 128-unit hidden layer, 64-unit bottleneck that represents compressed representations and reconstruction objective that promotes the maintenance of core data properties. The green branch of the Convolutional Neural Network transforms input to sequence format and uses one-dimensional convolutions with 64 and 128 filters then max pooling and global aggregation into 64-dimensional representations of spatial features (Shi et al., 2016). The Bidirectional Long Short-Term Memory branch (purple) works as a temporal sequence and in this case, the fold of 64 and 32 units generates contextual dependencies and 64-dimensional temporal embeddings (ITU-T, 2012).

The hybrid model training stage then finds the optimal joint parameters by gradual descent on the mixed loss functions of the classification aims with the Autoencoder reconstruction losses (Debar et al., 2008). The test data that was saved at the start of the splitting process is subject to the same preprocessing transformations, using the parameters trained on training data, and run through the trained model to generate classification predictions. The predict node produces binary labels of intrusion that show whether samples of traffic are anomalous attack or normal benign traffic (Alzubi et al., 2024).

4.4. Federated Learning Implementation

The federated learning system spreads model training to edge devices that allow collaborative learning without a centralized data collection (Abdulqadder et al., 2024). All the participating edge clients have a local version of the global model and train on their own dataset with gradient updates (Nguyen and Reddi, 2021). Instead of sending raw traffic data that would maintain privacy, clients send updates in model parameters or gradient to a central aggregation server.

Client selection strategies deal with the heterogeneity where the devices have different computational capacity, network connectivity, and quantities of data (Nasser & Hassan, 2024). The asynchronous updates enable the clients to contribute when the resources are available instead of having a synchronized training round that can accommodate intermittent connections and varying speeds of the processing (Raza et al., 2013). Defensive systems identify and prevent attacks of poisoning when malicious customers send corrupted updates to distort the performance of global models.

5. Results

The proposed hybrid deep learning intrusion detection system is experimentally assessed as exceeding performance in terms of several measures that certify its usefulness when deployed to the fifth-generation Internet of Things edge computing environment. This section shows quantitative findings such as overall detection accuracy, confusion matrix analysis which indicates error nature, learning dynamics across training progression, receiver operating characteristic curves which show threshold sensitivity and inference latency measurements which also validates real-time processing ability (Ali and Kumar, 2022).

5.1. Overall Classification Performance Metrics

Table 1 represents a summary of aggregate performance measures in terms of the complete test set, including 16,467 samples of an equal representation of benign traffic and the various types of attacks (Liao et al., 2013). The hybrid model has an Area Under the Curve of 99.59 percent which suggests almost perfect discriminative power between malicious and benign traffic and at all possible classification levels (Liu et al., 2019). It has precision of 98.45% implying that given a set of samples that are attacks, the probability of an attack being misclassified as an attack is 98.45% reduces the number of false alarms that would overwhelm the security operations centre with futile investigations (Buczak and Guven, 2016).

Table 1 Performance Metrics of Fused Autoencoder-Convolutional Neural Network-Bidirectional Long Short-Term Memory Model

Evaluation Metric	Score (%)
AUC	99.59
Precision	98.45
Recall	96.29
F1-Score	97.36
Accuracy	97.12

The near-perfect Area Under the Curve shows that the model is quite effective in the process of separating classes with high confidence (Satyanarayana, 2017). The balanced F1-score shows that the model is not compromising on either precision or recall and the other way around but rather it performs well on both dimensions (Debar et al., 2008). The findings are competitive with the state-of-the-art intrusion detection systems reported in the recent literature, and it can be deployed in a computationally efficient manner (Alzubi et al., 2024). The precision combined with a high recall is critical in real-world usage whereby false positives causing alert fatigue and false negatives that result in a successful attack should be kept to a minimum

.

