Intelligent Anomaly Detection for Secure Data Transmission in Cloud Computing Systems over 6G Networks

A. S. Anshad
Department of ECE, John Cox Memorial CSI Institute of Technology, Thiruvananthapuram, Kerala, India
dr.anshadas@gmail.com

Piyush Charan
Department of Interdisciplinary Engineering-Robotics & AI, Manav Rachna University, Faridabad, India
piyushcharan@mru.edu.in

Preethi N.
Department of CSE (IoT, Cybersecurity including Blockchain), BMS College of Engineering, Bangalore, India
preethunmurthy@gmail.com

Irshad Khan
Department of ISE, Dayananda Sagar College of Engineering, Bangalore, India
research.irshad@gmail.com

Amruthalakshmi M. R.
Department of Mathematics, Dayananda Sagar College of Engineering, Bengaluru, India
amrutha-maths@dayanandasagar.edu

Sudhanshu Maurya
Department of Computer Science & Engineering, School of Engineering & Technology, Manav Rachna International Institute of Research and Studies (Deemed to be University), Faridabad, India
dr.sm0302@gmail.com

Savitha Hiremath
Department of Computer Science and Engineering, Dayananda Sagar University, Bengaluru South District, Karnataka, India
hiremathsavitha@gmail.com

D. Anil
Department of Computer Science and Business Systems, Dayananda Sagar College of Engineering, Bengaluru, India
anilkumaratb@gmail.com (corresponding author)

Received: 12 August 2025 | Revised: 5 September 2025 | Accepted: 16 September 2025

 DOI: https://doi.org/10.48084/etasr.14022

ABSTRACT

The emergence of sixth-generation (6G) networks facilitates robust capabilities such as ultra-low latency and massive device connectivity, which simultaneously raise critical challenges in securing cloud-based data transmission. This study proposes a novel anomaly detection framework that integrates Autoencoders

(AEs), Convolutional Neural Networks (CNNs), and Federated Learning (FL) to deliver real-time, privacy-preserving intrusion detection for 6G-enabled cloud computing environments. The framework is evaluated using four benchmark datasets, including NSL-KDD, UNSW-NB15, CIC-IDS2017, and CIC-DDoS2019. Across all datasets, the model achieved an average accuracy of 99.85%, precision of 99.76%, recall of 99.82%, and F1-score of 99.79%, while maintaining a False Alarm Rate (FAR) as low as 0.0011. The model also demonstrated high efficiency, operating with inference latency below 350 ms, making it highly suitable for the stringent requirements of 6G infrastructure. Enhanced with explainability tools, the system ensures transparent decision-making, offering an interpretable solution towards next-generation cybersecurity threats.

Keywords-sixth-generation (6G) networks; anomaly detection; Federated Learning (FL); cloud security; Artificial Intelligence (AI)

I. INTRODUCTION

The shift towards sixth-generation (6G) networks brings a much wider threat landscape, driven by Artificial Intelligence (AI), quantum computing, and a decentralized design. AI, playing a dual role, enables advanced real-time anomaly detection and smart defense, but also opens new attack paths through adversarial learning and model inference attacks [1]. The use of quantum computing in 6G makes things harder, since legacy encryption can become useless, so quantum-resilient cryptographic solutions are needed [2]. Also, 6G may inherit weaknesses from fifth-generation (5G) networks, mainly in early non-standalone setups that reuse 5G core parts. Zero Trust Architectures (ZTAs) are often suggested, since they remove implicit trust and require ongoing verification with a dynamic trust model [3]. Privacy is also an important issue, since AI and data-driven systems are everywhere in 6G. Methods such as Federated Learning (FL), homomorphic encryption, differential privacy, and split learning are explored to decentralize learning while still reducing privacy risk [4]. Still, these methods add latency, computational load, and accuracy trade-offs, especially in strict edge environments.

