5G Network Intrusion Detection Method Based on Robust Federated Optimization

Changjie Wang[1,*]
[1]Department of Network Security, Henan Police College, Zhengzhou 450046, HeNan, China
Corresponding author: Changjie Wang (e-mail: wcj6931@126.com).

ABSTRACT High-speed, low-latency and massive connectivity have emerged as a result of the rapid development of 5G networks, but so have security threats. Current intrusion detection tools are poorly adapted to the distributed, heterogeneous, and dynamic 5G environment where a flood of real-time information is generated over a spectrum of devices at the edges and network layers. Federated learning has been suggested in response to these threats as a new paradigm to aid in the training of intrusion detection systems without having to aggregate the information. This review provides a detailed study of intrusion detection systems in 5G networks that are federated learning-based, and how the federated learning-based intrusion detection systems can address the challenges mentioned above. The paper will also entail the discussion of the basic ideas and principles of federated learning, the importance of robust federated optimization techniques to enhance the robustness of models, and architectural design of distributed intrusion detection systems. Moreover, accuracy, efficiency, and resilience to adversarial attacks are also used as indicators of performance, which emphasizes the potential and strength of federated learning when used in complex network conditions. The key challenges and the difficulties, including the heterogeneity, communication, and security, are also discussed and analyzed. Lastly, the new trends and possible directions of research, such as the combination of AI explanations, adaptive learning, and federated learning with other emerging technologies, such as edge computing and blockchain, are also presented. In general, the paper provides a detailed and extensive perspective on the design and development of scalable and privacy-conserving and smart intrusion detection mechanisms on next-generation 5G networks.

INDEX TERMS 5G Networks, Intrusion Detection Systems (IDS), Federated Learning, Network Security, Privacy-Preserving Learning, Robust Federated Optimization, Edge Computing, Non-IID Data, Adversarial Attacks, Explainable Artificial Intelligence (XAI), Distributed Machine Learning, Cybersecurity in 5G

I. INTRODUCTION

The accelerated development of the fifth-generation (5G) communication technologies, the geometric increase of the Internet of Things (IoT) devices and cloud-based services have already altered the contemporary digital ecosystems considerably (Altowaijri and Ayari, 2025). The developments promise ultra-high data rates, low latency and massive connectivity, and support applications like smart cities, autonomous systems and real-time analytics. However, the growing size, heterogeneity, and complexity of 5G networks have made network infrastructures more vulnerable to a wide spectrum of advanced cyber threats including distributed denial-of-service (DDoS) attacks, data breaches, and advanced persistent threats (Rasheed and Alam, 2024).

IDS are indeed valuable, in the maintenance of network security. They monitor what is occurring on the network discover things that do not appear right and inform us when someone is possibly attempting to assault us. The traditional method of operating the Intrusion Detection Systems whereby all the operations are centrally managed and we apply hard-coded rules to determine what is bad is not effective in 5G environments.

There is plenty of data in 5G environments we are looking at to say that the network is distributed throughout the space and nothing ever stays the same. This renders it difficult to maintain the old Intrusion Detection Systems and keep them functioning properly. To remain safe in 5G environments Intrusion Detection Systems must be capable of handling large amounts of data and adapt rapidly (Serôdio et al., 2023).

Intrusion detection systems (IDS) are increasingly using machine learning (ML) and deep learning (DL) methods

to overcome these challenges. These methods are able to automatically discover complex and nonlinear patterns in large network data, and identify anomalies and novel forms of attacks. Centralized ML-based methods, despite their benefits, pose serious issues associated with data privacy, communication overhead, and the necessity to centralize sensitive data at the point of aggregation that is in most cases unfeasible and dangerous in distributed 5G settings.

Federated Learning (FL) has become one of the most promising solutions to those problems because it allows decentralized training of models on multiple devices or edge nodes without any need to exchange raw data. This privacy-saving paradigm enables joint learning on distributed data without loss of the confidentiality of the data. Federated learning in the context of 5G networks can be applied to create intelligent intrusion detection systems, which can use a variety of data sources among network elements and IoT devices to enhance detection accuracy and generalization (Rashid et al., 2023).

Nevertheless, federated learning in intrusion detection is not implemented with ease. The heterogeneity of 5G environments and the distribution of data variability and untrustworthy or malicious participants may negatively impact the quality of models (Blika et al., 2024). Also, federated systems are susceptible to adversarial attacks, including data poisoning and model manipulation, that can affect the integrity of the learning process and decrease the quality of intrusion detection.

Federated learning-based intrusion detection systems have been proposed to be supported by robust federated optimization methods to improve the reliability and robustness of the systems. The objectives of such methods are to enhance model resilience to noisy, biased or adversarial data and provide efficient convergence and scalability. Robust federated optimization, with mechanisms of secure aggregation, anomaly-resistant training and adaptive learning, can offer a promising avenue to the development of trustworthy and high-performance intrusion detection solutions in dynamic 5G networks (Su, 2024).

This review brings out an extensive discussion of intelligent intrusion detection techniques in 5G networks with specific emphasis on effective federated optimization techniques. It reviews contemporary developments, outlines major issues, and points out further research opportunities to introduce secure, scalable, and privacy-compliant intrusion detection in the next-generation communication systems as shown in Figure 1.

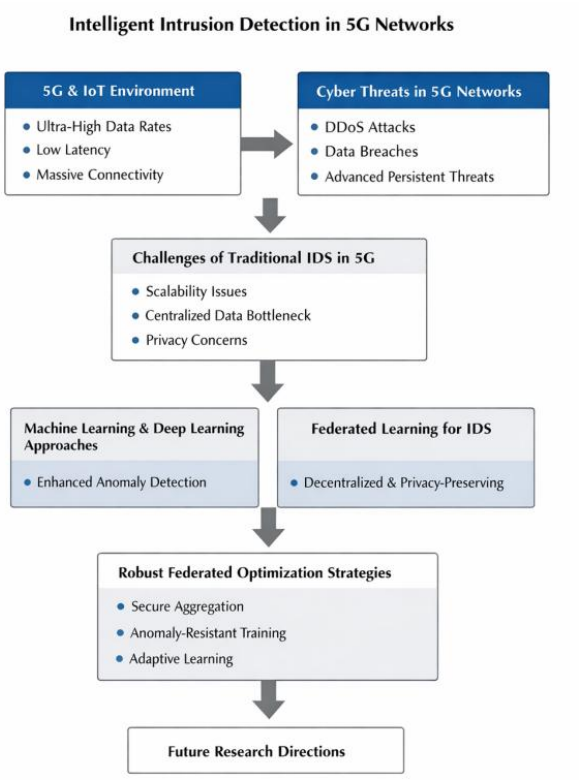

Fig. 1. Intelligent Intrusion Detection in 5G Networks: A flowchart of how IDS challenges in the past have evolved to be more intelligent with machine learning, federated learning, and robust optimization techniques to achieve better network security.