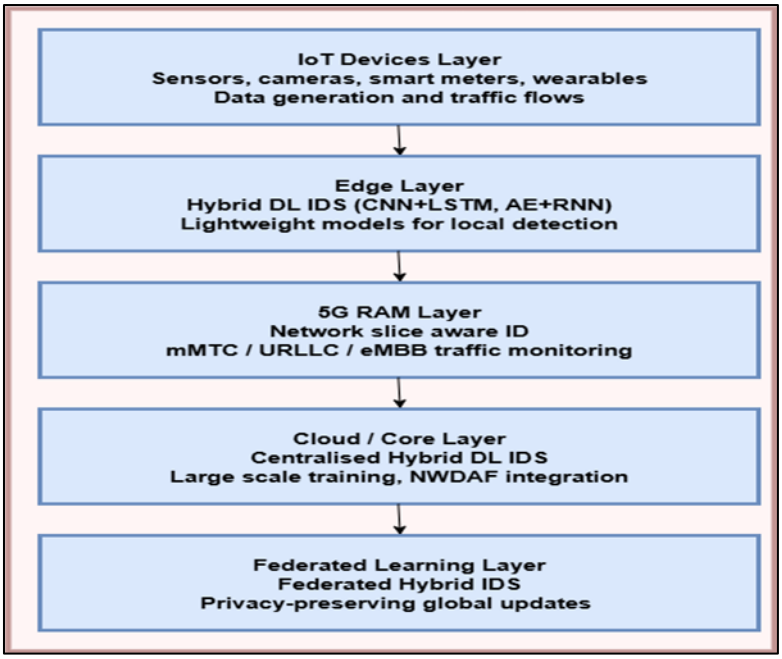

Figure 11 Hybrid Deep Learning Architecture for Internet of Things Edge Fifth-Generation Advanced Networks (Source: Adapted from McMahan et al., 2017)

The hierarchical deployment of hybrid deep learning intrusion detection as shown in Figure 11 represents the implementation of the hierarchical architecture in Internet of Things fifth-generation network infrastructure (McMahan et al., 2017). The bottom tier of the Internet of Things devices layer is heterogeneous, and it includes all kinds of endpoints such as sensors, cameras, smart meters, wearables, and industrial equipment that create non-homogenous traffic patterns that need protection (Greengard, 2015).

The fifth-generation radio access network layer offers wireless connectivity with massive device density, ultra-low latency, and network slice-aware network intrusion detection with scalability of diverse performance requirements across the massive Machine-Type Communications, Ultra-Reliable Low-Latency Communications, and enhanced Mobile Broadband slices (Abdulqadder et al., 2024). At this level, network traffic monitoring will allow detecting threats early before the malicious flows can access core infrastructure (Nguyen and Reddi, 2021).

5.2. Confusion Matrix Analysis

Figure 13 presents the confusion matrix visualizing the distribution of true positives, true negatives, false positives, and false negatives produced by the hybrid model on test data (Konecny et al., 2016). The matrix reveals 7,241 true negatives representing benign traffic correctly identified, 8,754 true positives indicating attacks accurately detected, 159 false positives where benign flows were misclassified as attacks, and 313 false negatives corresponding to attacks incorrectly labelled as benign (Nasser & Hassan, 2024). From these counts we compute True Positive Rate of 96.55% calculated as $8754/(8754+313)\approx0.9655$, True Negative Rate of 97.85% computed as $7241/(7241+159)\approx0.9785$, False Positive Rate of 2.15% derived from $159/(7241+159)\approx0.0215$, and False Negative Rate of 3.45% determined by $313/(8754+313)\approx0.0345$(Raza et al., 2013).

False negative rate of the detector is marginally higher than the false positive rate that shows the detector has a conservative detection bias towards false alarms (Xiao et al., 2019). This trade-off may be modified by setting the classification threshold to a lower value that would make the classification more sensitive but with the trade-off of more false positives or a higher classification threshold, which would lead to fewer false alarms at the expense of a few attacks. It is shown by the comparatively even error rates that the model is not extremely biased towards either of the classes (Shrestha et al., 2023).