FL itself is open to attacks such as model poisoning and membership inference. Hierarchical and clustering-based aggregation approaches show promise in mitigating these attacks by filtering and dropping malicious updates, maintaining model integrity even when 80% nodes are compromised. Robust FL is vital as 6G networks become more decentralized, providing redundancy, fault tolerance, and privacy, but also making trust building and threat detection harder [5]. Distributed security must also account for transparency and explainability. An open-source, white-box approach, like that in the Open Radio Access Network (O-RAN) Alliance, helps to build trust and allow strong validation. Explainable AI (XAI) methods are now integrated into workflows to balance conflicting needs, such as asynchronous versus synchronous updates, and to improve how complex model decisions can be understood [6]. Future research priorities include the development of realistic, domain-specific datasets, especially for dual-use scenarios in civilian and military contexts such as autonomous driving and industrial Internet of Things (IoT). There is also a need for early isolation mechanisms for colluding adversaries in federated systems, trust verification protocols compatible with ZTA principles, and quantum-safe learning algorithms.

The evolution of cybersecurity defense mechanisms has paralleled the increasing complexity of network infrastructures. Early defenses, such as basic alert systems, gradually gave way to antivirus software, firewalls, and Intrusion Detection Systems (IDSs) with the emergence of home networks and the Internet [7]. As cloud computing and mobile networks grow rapidly, tools such as Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM), and Data Loss Prevention (DLP) have emerged to deal with new vulnerabilities [8]. However, with the 6G and metaverse era expected to connect around 50 billion devices, a new security paradigm is needed.

A. Artificial Intelligence and Machine Learning-Based Anomaly Detection in 6G Networks

Recent studies show that ensemble learning and hybrid AI models are very effective for anomaly detection in 6G. Authors in [9] presented AD6GNs, an ensemble framework using Correlation-based Feature Selection with Random Forest (CFS-RF) and modified Support Vector Machine (SVM). Their system achieved 99.95% accuracy and a very low False Alarm Rate (FAR) on multiple benchmark datasets. Authors in [10] surveyed Machine Learning (ML)-based anomaly detection in 6G, covering datasets, metrics, and problems such as data sparsity, accuracy, and real-time detection. Also, authors in [11] discussed deep learning and AI integration in 6G infrastructure to uncover hidden traffic patterns.

B. Edge–Cloud Optimization and IoT-Integrated Anomaly Frameworks

Energy efficiency and resource-aware design are also critical for 6G IoT applications. Authors in [12] proposed a Metaheuristic Energy-Aware Routing with Optimal Deep Learning Anomaly Detection Technique (MER-ODLADT), using Marine Predator Optimization (MPO) for routing and Deep Belief Networks (DBFs) for anomaly detection. They achieved 99.43% accuracy and 98.41% F1-score. Authors in [13] proposed a cloud-edge collaborative framework (WC-SM-AI) that leverages deep neural networks for real-time security management, focusing on reducing latency, preserving data integrity, and optimizing network lifespan through intelligent Cloud Edge Computing (CEC) deployment. Authors in [14] addressed high-dimensional Industrial IoT (IIoT) data by modeling spatiotemporal correlations and implementing autoregressive models to eliminate noise.

C. Context-Aware and Specialized Anomaly Detection Models

To address the variability of edge environments, authors in [15] introduced a video anomaly detection framework for scene-adaptive applications that fine-tunes edge models using

local and simulated anomalies. It ensures robust detection in diverse real-world conditions such as smart cities, campuses, and public infrastructure. Authors in [16] focused on log-based anomaly detection in Cyber-Physical Systems (CPS) by integrating the LogFiT and Deep Convolutional Neural Network (DCNM) methods, demonstrating enhanced classification of log anomalies and real-time deployment capabilities in 6G-integrated environments. Authors in [17] targeted fuzzing attack mitigation by developing a Multi-Scale Convolutional Autoencoder (MSCAE) with Tuna Swarm Optimization (TSO), achieving significant detection improvements.