II. BACKGROUND ON 5G NETWORKS

The fifth-generation (5G) mobile communication paradigm is an important innovation in the network architecture, providing ultra-low latency, massive machine type communication (mMTC), and ultra reliable low latency communication (URLLC), in addition to mobile broadband (eMBB) enhancement(Jain, 2025). Such applications can include transformative applications like autonomous vehicles, distant surgery, immersive AR/VR, and large scale industrial IoT implementations. It has been observed that globally 5G subscriptions are increasing at a high pace and it is estimated that the subscriptions are going to surpass billions in the next few years, a situation that indicates the large number of subscriptions being introduced in commercial and critical infrastructures. As a result, security concerns have taken a more prominent role in 5G research and deployment (Cook et al., 2023).

Although it has its benefits, the 5G architectural innovations such as network slicing, software defined networking (SDN) and network function virtualization (NFV) present distinct security vulnerabilities and considerably increase the attack surface. In contrast to legacy cell systems, 5G spreads both control and data plane tasks on distributed cloud native environments, rendering them vulnerable to advanced threats, including control plane attacks, API abuse, and slice based exploitation (Theodoropoulos et al., 2023). The implementation of SDN also complicates the conventional security postures with decoupling network logic and hardware, and posing a threat to the conventional intrusion detection mechanisms.

These challenges are enhanced by the ubiquity of 5G connectivity, especially in the industrial and IoT markets. As the number of tens of billions of IoT devices interconnected around the globe is projected to grow in the near future, 5G

networks will be required to support exponentially larger amounts of heterogeneous traffic. Such an upsurge increases susceptibility to distributed denial of service (DDoS), eavesdropping, and subsequent lateral movement attacks that require real time and adaptive intrusion detection systems (Wang et al., 2025).

Traditional intrusion detection systems (IDS) are not very scalable to dynamic 5G settings because of their fixed signature based models and low adaptability. The urgent necessity is to adjust IDS structures to the next generation network designs, and evaluate the relevance of features in SDN control space. The heterogeneity and high throughput of 5G traffic require anomaly based detection mechanisms that are capable of analyzing complexing temporal patterns, detecting new threats and working with low false alarms (Rahman et al., 2022).

In order to address these needs, extensive research has aimed at incorporating machine learning (ML) and deep learning (DL) into intrusion detection systems. These techniques use the modern pattern recognition to identify unknown and adaptive threats that the traditional signature based systems cannot identify. Federated learning based on edge AI is one of those methods that promise to become a viable paradigm in the future, allowing joint model learning on decentralized clients without the sharing of raw data hence improving privacy and scaling anomaly detection in 5G enabled IoT ecosystems (Duan et al., 2023).

On device inference On device inference Deep learning models Lightweight models like autoencoders and long short term memory (LSTM) networks have proven effective in threat detection in real time. Autoencoders have been shown to be especially effective in the latent representation of normal network behavior, which in turn allows robust detection of anomalies in high velocity 5G traffic. The time series network data that 5G delivers can be effectively handled by LSTM networks due to their ability to capture sequential and time series dependencies an essential requirement considering the high throughput and the variety of services that 5G can provide (Baz et al., 2024).

In addition to recurrent architectures, Transformer based models with multi head self attention mechanisms have also recently achieved state of the art performance on global temporal dynamics of heterogeneous network traffic. Such models are always more effective than conventional convolutional architecture in identifying complex time-dependent patterns among network slices, which allows more precise and scalable intrusion detection in multi-tenant 5G settings (Fernando, 2024).

III. CHALLENGES IN 5G INTRUSION DETECTION SYSTEMS (IDS)

The emergence of 5G networks represents a transformative step in telecommunications, introducing ultra-low latency, massive device connectivity, network slicing, and highly virtualized architectures such as Open Radio Access Networks (Nuriev et al., 2024). Although these innovations make a wide range of applications possible, including autonomous vehicles and industrial IoT, they also pose new challenges to intrusion detection systems on an unprecedented scale. The decentralized, diverse, and dynamic property of 5G ecosystems creates massive amounts of real-time traffic of mobile users, IoT devices, and edge computing nodes, rendering traditional centralized or signature-based IDS frameworks ineffective in detecting threats in time. Network slicing and virtualized network functions increase the attack surface, which doesn't limit the attack but provides several points of vulnerability where more advanced cyberattack can spread through layers without being readily detected. Artificial intelligence and deep learning integration in IDS boosts its detection ability but presents other security threats, such as adversarial attacks, model poisoning, and the challenge of maintaining robustness and interpretability in complex artificial intelligence models (Alotaibi and Rassam, 2023). Another important obstacle is the computational complexity, with resource-intensive models (especially generative and deep neural networks) having difficulties with efficient operation in real-time, and requiring an invention in model compression, pruning, and hardware acceleration. Moreover, the lack of annotated data on a variety of 5G applications does not allow training generalized models, and the disparate performance of devices between high-performance smartphones and low-performance IoT sensors makes it difficult to implement homogenous detection policies (Ahad et al., 2026). The issues of privacy also limit the data sharing, which makes the idea of centralized training methods difficult, and the unstable network conditions at the edge make the possibility of detecting all data incomplete or delayed. All these contribute to a challenge in ensuring high detection rates, low false-positive rates, and low response time, which is essential to ensure the quality of service and reduce packet loss in 5G applications. Consequently, the demand is high to find intrusion detection solutions that are not merely adaptive, scalable, and privacy-sensitive but are also capable of confronting high traffic, in real-time, and in large volumes without collapsing under the pressure of advanced and emerging cyber threats. These difficulties demonstrate the need to carry out studies on distributed, intelligent, and strong IDS architectures capable of functioning within the multifaceted 5G ecosystem (Alam et al., 2026) as shown in Figure 2.