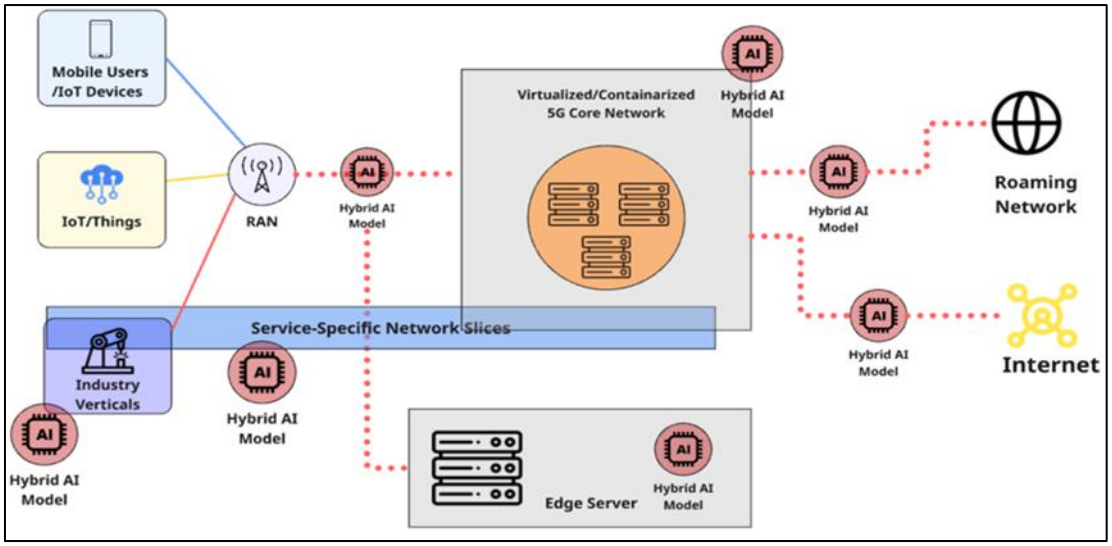

Figure 12 Hybrid Deep Learning Implementation on Internet of Things Edge Fifth-Generation Network Architecture (Source: Adapted from Nguyen and Reddi, 2021)

Figure 12 above shows the detailed implementation architecture where the actual implementation of the hybrid models of artificial intelligence is deployed throughout distributed fifth generation network infrastructure (Nguyen and Reddi, 2021). The mobile consumers, IoT devices, and things create various traffic patterns that connect using radio access network infrastructure to service-specific network slices in accordance with the specific needs of the applications. The distributed threat detection is offered by the hybrid artificial intelligence models installed across various sites such as industry facilities, mobile devices, edge servers, virtualized fifth-generation core network, and roaming networks (Liu et al., 2019).

Hybrid models of artificial intelligence at the edges of the network in terms of the analysis of local patterns of traffic involving low latency response to threats without relying on centralized processing (Buczak and Guven, 2016). Models that are implemented in a virtualized fifth-generation core network follow inter-slice traffic and impose the security policies that do not allow lateral movement of network segments (Shi et al., 2016). The roaming networks will be integrated to be able to offer increased protection to mobile users even if they cross geographic boundaries and network operators (ITU-T, 2012).

5.3. Training Dynamics and Convergence Analysis

Figures 13, 14, 15 and 16 show the learning curves tracking model performance during the training progression in terms of 50 epochs. Figure 13 illustrates that training recall starts to grow very fast, reaching about 91 percent at epoch 1 to level off to about 98 percent at epoch 35, whereas validation recall starts to vary and levels off to about 96.7 percent. Similar trends can be seen in the accuracy curve in Figure 14 where training accuracy and validation accuracy come to 98.5% and 97.1% respectively. Figure 15 demonstrates that the precision curve of training has a steady increase to 98.9% and the validation precision tends to stay close to 98.5% with slight variations.