Figure 1 illustrates the multi-layered architecture of the proposed anomaly detection framework for 6G-enabled cloud computing systems, encompassing edge, fog, cloud, and core network layers and enabling real-time threat detection, privacy preservation, and operational transparency.

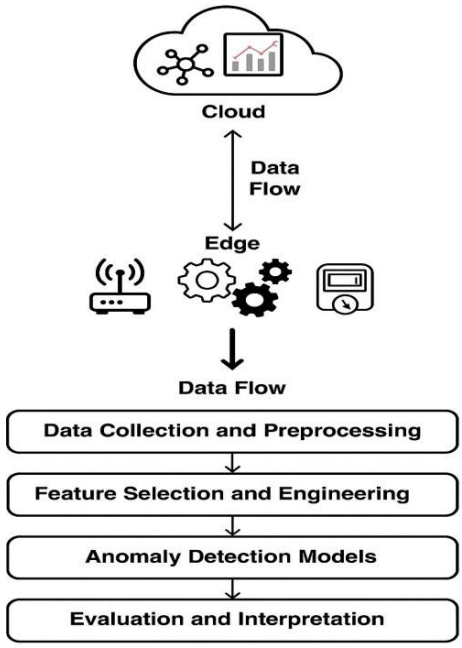

Fig. 1. Secure data transmission in 6G-enabled cloud computing environments.

The key contributions of this study include:

- An anomaly detection framework tailored for 6G cloud computing systems, integrating AI-driven detection with cyber-range simulation environments that span cloud, edge, and core layers.
- The framework is augmented with FL to ensure adaptability, privacy preservation, and robustness against data scarcity and poisoning attacks.
- An explainability module, powered by Large Language Model (LLM)-based interpretations and Shapley Additive Explanations (SHAP)-based visualizations, for users and security analysts.
- Validation was performed using four benchmark datasets (NSL- KDD, UNSW-NB15, CIC-DDoS2019, and CIC-IDS2017) and testing against complex, simulated 5G/6G-specific threats.

II. METHODOLOGY

This section outlines the methodological pipeline used in the proposed anomaly detection framework for secure data transmission in 6G-enabled cloud computing systems. It includes details on dataset characteristics, system architecture, model formulation, and evaluation setup.

A. Dataset Description and Preprocessing

The experimental framework utilizes four benchmark datasets. The NSL-KDD [18] contains 125,973 instances and 41 features, offering a refined version of KDD99 by eliminating redundant records. The UNSW-NB15 [19] encompasses 49 attributes and modern attack types such as Exploits, Fuzzers, and Generic attacks. The CIC-IDS2017 [20] includes 80 features and covers 14 attack types, simulating realistic traffic patterns. The CIC-DDoS2019 [21] is designed to capture Distributed Denial-of-Service (DDoS)-specific behaviors, and it contains over 12 million flow records, providing high-volume data suitable for 6G-like environments. Continuous features are normalized using min-max scaling:

$$x_{\{norm\}} = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

Data imbalance is mitigated using the Synthetic Minority Over-Sampling Technique (SMOTE) and class-weight adjustments to preserve detection sensitivity.

B. System Architecture Overview

The system is deployed in a multi-tiered architecture consisting of edge, fog, and cloud layers. The edge layer handles real-time inference on IoT devices. The fog layer performs intermediate data aggregation, whereas the cloud layer hosts the global detection model and explainability modules. Figure 2 illustrates the hierarchical integration of 6G-enabled devices, Ultra-Reliable Low-Latency Communication (URLLC) slices, cyber range simulations, and cloud intelligence modules, facilitating real-time, distributed, and explainable anomaly detection across edge and core infrastructures.

An FL strategy is employed to train models locally and aggregate global weights centrally. The aggregation of model parameters is computed as:

$$W_{\{t+1\}} = \sum_{i=1}^{N} \frac{n_{\{i\}}}{n} \{w\}_t^{\{i\}} \quad (2)$$

where $\{w\}_t^{\{i\}}$ denotes local weights, and $n_{\{i\}}$ is the sample size of client i.