IV. FUNDAMENTALS OF FEDERATED LEARNING IN NETWORK SECURITY

Federated learning has become a revolutionary framework of overcoming the shortcomings of traditional intrusion detection tools, especially when it comes to distributed and privacy-aware 5G networks (Rezaei et al., 2025). In contrast to centralized learning, federated learning allows multiple devices or edge nodes to jointly train machine learning models without having to transfer raw data to a central repository. The individual nodes have their own local dataset and train a model separately, and only send model updates

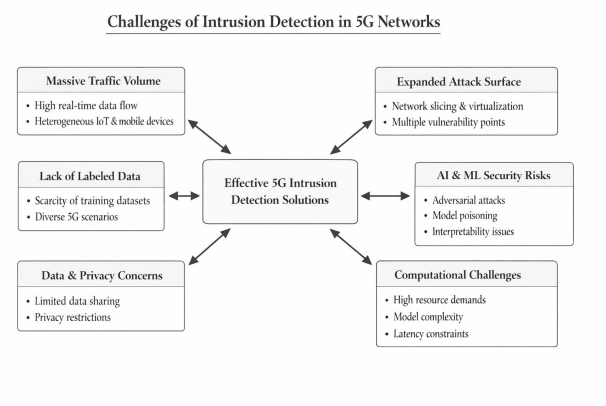

Fig. 2. Intrusion Detection challenges in 5G Networks: A flow chart identifying major challenges that include the volume of traffic, expanded attack surfaces, AI/ML security risk and data privacy issues all boiling down to the fact that effective and adaptable intrusion detection solutions are required in 5G environments.

or gradients to a central aggregator to build a global modeL (Fang et al., 2023).

This decentralized model maintains privacy of data, lessens overhead communication and taps the diversity of traffic patterns and operational information among distributed network elements to allow intrusion detection systems to generalize better and identify a previously unknown threat. Federated learning minimizes the latency by processing data nearer to its origin, and thus is ideal in real-time detection in high-speed 5G networks (Liu et al., 2024). Moreover, the paradigm enables models to dynamically change with changing attack vectors and non-identically distributed and non-uniform (non-IID) data, increasing resilience to advanced cyber threats and reducing the risk of data disclosure and adversarial examples.

In addition to privacy, federated learning also solves more practical problems with traditional centralized systems such as computational limits on resource-constrained edge devices, dynamic network topologies, and fault tolerance. Nonetheless, federated learning brings with it a different set of complications. The heterogeneity of data about clients and computational resources may result in incompatibility of local model updates, whereas it is essential to uphold the security of local model updates in aggregation to avoid inference attacks or model poisoning (Nabavirazavi et al., 2023). The training efficiency, participation encouragement, and integrity of the global model requires efficient aggregation mechanism, adaptive weighting of client contribution, and incentive structure. Along with these obstacles, federated learning provides a powerful structure of intrusion detection, allowing the privacy preserving, scalable, and adaptive security solutions to work efficiently in the complex, dynamic, and high-volume 5G networks. It also decreases storage and computation overhead on clients and central servers, protects sensitive user and operational information and increases the responsiveness and dependability of real-time threat detection systems through decentralizing the learning process (Hammad and Abu-Zaid, 2024).

V. ROBUST FEDERATED OPTIMIZATION TECHNIQUES FOR IDS

In order to overcome the fundamental weaknesses of federated learning in intrusion detection systems, especially in the dynamic and heterogeneous nature of 5G networks, powerful federated optimization methods have been created to maximize model resilience and reliability. The aim of these techniques is to alleviate the impact of noisy, biased or malicious updates, which are propagated by the edge nodes or other involved devices, which, when unmitigated, may jeopardize the integrity of the global model (Mahadevappa et al., 2024).

The major techniques are secure aggregation schemes, which make updates of models to be aggregated without revealing individual gradients, anomaly-resistant gradient processing, which removes the outliers, and adaptive weighting schemes, which can assign influence depending on the reliability and quality of client gradients. Furthermore, the convergence rates and model accuracy in the case of various data distributions and different client devices can be enhanced by the use of advanced optimization algorithms, including robust stochastic gradient descent, proximal federated methods, and hybrid ensemble approaches (Khan et al., 2025).

With a combination of these methods, the intrusion detection system can be very precise and recalls high, even under adversarial scenarios, and less vulnerable to data poisoning, model inversion, and other targeted attacks. Federated learning is inherently decentralized, which, in turn, means the absence of single-points of failure, which improves continuity and resiliency of operations in case of coordinated network attacks. In addition, these powerful methods enable the implementation of lightweight and resource-efficient models that can be deployed to edge computing nodes, optimize memory, computational expenses, and communication overheads, and do not compromise detection accuracy (Khalid et al., 2026).

Client-level data balancing, gradient clipping, reputation-based aggregation further techniques are used to make sure that the minority or infrequent classes of attack are sufficiently represented during the training process, and that improperly low-frequency and yet crucial intrusion incidents are detected. Hybrid aggregation system, which combines reputation and statistical filtering provides additional protection against bad nodes and allows strong functioning without trusted validation datasets (Sheikhi et al., 2025). Notably, these approaches are also privacy-sensitive, which allows the IDS to incorporate the knowledge of several sources without revealing sensitive user or operational information. Together, powerful federated optimization will make federated learning-based IDS a scalable, resilient and privacy-preserving system, which can autonomously adapt to the changing and complex threat landscape of 5G networks whilst achieving high efficiency, low latency, and wide

applicability to an extensive range of network topologies and devices (Banafaa et al., 2024).

VI. PROPOSED 5G INTRUSION DETECTION FRAMEWORK

The proposed solution is a strong federated optimization-based intrusion detection system in 5G networks to overcome the issues of scalability, privacy protection, and real-time threat detection in highly distributed systems (Chennoufi, 2025). Within this structure, edge devices and network nodes are constantly gathering traffic data and extracting local feature, which allows the detection of anomaly preliminary near the source of data. Federated learning protocols are used to train local models, so that sensitive raw data is never transferred out of the device, but only model updates are exchanged with a central aggregation server (Khan et al., 2025).

This aggregator uses powerful optimization techniques to amalgamate updates, which reduces the effects of noisy, biased, or malicious updates, and produces a global model, which is replicated by all the participating nodes. This feedback mechanism allows learning and adjustment to changing attack patterns, which makes the system very receptive to the changing conditions of 5G networks. The layered architecture facilitates the large-scale implementation on a wide variety of devices and network segments and reduces communication overhead and ensures high privacy assurances (Jangjou and Sohrabi, 2022).