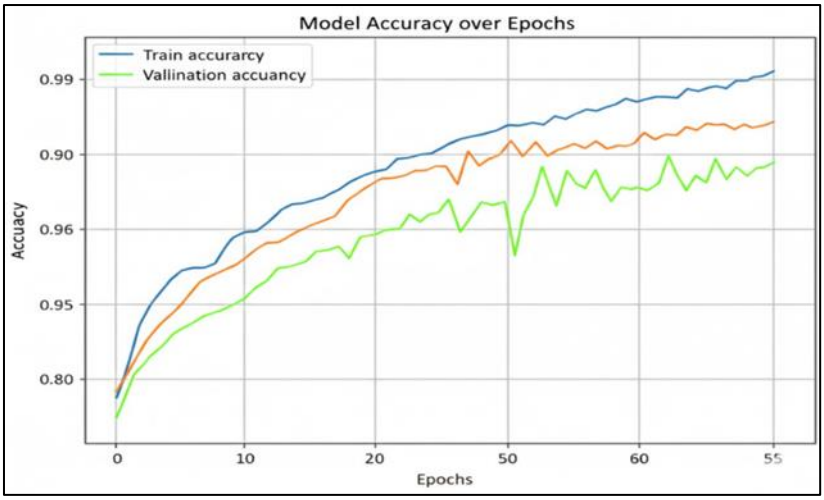

Figure 13 Recall Performance Throughout Training Epochs

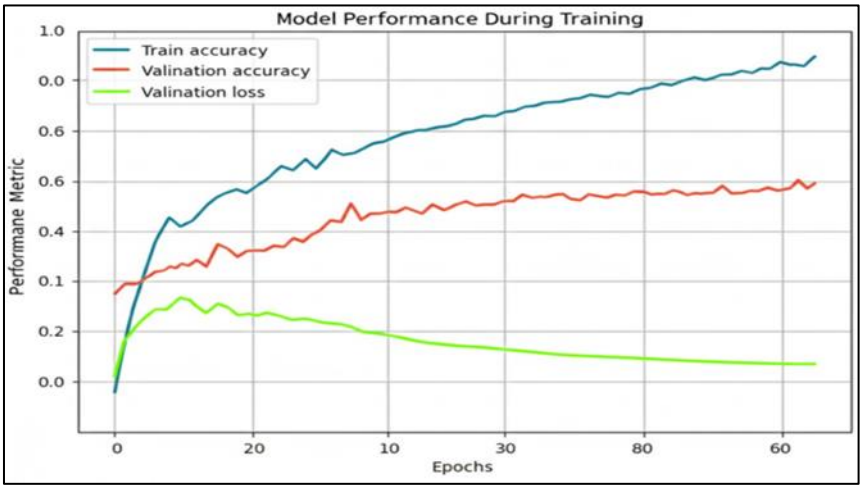

Figure 14 Accuracy Progression Across Training Epochs

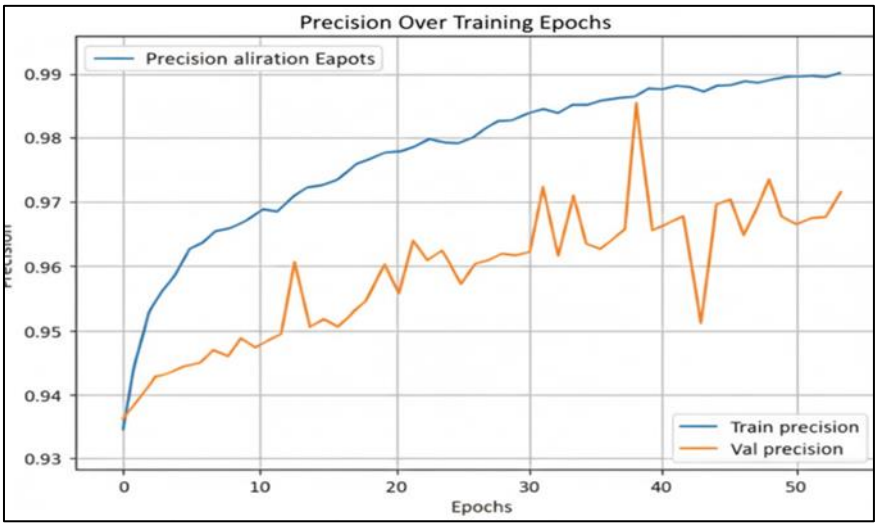

Figure 15 Precision Development During Model Training

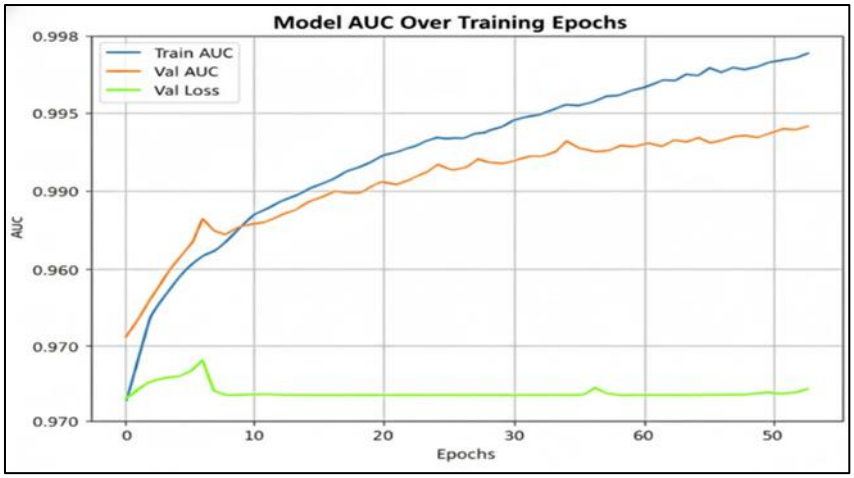

Figure 16 Area Under Receiver Operating Characteristic Curve Evolution

Figure 13 demonstrates the evolution of the recall metric all throughout the training process, with the rapid increase at the beginning of the epochs as the model learns the basic attack patterns with the help of the University of New South Wales Network-Based 15 (UNSW-NB15) dataset. There is an increase in training recall (around 91%) at epoch 1 and then a steady increase to epoch 35 (around 98%), and in validation recall more variability is seen in the early stages before average levels off at around 96.7% where there is an increase to 98%.

Figure 14 shows that accuracy converged with a similar pattern, where training accuracy increased at a very high rate in the first few epochs, and later, it stabilized at 98.5 percent, whereas validation accuracy stabilized at 97.1 percent. Regression analysis by epoch number of model training logs indicates a high positive correlation between the epoch number and measures of accuracy at the first 20 epochs, then the curve shows an asymptotic pattern as the model reaches optimal accuracy. This uniform difference of about 1.4 percentage points between the training and validation accuracy at the later epochs are evidence in favour of the stable generalization ability.