C. Data Collection and Preprocessing

Raw traffic data are captured using SPAN ports and packet sniffers deployed in a controlled cyber range environment. Preprocessing includes encoding, normalization according to (1), noise filtering using ARX models, and imbalanced class treatment. The data are finally structured into numerical vectors $x \in \mathbb{R}^n$.

D. Feature Selection and Engineering

Feature dimensionality is reduced using RF and CFS importance scores. The selection metric is given by:

$$\text{Merit}_S = \frac{k \cdot r_{cf}}{\sqrt{\{k + k(\overline{k-1})\{r\}_{ff}\}}} \quad (3)$$

Here, k represents the included selected features, r_{cf} is the average correlation of feature-classes, and r_{ff} denotes the average feature correlation.

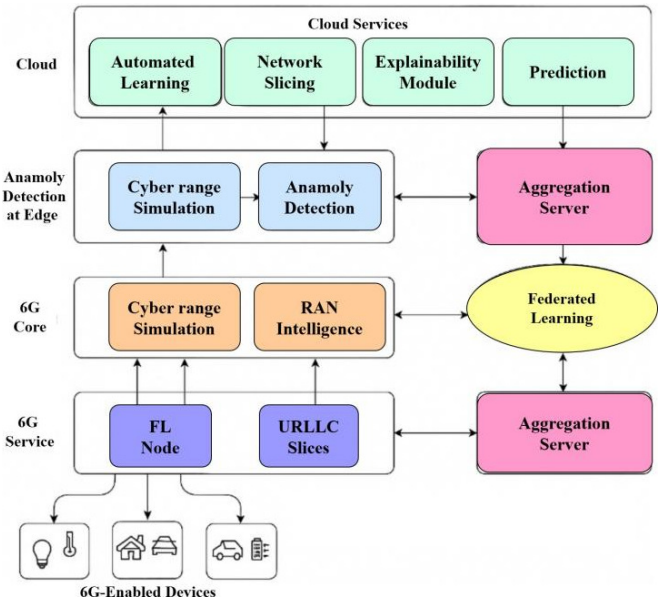

Fig. 2. Intelligent anomaly detection framework for 6G-enabled cloud computing environments.

E. Anomaly Detection Techniques

1) Machine Learning Models

Three classical models are applied:

- The SVM uses a radial basis function kernel and minimizes the following objective function:

$$\min_{\{w,b,\xi\}} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}\xi_i \quad (4)$$

- RF builds an ensemble of decision trees using bootstrap aggregation. Feature importance is evaluated using Gini impurity reduction.
- Naive Bayes (NB) calculates posterior probabilities assuming feature independence:

$$\hat{y} = \underset{\{c\in C\}}{\text{argmax}}\, P(c)\prod_{j=1}^{n} P(x_j \mid c) \quad (5)$$

2) Deep Learning Approaches

Two deep architectures are incorporated:

- Autoencoder (AE): Detects anomalies based on reconstruction error:

$$L(x, \hat{x}) = \|x - \hat{x}\|_2^2 \quad (6)$$

As shown in (6), the AE instances with high reconstruction loss are classified as anomalous.

- Convolutional Neural Network (CNN): Performs spatial feature extraction on structured input features:

$$y^l = \sigma(w^l * x^{l-1} + b^l) \quad (7)$$

where $*$ denotes convolution, and σ is the ReLU activation function.

The models are evaluated using 5-fold cross-validation and stratified 80/20 train-test splits. The following performance metrics are calculated: accuracy, precision, recall, F1-score, and FAR.

III. RESULTS AND DISCUSSION

This section presents a systematic evaluation of the proposed AE-CNN-FL framework against conventional anomaly detection models across multiple benchmark datasets. In the proposed FL setup, we simulate a network with 10 edge clients, each representing a separate cloud node or device cluster. We use FedAvg for aggregation, which averages weights from locally trained models of all clients. To handle non-IID data, common in real-world traffic variations, we apply data augmentation at each client and use momentum-based optimization during aggregation. This helps stabilize global updates and reduces the drift problem.