The cross-silo and cross-device federated learning mechanisms can be added to promote flexibility in heterogeneous environments and enable the cross-collaboration between various administrative domains and network slices and the efficient processing of non-identically distributed data. The combination of smart data processing methods, such as sophisticated feature engineering and context-sensitive analysis, enhances the capacity of the system to identify sophisticated and multi-phase attacks at more than one layer of the network (Abou Elasaad et al., 2025).

Moreover, the incorporation of the semantic analysis facilities via the lightweight language-based models facilitates processing of unstructured network logs, refutes feature representations and enhances detection capabilities of subtle or previously unknown attack patterns. Such semantic improvement enables the framework to go beyond the conventional statistical detection and integrate the contextual understanding, which is especially useful when it comes to detecting more advanced threats (Alzaabi and Mehmood, 2024).

The other important element of the recommended framework is the integration of explainable artificial intelligence mechanisms, which overcome the absence of transparency that can be linked to sophisticated machine learning models. The system has the benefit of increasing the level of trust, accountability and usability of the network by administrators because it provides interpretable insights as to why certain network behaviors are considered malicious (Aminu). The latter explainability features allow security analysts to get insights into the rationale behind detection decisions, which can be used to respond to incidents more effectively and audit the system more effectively. Moreover, the mechanisms of detecting and segregating compromised or unreliable nodes are internalized into the framework, which guarantees the integrity and reliability of the global model under adversarial conditions.

Federated learning, strong optimization, semantic intelligence, and explainable AI create a full-scale intrusion detection system that can work effectively in an intricate and dynamic environment of 5G networks. This system is capable of providing high accuracy in detection, flexibility, and transparency besides maintaining data privacy and minimizing latency. With the help of distributed intelligence and a high level of analytical functions, the suggested framework can be seen as a crucial move towards the creation of next-generation intrusion detection systems that have the potential to protect large-scale, heterogeneous, and mission-critical 5G infrastructures (Kalodanis et al., 2025).

VII. PERFORMANCE EVALUATION AND EXPERIMENTAL RESULTS

Federated learning-based intrusion detection systems in 5G networks need to be evaluated in terms of a range of criteria, such as detection accuracy, false positive rates, communication efficiency, computation overhead, scalability, and resistance to adversarial attacks. The experimental results are consistent, showing that federated IDS structures could detect at a similar or better accuracy than traditional centralized ones, and at the same time, retain data privacy (Fedorchenko et al., 2022).

This is augmented by the adoption of strong federated optimization methods, which increase the stability of the system by reducing the effect of noise, biased, or malicious client updates, increasing the reliability and stability of the global model. Such systems exhibit high potentials in identifying sophisticated and decentralized attack patterns on a large number of edge devices, and adapting to changing threat environments and supporting performance on 5G high volume and real-time networks. Common evaluation measures like precision, recall, F1-score, accuracy, and convergence speed have become common measures to assess the performance of a system to provide a balanced perspective on the effectiveness of detection and the efficiency of the operation (Diallo et al., 2024).

In addition to these basic measures, performance analysis may take into account the implications of communication limits, the distribution of data differently in clients, and the use of adversarial or Byzantine participants on convergence properties and model robustness. Federated IDS models have been shown to be significantly more efficient, and the efficiency of some of the implementations have been reported as high as 99, precision 95, and recall rates of 94, and the latency and communication overhead has been reduced by large factors over centralized models. Besides

this, it has also been shown that time savings of over 80 percent have been achieved with some configurations, which points to how efficient distributed learning can be in reducing computational load without reducing detector performance. The capability to keep the rates of false positives low is especially important in the real world deployment because a high number of false alarms will overload network administrators and make people distrust automated detection systems (Alahmadi et al., 2022).

More empirical experiments indicate that federated models can reach macro-F1 scores of up to 98 percent, with an accuracy of between 92 percent and 98 percent on a variety of data sets and deployment scenarios, both in-domain and cross-domain. The findings highlight the high level of generalization of federated learning, which is improved with iterative model updates to constantly improve the level of detection (Li et al., 2025).

Relative to more basic approaches to federated optimization like standard federated averaging and proximal optimization, more sophisticated approaches to federated optimization have shown observable gains in accuracy, precision, recall, and F1-score, and are also very likely to provide performance gains without sacrificing energy usage and communication expenses. The integration of privacy-preserving techniques, such as differential privacy and encryption-based ones, have also demonstrated little effects on the overall performance of the models, preserving a high level of detection accuracy and preserving the confidentiality of sensitive information (Xu et al., 2021).

Besides, federated deep learning models have levels of performance that are very similar to those of centralized deep learning models with limited differences in accuracy and significant advantages in terms of training time reduction and scalability. Federated IDS structures have even shown superiority over centralized models in some situations especially those where data are non-identically distributed and in a diverse environment (Khraisat et al., 2024).

This benefit is further increased by the fact that federated learning is iterative and adaptive, thus improving model generalization and addressing the impact of concept drift in changing network conditions. Constant review of benchmark datasets prove that federated IDS can reach a high accuracy (more than 97 percent) and effectively recognize a great variety of attack types without losing its strength and efficiency. All these findings illustrate the great potential of federated learning and robust optimization-based methods to provide high-performance, scalable and privacy-friendly intrusion detection solutions specifically designed with the complex and data-intensive environment of 5G networks (Noor et al., 2025).

VIII. FUNDAMENTALS OF FEDERATED LEARNING

As one of the potent distributed machine learning frameworks, federated learning has established itself as a strong model that allows the training of models in a decentralized environment involving multiple clients without allowing the flow of raw data, thus maintaining the privacy and security of data (Beltrán et al., 2023). Federated learning is an alternative to traditional centralized methods, in which data has to be aggregated at one location, unlike federated learning where individual devices or edge nodes can train models on their own data and send only model updates to one central aggregator. This decentralized structure greatly limits the risks involved in data exposure and fits the description of environments in which there are stringent regulatory demands or corporate policies that prevent sharing of data. These properties ensure that federated learning is especially appropriate to 5G networks, where large amounts of sensitive and heterogeneous data are being constantly created at the network edge by mobile devices, IoT systems, and distributed applications (Lee et al., 2024).