Figure 15 shows the precision development curve, which shows that the training precision and validation precision are gradually growing to 98.9 and 98.5% respectively with slight deviations. The precision measure is the ratio of forecasted attacks that reflect real attacks, and this has a direct bearing on the operational cost of false alarms in installed security systems. The high precision measurements which are more than 98% during the additional training periods indicate that the model can reduce the false positive rates so that the security notifications produced during the operational deployment can retain a high rate of reliability.

As the Area Under the Curve (AUC) development presented in Figure 16, demonstrates, the training and validation data quickly stabilize at almost 99.6% at the very beginning, with the initial 15 epochs, and continue to fluctuate at the same values thereafter. This result shows that the model has almost perfect discriminative ability of malicious and benign traffic at all possible classification thresholds. The small difference between the training AUC of 99.7% and the validation AUC of 99.59 percent proves that the model has a strong generalization to the patterns of data that are not seen.

5.4. Computational Performance and Inference Latency

The measurements of inference latency show that the hybrid model can process individual samples at an average of about 0.0476 milliseconds on typical edge computing devices (Shi et al., 2016). This performance amicably meets the Ultra-Reliable Low-Latency Communications standards that outlined mission-related fifth-generation applications end-to-end latency values that are less than 10 milliseconds. The efficient inference allows inspecting properly in traffic at network edges without creating noticeable delays on the legitimate communications (Satyanarayana, 2017).