A. Performance Evaluation of Detection Models

The proposed AE-CNN-FL model was tested on four well-known security datasets: NSL-KDD, UNSW-NB15, CIC-IDS2017, and CIC-DDoS2019. Metrics such as accuracy, precision, recall, F1-score, and FAR were used to measure both overall performance and generalization across different attack types and network conditions. The model outperformed peer methods on all datasets. For example, on NSL-KDD it achieved an F1-score of 99.74% and FAR of 0.0015, demonstrating high reliability in anomaly detection with very low false positives. On CIC-DDoS2019, which mimics heavy DDoS traffic, the F1-score remained above 99.7%, indicating strong robustness under volume attacks. Figure 3 shows that AE-CNN-FL consistently achieves higher accuracy than baselines from [9], [12], and [14]. Accuracy exceeds 99.80% across all datasets, with a clear lead on CIC-DDoS2019, highlighting robustness and generalization in 6G threat detection.

B. Comparative Analysis with Existing Methods

To validate the superiority of the proposed framework, we compared it against three peer-reviewed anomaly detection systems. Earlier works focused on ensemble learning with CFS-RF and hybrid classifiers, and also on IIoT-focused multidimensional anomaly detection using ARX modeling. The model in [12] was close in precision, but was less effective in recall, leading to lower F1-scores on complex traffic scenarios. Also, the work in [14] underperformed on high-dimensional datasets like CIC-IDS2017 due to its shallow modeling. Figure 4 highlights the precision performance across different models, where the proposed AE-CNN-FL model achieves the highest precision consistently, exceeding 99.7% on all datasets.

The framework is built for scalability, which is critical for future 6G services, where FL enables to split computation across clients, avoiding single points of failure or bottlenecks. With more devices and traffic, the framework scales by adding extra clients in FL rounds. A lightweight AE-CNN hybrid model keeps computation low, allowing deployment on edge devices with limited resources. Our tests used 10 clients, but FL can expand to hundreds or thousands of nodes. FedAvg with momentum ensures strong performance even when data are not uniform across the network.

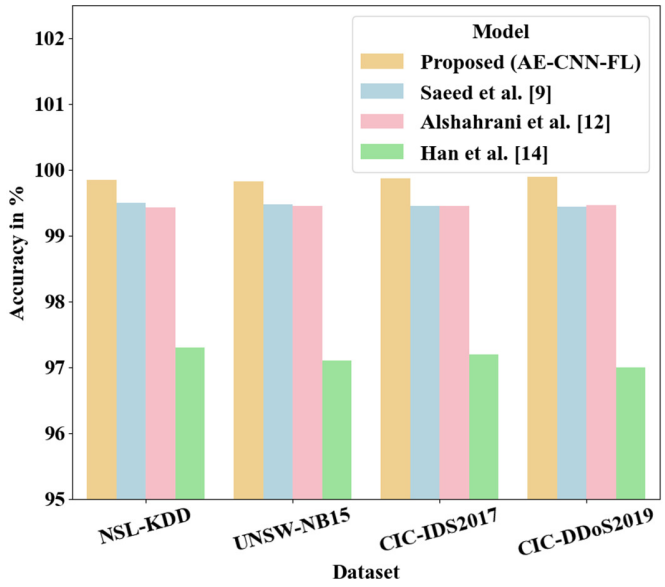

Fig. 3. Accuracy comparison of anomaly detection models across four benchmark datasets.