Local processing also promotes privacy, in addition to better efficiency, as it lowers the communication overhead and allows low-latency processing, which is essential to real-time applications in 5G settings. Federated learning can ease the pressure on core network infrastructure by only transmitting model parameters, rather than raw data, and enable them to scale to a large number of devices, including those with low computational and storage resources. This is particularly relevant to resource constrained edge environments, where it is vital to utilize bandwidth and processing power efficiently. Moreover, the decentralized structure of federated learning facilitates the combination of knowledge based on a wide variety of different and geographically dispersed sources, which allows intrusion detection systems to learn a wider range of network behaviors and attack patterns, and as a result, enhances the generalization of models and the accuracy of detection (Khraisat et al., 2024).

The other important merit of federated learning is that it can accommodate heterogeneous and non-identically distributed data, which is typically one of the features of real-world 5G networks. The distribution, patterns, and characteristics of data produced by different devices and network segments are often diverse, and federated learning can address this diversity by enabling localized training and still participating in a single global model. This feature improves the strength and flexibility of intrusion detection systems to work well in different working conditions. Furthermore, federated learning allows continuous and incremental updates of models to ensure that systems can change along with network conditions and new cyber threats without having to be retrained entirely (Ghimire and Rawat, 2022).

To enhance further privacy and protection, federated learning systems can be improved with more sophisticated methods, including differential privacy, secure aggregation and gradient obfuscation, that assist in safeguarding sensitive data even at the stage of model updates shared. Such mechanisms make sure that the individual data contributions cannot be reverse-engineered, which increases the confidence in collaborative learning environments. Simultaneously, the federated learning nature makes it less dependent

on centralized infrastructure, which eradicates the system weak points and enhances the system resilience to targeted attacks. Federated learning can offer a scalable, efficient, and privacy-sensitive basis of current intrusion detection systems, especially in the complex, fast-paced, and data-rich environment of 5G networks by permitting collaborative intelligence among multiple devices, maintaining the privacy of data (Rehman et al., 2024).

IX. CHALLENGES IN FEDERATED LEARNING-BASED INTRUSION DETECTION SYSTEMS FOR 5G NETWORKS

Although federated learning-based intrusion detection systems have many benefits, their implementation in 5G settings raises many important challenges that need to be resolved to achieve stable and scalable performance (Chennoufi et al., 2024). The data heterogeneity among distributed clients is one of the most important ones: the data collected locally tend to be non-identically distributed (non-IID). This inconsistency may adversely affect convergence behavior and generalization ability of the global model resulting in decreased detection accuracy, especially in complex and dynamic network scenarios. The solution to this problem is the creation of new optimization techniques that would be able to properly combine different model updates without compromising the stability of the system and its functionality on heterogeneous devices and data streams (Liu et al., 2026).

Another significant issue in federated learning systems is communication overhead, particularly in large-scale 5G networks with the high connectivity of a large number of devices. High frequency transfer of model updates between edge devices and central aggregators may cause a strain on network resources, add latency and reduce scalability. The concern is also worsened by the fact that real-time intrusion detection is required which necessitates fast and low latency communication protocols (Tsikoudis et al., 2014). Thus, in order to render fed learning mechanisms like update compression, selective participation, asynchronous training communication, communication-efficient mechanisms must be designed in practice. In addition to that, the dynamic nature of 5G networks with changing topology, in-between connectivity, and variable network state makes the task of model synchronization hard and may be subject to inconsistencies during the training (Gkonis et al., 2020).

Security vulnerabilities also pose a significant challenge to federated learning-based IDS. The decentralized structure of the framework is vulnerable to different adversarial attacks, such as data poisoning, manipulation and evasion attacks, and inference-based privacy attacks. The integrity of the global model can be compromised by malicious actors who can inject updates into the training process that are corrupted, making the model ineffective (Chen et al., 2020). To alleviate these risks, strong defense protocols, like secure aggregation, client update anomaly detection, and Byzantine-resilient optimization are needed. It is also essential to make sure that the updates of the models are confidential since it is possible to infer sensitive information by the presence of gradients unless privacy-preserving methods are applied (Shokri and Shmatikov, 2015).

Practically, edge devices have limited computational and power resources which further inhibit deployment. Most 5G-connected devices, especially IoT sensors, are limited in the processing power, memory, and battery life, as it is difficult to run complex machine learning models. This requires the design of lightweight and power efficient algorithms that can work efficiently within the resource constraints without affecting the detection performance. In addition, scaling of federated learning systems in large and highly dynamic settings is an unresolved issue especially when trying to adjust to changes in client participation and differences in the quality of data between nodes (Beltrán et al., 2023).

The other significant weakness is the quality and accessibility of datasets to train and test. The absence of heterogeneous, representative, and realistic 5G data prevents the possibility to strictly evaluate the performance of models and their generalization. This is even complicated by the fact that realistic attack scenarios and dynamic traffic patterns are difficult to capture and are fundamental in developing effective intrusion detection systems. Also, the theoretical premises of most federated learning algorithms, including similarity in the data between clients or consistent attendance, are frequently not met in practice, and the convergence behavior is unpredictable, and efficiency in anomaly detection tasks is diminished (Gow et al., 2017).

Lastly, the fast propagation of 5G-based IoT environments compounds these pressures further by raising the complexity of systems, resource consumption, and vulnerability to risks. To deal with such problems, a comprehensive solution is needed that involves powerful optimization methodologies, effective communication systems, sophisticated security solutions, as well as the implementation of adaptive learning systems. Further studies in these directions are crucial to achieve the full potential of federated learning in intrusion detection to create scalable, secure, and efficient solutions that can operate in the highly dynamic and heterogeneous environment of the current 5G networks (Noor et al., 2025).

X. FUTURE DIRECTIONS

The 5G intrusion detection systems research in the future will mainly aim at improving robustness, scalability, adaptability, and interpretability in federated learning. The necessity of autonomous and intelligent security mechanisms increases as 5G networks keep becoming more and more complex (Blika et al., 2024). Among the main directions, the creation of more sophisticated aggregation methods and customized federated learning frameworks capable of managing heterogeneous data distributions in various network nodes can be observed, benefiting the accuracy of detection and efficiency of work. Concept drift in online, continual and transfer learning is also a crucial concept to address to ensure that online intrusion detection systems are still valid in the environment of dynamically varying traffic patterns

and the development of cyber threats (Jemili et al., 2025). In this regard, adaptive learning processes that dynamically update model parameters on real time basis will be very important in ensuring system relevance and responsiveness.