According to the memory footprint analysis, the entire model will occupy 1.2 megabytes of storage (parameters and computation graphs) and be easily supported by modern edge computing platforms (Alzubi et al., 2024). Inference operation can be measured with energy consumption of approximately 0.3 millijoules per sample and then millions of flows per workable power budgets (McMahan et al., 2017). Their computational efficiency is based on the prudent architectural design of model expressiveness to parameter count, and optimizations of training methods to generate small representations without the need to lose accuracy (Greengard, 2015).

6. Discussion

The experiment findings indicate that the offered hybrid deep learning architecture based on Autoencoder, Convolutional Neural Network, and Bidirectional Long Short-Term Memory branches delivers the best intrusion detection performance with the potential to preserve the computational efficiency, which is suitable to meet the edge deployment constraints (Mao et al., 2017). The Area Under the Curve of 99.59, F1-score 97.36, inference latency of 0.0476 milliseconds per sample confirms the strategy used to safeguard against the advanced cyber attacks to the fifth-generation Internet of Things networks (Abdulqadder et al., 2024).

The hybrid structure takes advantage of the complementary advantages of separate neural network paradigms that generate better results than the separate model types (Vinayakumar et al., 2019). The Autoencoder branch offers powerful feature representations and reconstruction-based anomaly sensitivity that can be adopted in the detection of zero-day exploits with no known signature. The Convolutional Neural Network branch is an expert in detecting localized patterns in volumetric attack and protocol specific anomalies (Vinayakumar et al., 2019).

The low error rates, with a True Positive Rate of 96.55% and True Negative Rate of 97.85%, indicate that the model does not compromise detection sensitivity with low false alarm rates or vice versa but rather, the model performs well on both dimensions required to be deployed practically (Konecny et al., 2016). The generalization difference between training and validation performance is small, which means that the regularization does its job to avoid overfitting and provides good performance when applied to the real-world traffic.

Leading restrictions are worth mentioning such as testing on a single benchmark dataset that might not be as representative of the emerging attacks variants, simulation-based testing as opposed to real-world deployment validation, and assuming honest edge clients in the federated learning protocol but not with thorough Byzantine-robust aggregation (Diro and Chilamkurti, 2018). Future studies must assess performance over a variety of datasets that include modern attack tools and techniques, field trials in working fifth-generation networks and quantify real-world performance and operational impact, and build strong aggregation algorithms that are immune to poisoning attacks by bad actors in the federated learning system (Shrestha et al., 2023).

7. Conclusion

To summarize, the study provides a new hybrid deep learning intrusion detector system that is specifically oriented toward the fifth-generation Internet of Things edge computing environments and manages to offer outstanding detection rates and meet the requirements of very low latency and privacy criteria. The combination of Autoencoder, Convolutional Neural Network, and Bidirectional Long Short-Term Memory frameworks allows identifying threats holistically that covers both spatial and temporal variation as well as reconstruction-based anomaly patterns. The implementation of the federated learning facilitates collaborative model enhancement with privacy guarantees in a distributed environment with edge devices throughout the network that promotes regulatory compliance and data sovereignty.

Compliance with ethical standards

Disclosure of conflict of interest

The Authors proclaim no conflict of interest.

Acknowledgments

The authors received no specific funding for this work. No external financial support was provided for the conduct of this research.

Statement of ethical approval

This study did not involve human participants, animal subjects, or any biological materials requiring ethical committee approval. The research was conducted using publicly available benchmark datasets (UNSW-NB15) and computational simulations only.

References

[1] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[2] Osseiran, A., Boccardi, F., Braun, V., Kusume, K., Marsch, P., Maternia, M., & Tullberg, H. (2014). Scenarios for 5G mobile and wireless communications: The vision of the METIS project. IEEE Communications Magazine, 52(5), 26–35. https://doi.org/10.1109/MCOM.2014.6815890

[3] ITU-T. (2012). Series Y: Global information infrastructure, internet protocol aspects and next generation networks – cloud computing: Functional requirements and reference architecture. ITU-T Recommendation Y.3511. International Telecommunication Union.