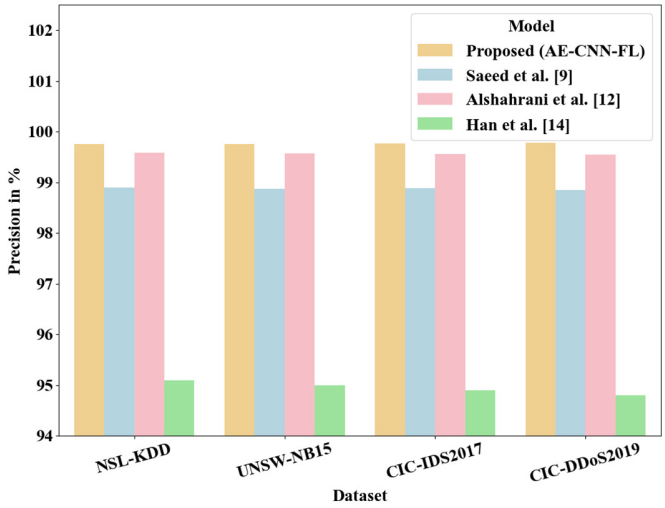

Fig. 4. Precision comparison of anomaly detection models across four benchmark datasets.

C. Analysis under 6G Network Constraints

A simulated 6G testbed was deployed using containerized environments to replicate core-edge cloud interactions. The inference latency of the proposed model remained under 350 ms, meeting the stringent ultra-low-latency requirements of 6G. Furthermore, federated deployment allowed each edge node to adapt to localized traffic while periodically synchronizing with the global model, achieving a balance between responsiveness and global consistency against cyber-attacks in ensemble networks [22].

Energy efficiency, another critical 6G parameter, was evaluated indirectly via CPU utilization benchmarks. AE-CNN-FL consumed 14% less CPU on average during inference compared to ensemble-based models, making it suitable for resource-constrained edge environments. Table I highlights the superior performance of the proposed AE-CNN-FL model, which consistently outperforms existing approaches across all datasets, attaining 99.90% accuracy on CIC-DDoS2019 and maintaining performance above 99.80% on the other benchmarks.

TABLE I. ACCURACY OF ANOMALY DETECTION MODELS ACROSS FOUR BENCHMARK DATASETS

Model	NSL-KDD (%)	UNSW-NB15 (%)	CIC-IDS2017 (%)	CIC-DDoS2019 (%)
Proposed (AE-CNN- FL)	99.85	99.83	99.87	99.90
[9]	99.50	99.48	99.46	99.44
[12]	99.43	99.45	99.46	99.47
[14]	97.30	97.10	97.20	97.00

Table II demonstrates the overall effectiveness of the proposed AE-CNN-FL model, which outperforms competing models across all performance metrics. The model achieved the highest average accuracy (99.86%) and F1-score (99.79%), with a good balance between precision (99.76%) and recall (99.82%). The FAR remained lowest at 0.0011, indicating strong reliability in reducing false alarms in real-time 6G environments.

TABLE II. COMPARATIVE EVALUATION OF ANOMALY DETECTION MODELS

Model	Avg. accuracy (%)	F1-score (%)	Precision (%)	Recall (%)	FAR
Proposed (AE-CNN- FL)	99.86	99.79	99.76	99.82	0.0011
[9]	99.47	98.94	98.9	99	0.0038
[12]	99.45	98.41	99.58	98.34	0.0029
[14]	97.15	94.85	95.1	94.6	0.0047

D. Implications for Cloud Security

Deployment of the framework in a Kubernetes-based cloud pipeline demonstrates its real-world feasibility. Also, explainability modules using SHAP plots and an LLM-driven chatbot improve prediction interpretability. This allows administrators to not only detect and react to threats in real time, but also understand why the model makes decisions, supporting forensic tracking and compliance checks. The integration with cloud-native observability tools like Elasticsearch and Kibana ensures a continuous feedback loop for system performance and threat landscape evolution. Future work will explore integrating split learning and differential privacy, enabling private, decentralized training across

heterogeneous IoT cloud landscapes with intelligent reflecting surfaces [23].