The other valuable area of research is the incorporation of explainable artificial intelligence into federated learning systems. As intrusion detection models grow more complex, it is critical to offer transparent and understandable insights into such models to gain trust, speed of incident response and accountability in critical processes. Further ways of improving the scalability, interpretability, and performance of the models are advanced methods like attention mechanisms, knowledge distillation, and self-supervised learning. Simultaneously, the integration of advanced deep learning structures such as graph-based models and multi-modal learning techniques may be of great value to the capacity of the IDS to identify intricate constraints and identify subtle and multi-contextual attack patterns in highly dynamic 5G settings (Yao, 2023).

The security and integrity of a federated learning system itself is also a difficult concern, especially when it is subject to adversarial attacks, including data poisoning, model inversion, and gradient manipulation attacks. The next generation of work should be directed at creating strong defense measures that will help identify and eliminate such attacks without disrupting the collaborative characteristics of federated learning. The hierarchical federated architectures and decentralized client-clustering strategies provide potential solutions to the enhancement of scalability and efficiency in large-scale IoT and edge computing systems. Also, it is necessary to test IDS frameworks in adversarial settings and in hostile environments to confirm their resilience and practical use (SABRINE et al., 2024).

Federated learning as a technology combined with complementary technologies also has great potential of being innovated. Federated IDS can be used in conjunction with other security strategies, including intrusion prevention systems and adaptive firewalls, which may result in more thorough and multilayered security solutions. Moreover, the integration of blockchain technology may contribute to greater transparency, confidence and tracking of model updates, which will allow the network participants to collaborate securely and in a decentralized manner. Privacy-protecting methods, such as differential privacy and secure multi-party computation will remain crucial in keeping the data protection regulations and high detection rates (Balamurugan, 2025).

In addition to technical improvements, the effects of network-level issues, including the instability of the communication, changes in latency, and resource limitations, on federated IDS performance should also be included in future research. To make practical deployments, it is necessary to develop lightweight, energy efficient models that can work under these conditions.

Besides, the ability to extend federated intrusion detection architectures to a variety of 5G applications, such as industrial IoT, smart cities, and mission-critical applications, will necessitate domain-specific solutions that consider domain-specific requirements and constraints (Rafique et al., 2024). Lastly, the societal and ethical aspects of AI-based intrusion detection systems should be taken into account.

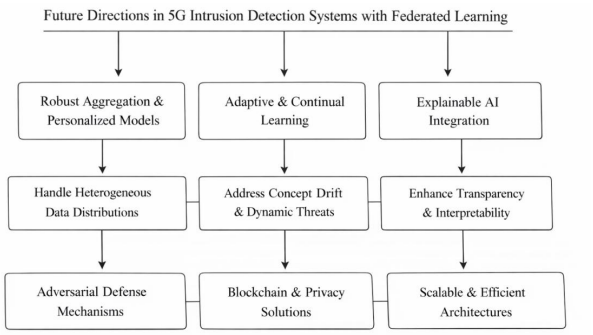

Fig. 3. Future Research in 5G Intrusion Detection Systems using Federated Learning: A flowchart of the main research topics such as robust aggregation, adaptive learning, explainable AI, and scalable security solutions to the changing 5G environments.

There should be problems concerning the algorithmic bias, fairness, and responsible use of automated decision-making processes to provide fair and reliable security practices. The privacy preservation versus effective threat detection is another interesting aspect that concerns exploration, especially in multi-stakeholder 5G environments where contradictory demands might occur.

On the whole, the further evolution of federated learning, along with powerful optimization, explainable AI, and new technologies, offers a bright future of creating safe, scalable, and intelligent intrusion detection systems that could protect the diverse and dynamic environment of 5G network (Alanazi, 2023) as shown in Figure 3.

XI. CONCLUSION

To sum up, federated learning as an extension of intrusion detection systems is a major step in the right direction in combating the security threats of contemporary 5G networks. Federated learning due to its distributed and privacy-preserving nature can be used to train a model collaboratively across a variety of network nodes without sharing sensitive data, making it especially suitable to the decentralized and data-heavy nature of 5G environments. In this review, the federated learning-based IDS frameworks have been proven to have high detection accuracy, scalability, and adaptability with low latency and minimized communication overhead. The integration of strong federate optimization strategies also contributes to the resilience of the system to adversarial attacks that guarantee efficient operation even with the presence of corrupt or untrustworthy actors.

In spite of these benefits, a number of issues persist, such as managing non-IID data distributions, providing efficient communication, managing resource limitations on the edge devices, and resistance to advanced adversarial attacks. There is also the limitation of the standardization of

datasets and real-world evaluation structures to fully validate such systems in real-world deployments. Nevertheless, the current developments of adaptive learning methods, privacy-sensitive approaches, and explainable AI should help overcome these shortcomings and further enhance the efficiency of federated IDS.

In the future, federated learning intersects with new technologies like edge intelligence, blockchain, and state-of-the-art deep learning architectures, which offer high innovation potential. Such developments will probably allow the development of more powerful, open, and scalable intrusion detection systems that can run effectively in highly dynamic and heterogeneous environments. Finally, federated learning provides a good direction to the development of next-generation security solutions that are capable of safeguarding not only critical 5G infrastructure but also guarantee privacy, trust, and resilience in an increasingly interconnected digital ecosystem.

FUNDING

This work was supported by "University Computer Fundamentals" 2025 Henan Provincial University General Education Excellence Course, and the 2025 China Police Association Research Project: "Risks and Regulatory Pathways of Generative Artificial Intelligence Technology in Smart Policing.".

REFERENCES

[1] M. M. Abou Elasaad, S. G. Sayed, and M. M. El-Dakroury, "AegisGuard: A Multi-Stage Hybrid Intrusion Detection System with Optimized Feature Selection for Industrial IoT Security," Sensors, vol. 25, p. 6958, 2025.

[2] A. Ahad, K. I. Ahmed, F. Ullah, M. A. Sheikh, M. Tahir, M. Hayajneh, and I. M. Pires, "Federated Learning and 5G/6G-Based Internet of Medical Things (IoMT): Applications, Key Enabling Technologies, Open Issues and Future Research Directions," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 16, p. e70065, 2026.