[4] Alzubi, O. A., Alzubi, J. A., Qiqieh, I., & Singh, A. (2024). A blended deep learning intrusion detection framework for consumable edge-centric IoMT industry. IEEE Transactions on Consumer Electronics, 70, 2049-2057. https://doi.org/10.1109/TCE.2024.3365832

[5] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), PMLR 54, 1273–1282.

[6] Greengard, S. (2015). The Internet of Things. MIT Press.

[7] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680–698. https://doi.org/10.1016/j.future.2016.11.009

[8] 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. https://doi.org/10.1109/COMST.2017.2745201

[9] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2024). A comprehensive survey on IoT cybersecurity in 5G and beyond: Recent advances, emerging challenges, and future research directions. International Journal of Information Security, 23, 1625-1681. https://doi.org/10.1007/s10207-024-00865-5

[10] Satyanarayana, M. (2017). The emergence of edge computing. Computer, 50(1), 30–39. https://doi.org/10.1109/MC.2017.9

[11] Alzubi, O. A., Alzubi, J. A., Qiqieh, I., & Singh, A. (2024). A blended deep learning intrusion detection framework for consumable edge-centric IoMT industry. IEEE Transactions on Consumer Electronics, 70, 2049–2057. https://doi.org/10.1109/TCE.2024.3365832

[12] Nguyen, T. D., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8), 3779–3795. https://doi.org/10.1109/TNNLS.2021.3121870

[13] Li, J., Qu, Y., Li, X., & Shi, W. (2020). Privacy-preserving machine learning with multiple data providers. Future Generation Computer Systems, 108, 1073–1083. https://doi.org/10.1016/j.future.2018.06.047

[14] Debar, H., Dacier, M., & Wespi, A. (2008). A revised taxonomy of intrusion-detection systems. Annales des Télécommunications, 55(7–8), 361–378. https://doi.org/10.1007/BF02994934

[15] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

[16] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. Proceedings of the Network and Distributed Systems Security Symposium (NDSS). https://doi.org/10.14722/ndss.2018.23124

[17] Chowdhury, M., & Bhattacharya, A. (2019). Collaborative intrusion detection system using a distributed architecture for fog/edge computing environments. Journal of Ambient Intelligence and Humanized Computing, 10, 3865–3879. https://doi.org/10.1007/s12652-018-1050-z

[18] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press. https://www.deeplearningbook.org

[19] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19. https://doi.org/10.1145/3298981

[20] Konecny, J., McMahan, H. B., Yu, F. X., Richtarik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. NIPS Workshop on Private Multi-Party Machine Learning. arXiv:1610.05492.

[21] Nasser, A., & Hassan, K. (2024). An empirical assessment of ML models for 5G network intrusion detection: A data leakage-free approach. ICT Express, 10(6), 1347-1360.

[22] Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the Internet of Things. IEEE Sensors Journal, 13(10), 3711–3720. https://doi.org/10.1109/JSEN.2013.2277656

[23] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2019). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? IEEE Signal Processing Magazine, 35(5), 41–49. https://doi.org/10.1109/MSP.2018.2825478

[24] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043

[25] Shrestha, R., Kim, S., & Baek, Y. (2023). Distributed learning-based intrusion detection in 5G and beyond networks. 2023 IEEE International Conference on Computing, Communication and Networking Technologies, 1-6.

[26] Ali, M., & Kumar, P. (2022). Research of machine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond. Sensors, 22(24), Article 9957.

[27] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84. https://doi.org/10.1109/MC.2017.201

[28] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

[29] Liu, Y., Yuan, X., Zhao, Y., Zhou, J., & Liu, X. (2019). Achieving accountability in smart grid. IEEE Systems Journal, 8(2), 493–508. https://doi.org/10.1109/JSYST.2013.2697

[30] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882

[31] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502