[3] B. A. Alahmadi, L. Axon, and I. Martinovic, "99% false positives: A qualitative study of {SOC} analysts' perspectives on security alarms," in 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 2783–2800.

[4] A. Alam, A. Umer, I. Ullah, and A. Alsayat, "AI-enabled cybersecurity framework for future 5G wireless infrastructures," Scientific Reports, 2026.

[5] M. N. Alanazi, "5g security threat landscape, ai and blockchain," Wireless Personal Communications, vol. 133, pp. 1467–1482, 2023.

[6] A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense," Future Internet, vol. 15, p. 62, 2023.

[7] S. M. Altowaijri and M. Ayari, "The Synergistic Impact of 5G on Cloud-to-Edge Computing and the Evolution of Digital Applications," Mathematics, vol. 13, p. 2634, 2025.

[8] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," IEEE Access, vol. 12, pp. 30907–30927, 2024.

[9] T. Aminu, "Unraveling Cybersecurity Threats Via Interpretable Machine Learning and Computer Algorithms Enhancing Trust in Data Science Pipelines."

[10] H. V. Balamurugan, "Enhancing Individual Privacy Preservation in Multi-Tenancy Cloud Environments through Secure Multi-Party Computations: A Differential Privacy-Based Data Partitioning Strategy," Dublin, National College of Ireland, 2025.

[11] M. K. Banafaa, Ö. Pepeoğlu, I. Shayea, A. Alhammadi, Z. A. Shamsan, M. A. Razaz, M. Alsagabi, and S. Al-Sowayan, "A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges," IEEE access, vol. 12, pp. 7786–7826, 2024.

[12] A. Baz, J. Logeshwaran, Y. Natarajan, and S. K. Patel, "Enhancing mobility management in 5G networks using deep residual LSTM model," Applied Soft Computing, vol. 165, p. 112103, 2024.

[13] E. T. M. Beltrán, M. Q. Pérez, P. M. S. Sánchez, S. L. Bernal, G. Bovet, M. G. Pérez, G. M. Pérez, and A. H. Celdrán, "Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges," IEEE Communications Surveys & Tutorials, vol. 25, pp. 2983–3013, 2023.

[14] A. Blika, S. Palmos, G. Doukas, V. Lamprou, S. Pelekis, M. Kontoulis, C. Ntanos, and D. Askounis, "Federated learning for enhanced cybersecurity and trustworthiness in 5G and 6G networks: A comprehensive survey," IEEE Open Journal of the Communications Society, vol. 6, pp. 3094–3130, 2024.

[15] Y. Chen, F. Luo, T. Li, T. Xiang, Z. Liu, and J. Li, "A training-integrity privacy-preserving federated learning scheme with trusted execution environment," Information Sciences, vol. 522, pp. 69–79, 2020.

[16] S. Chennoufi, "Privacy-preserving and robust attack-knowledge sharing in heterogeneous 5G networks via federated prototype-based intrusion detection," Institut Polytechnique de Paris, 2025.

[17] S. Chennoufi, G. Blanc, H. Jmila, and C. Kiennert, "SoK: federated learning based network intrusion detection in 5G: context, state of the art and challenges," in Proceedings of the 19th International Conference on Availability, Reliability and Security, 2024, pp. 1–13.

[18] J. Cook, S. U. Rehman, and M. A. Khan, "Security and privacy for low power iot devices on 5g and beyond networks: Challenges and future directions," IEEE Access, vol. 11, pp. 39295–39317, 2023.

[19] R. Diallo, C. Edalo, and O. O. Awe, "Machine learning evaluation of imbalanced health data: a comparative analysis of balanced accuracy, MCC, and F1 score," in Practical Statistical Learning and Data Science Methods: Case Studies from LISA 2020 Global Network, USA, Springer, 2024, pp. 283–312.

[20] Q. Duan, J. Huang, S. Hu, R. Deng, Z. Lu, and S. Yu, "Combining federated learning and edge computing toward ubiquitous intelligence in 6G network: Challenges, recent advances, and future directions," IEEE Communications Surveys & Tutorials, vol. 25, pp. 2892–2950, 2023.

[21] J. Fang, G. Zhao, H. Xu, C. Wu, and Z. Yu, "GRID: Gradient routing with in-network aggregation for distributed training," IEEE/ACM Transactions on Networking, vol. 31, pp. 2267–2280, 2023.

[22] E. Fedorchenko, E. Novikova, and A. Shulepov, "Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges," Algorithms, vol. 15, p. 247, 2022.

[23] O. A. Fernando, "Real-Time Application of Deep Learning to Intrusion Detection in 5G-Multi-Access Edge Computing," 2024.

[24] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," IEEE Internet of Things Journal, vol. 9, pp. 8229–8249, 2022.

[25] P. K. Gkonis, P. T. Trakadas, and D. I. Kaklamani, "A comprehensive study on simulation techniques for 5g networks: State of the art results, analysis, and future challenges," Electronics, vol. 9, p. 468, 2020.

[26] R. Gow, F. A. Rabhi, and S. Venugopal, "Anomaly detection in complex real world application systems," IEEE Transactions on Network and Service Management, vol. 15, pp. 83–96, 2017.

[27] A. Hammad and R. Abu-Zaid, "Applications of AI in decentralized computing systems: harnessing artificial intelligence for enhanced scalability, efficiency, and autonomous decision-making in distributed architectures," Applied Research in Artificial Intelligence and Cloud Computing, vol. 7, pp. 161–187, 2024.

[28] P. C. Jain, "Recent Advances in Next Generation Cellular Mobile Networks-5G, 5G-Adv., and 6G," in 2025 International Conference on Innovation in Computing and Engineering (ICE), IEEE, 2025, pp. 1–6.

[29] M. Jangjou and M. K. Sohrabi, "A comprehensive survey on security challenges in different network layers in cloud computing," Archives of Computational Methods in Engineering, vol. 29, pp. 3587–3608, 2022.

[30] F. Jemili, K. Jouini, and O. Korbaa, "Intrusion detection based on concept drift detection and online incremental learning," International Journal of Pervasive Computing and Communications, vol. 21, pp. 81–115, 2025.

[31] K. Kalodanis, C. Papapavlou, and G. Feretzakis, "Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention," Future Internet, vol. 17, p. 312, 2025.

[32] S. Khalid, M. U. Rehman, A. B. Usman, and M. Khawar, "Resource-efficient models for edge devices," Edge Intelligence: 111-153, 2026.

[33] N. Khan, S. Nisar, M. A. Khan, Y. A. U. Rehman, F. Noor, and G. Barb, "Optimizing federated learning with aggregation strategies: A comprehensive survey," IEEE Open Journal of the Computer Society, 2025.
[34] A. Khraisat, A. Alazab, S. Singh, T. Jan, and A. Jr. Gomez, "Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions," ACM Computing Surveys, vol. 57, pp. 1–38, 2024.
[35] J. Lee, F. Solat, T. Y. Kim, and H. V. Poor, "Federated learning-empowered mobile network management for 5G and beyond networks: From access to core," IEEE Communications Surveys & Tutorials, vol. 26, pp. 2176–2212, 2024.
[36] Y. Li, X. Wang, R. Zeng, P. K. Donta, I. Murturi, M. Huang, and S. Dustdar, "Federated domain generalization: A survey," Proceedings of the IEEE, 2025.
[37] J. Liu, Y. Du, K. Yang, J. Wu, Y. Wang, X. Hu, Z. Wang, Y. Liu, P. Sun, and A. Boukerche, "Edge-cloud collaborative computing on distributed intelligence and model optimization: A survey," IEEE Communications Surveys & Tutorials, 2026.
[38] X. Liu, X. Su, G. Del Campo, J. Cao, B. Fan, E. Saavedra, A. Santamaría, J. Röning, P. Hui, and S. Tarkoma, "Federated learning on 5g edge for industrial internet of things," IEEE Network, vol. 39, pp. 289–297, 2024.
[39] P. Mahadevappa, R. Al-Amri, G. Alkawsi, A. A. Alkahtani, M. F. Alghenaim, and M. Alsamman, "Analyzing threats and attacks in edge data analytics within IoT environments," IoT, vol. 5, pp. 123–154, 2024.
[40] S. Nabavirazavi, R. Taheri, M. Ghahremani, and S. S. Iyengar, "Model poisoning attack against federated learning with adaptive aggregation," in Adversarial Multimedia Forensics, Springer, 2023, pp. 1–27.
[41] K. Noor, A. L. Imoize, C. -T. Li, and C. -Y. Weng, "A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond," Mathematics, vol. 13, p. 1088, 2025.
[42] M. Nuriev, A. Kalyashina, Y. Smirnov, G. Gumerova, and G. Gadzhieva, "The 5G revolution transforming connectivity and powering innovations," in E3S Web of Conferences, EDP Sciences, 2024, p. 04008.
[43] W. Rafique, J. R. Barai, A. O. Fapojuwo, and D. Krishnamurthy, "A survey on beyond 5g network slicing for smart cities applications," IEEE Communications Surveys & Tutorials, vol. 27, pp. 595–628, 2024.
[44] A. Rahman, -U, M. Mahmud, T. Iqbal, L. Saraireh, H. Kholidy, M. Gollapalli, D. Musleh, F. Alhaidari, D. Almoqbil, and M. I. B. Ahmed, "Network Anomaly Detection in 5G Networks," Mathematical Modelling of Engineering Problems, 9, 2022.
[45] H. Rasheed and A. Alam, "COMPREHENSIVE EXAMINATION OF CYBERSECURITY THREATS AND VULNERABILITIES IN 5G NETWORKS: EXPLORING EMERGING RISKS, ADVANCED ATTACK VECTORS, AND CUTTING-EDGE MITIGATION STRATEGIES FOR FUTURE-READY SECURITY ARCHITECTURES," Computers and Education letters, vol. 1, pp. 1–13, 2024.
[46] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, "A federated learning-based approach for improving intrusion detection in industrial internet of things networks," Network, vol. 3, pp. 158–179, 2023.
[47] T. Rehman, N. Tariq, F. A. Khan, and S. U. Rehman, "Ffl-ids: a fog-enabled federated learning-based intrusion detection system to counter jamming and spoofing attacks for the industrial internet of things," Sensors, vol. 25, p. 10, 2024.
[48] H. Rezaei, R. Taheri, E. Nowroozi, M. Hajizadeh, S. Shiaeles, and T. Bauschert, "A Survey on Security and Privacy in Federated Learning-Based Intrusion Detection Systems for 5G and Beyond Networks," IEEE Open Journal of the Communications Society, vol. 7, pp. 253–300, 2025.
[49] E. Sabrine, F. de Gaspari, H. Dorjan, A. K. Bidi, and L. V. Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," arXiv preprint arXiv:2409.18736, 2024.
[50] C. Serôdio, J. Cunha, G. Candela, S. Rodriguez, X. R. Sousa, and F. Branco, "The 6G ecosystem as support for IoE and private networks: Vision, requirements, and challenges," Future Internet, vol. 15, p. 348, 2023.
[51] S. Sheikhi, P. Kostakos, and L. Loven, "Hybrid Reputation Aggregation: A Robust Defense Mechanism for Adversarial Federated Learning in 5G and Edge Network Environments," IEEE Open Journal of the Communications Society, vol. 7, pp. 370–385, 2025.
[52] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, 2015, pp. 1310–1321.
[53] Y. Su, "Developing federated analytical techniques for time series data," University of Warwick, 2024.
[54] T. Theodoropoulos, L. Rosa, C. Benzaid, P. Gray, E. Marin, A. Makris, L. Cordeiro, F. Diego, P. Sorokin, and M. D. Girolamo, "Security in cloud-native services: A survey," Journal of Cybersecurity and Privacy, vol. 3, pp. 758–793, 2023.
[55] N. Tsikoudis, A. Papadogiannakis, and E. P. Markatos, "LEoNIDS: A low-latency and energy-efficient network-level intrusion detection system," IEEE Transactions on Emerging Topics in Computing, vol. 4, pp. 142–155, 2014.
[56] J. Wang, L. Yu, J. Lui, and X. Luo, "Modern DDoS threats and countermeasures: insights into emerging attacks and detection strategies," arXiv preprint arXiv:2502.19996, 2025.
[57] R. Xu, N. Baracaldo, and J. Joshi, "Privacy-preserving machine learning: Methods, challenges and directions," arXiv preprint arXiv:2108.04417, 2021.
[58] J. W. Yao, "A 5G Security Recommendation System Based on Multi-Modal Learning and Large Language Models," Concordia University, 2023.