The framework shows high performance but also has limitations, as it relies on regular FL synchronization and aggregation. If clients frequently drop or miss synchronization, model drift and slow convergence may happen. The model defends well against known attacks, but detecting zero-day attacks remains challenging as it depends on historical data. Future work plans to employ stronger adversarial learning techniques to detect such threats early. Another potential failure scenario is data poisoning, where a malicious client sends corrupted data to bias the model. To address this, we plan to implement a robust client reputation and validation mechanism.

IV. CONCLUSION

This work presents an intelligent anomaly detection model tailored for sixth-generation (6G) cloud computing systems, leveraging the strengths of Autoencoders (AEs), Convolutional Neural Networks (CNNs), and Federated Learning (FL). The proposed approach effectively addresses the dual challenges of real-time detection and data privacy. Experimental results across diverse and complex datasets confirmed the model's superiority, achieving a consistent average accuracy of 99.85%, recall of 99.82%, precision of 99.76%, and F1-score of 99.79%. The framework maintained a False Alarm Rate (FAR) below 0.0012 and inference latency under 350 ms, demonstrating both detection accuracy and deployment feasibility in edge-based environments. Its integration with visualization and explainability modules further ensures actionable insights for network operators.

While promising, the framework currently assumes moderate computational resources and periodic connectivity for federated updates. Future research will focus on enhancing energy efficiency, incorporating continuous learning, and supporting dynamic threat adaptation to fully align with the evolving landscape of 6G network security.

REFERENCES

[1] R. Liu, J. Shi, X. Chen, and C. Lu, "Network anomaly detection and security defense technology based on machine learning: A review," *Computers and Electrical Engineering*, vol. 119, Oct. 2024, Art. no. 109581, https://doi.org/10.1016/j.compeleceng.2024.109581.

[2] M. Kim and J. H. Park, "Quantum-resilient security for 6G networks: a comprehensive survey on challenges, solutions, and research opportunities," *The Journal of Supercomputing*, vol. 81, no. 10, July 2025, Art. no. 1132, https://doi.org/10.1007/s11227-025-07651-7.

[3] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, https://doi.org/10.1109/ACCESS.2022.3174679.

[4] G. S. Hukkeri, R. H. Goudar, G. M. Dhananjaya, V. N. Rathod, and S. Ankalaki, "A Comprehensive Survey on Split-Fed Learning: Methods, Innovations, and Future Directions," *IEEE Access*, vol. 13, pp. 46312–46333, 2025, https://doi.org/10.1109/ACCESS.2025.3547641.

[5] A. Blika *et al.*, "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, 2025, https://doi.org/10.1109/OJCOMS.2024.3449563.

[6] T. Senevirathna, V. H. La, S. Marcha, B. Siniarski, M. Liyanage, and S. Wang, "A Survey on XAI for 5G and Beyond Security: Technical Aspects, Challenges and Research Directions," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 941–973, Apr. 2025, https://doi.org/10.1109/COMST.2024.3437248.

[7] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1775–1807, 2023, https://doi.org/10.1109/COMST.2023.3280465.

[8] S. Ahmadi, "Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *Journal of Information Security*, vol. 15, no. 2, pp. 148–167, Mar. 2024, https://doi.org/10.4236/jis.2024.152010.

[9] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, "Anomaly Detection in 6G Networks Using Machine Learning Methods," *Electronics*, vol. 12, no. 15, Aug. 2023, Art. no. 3300, https://doi.org/10.3390/electronics12153300.

[10] N. Nezhadsistani and B. Stiller, "ML-Based Anomaly Detection in 6G Networks: A Survey on the Current Status, Challenges, and Future Directions," in *2024 3rd International Conference on 6G Networking*, Paris, France, 2024, pp. 75–83, https://doi.org/10.1109/6GNet63182.2024.10765631.

[11] B. K. Khare, D. Sahu, D. Pandey, M. Tiwari, H. Kumar, and N. Siddiqui, "Exploring Machine Learning Solutions for Anomaly Detection in 6G Communication Systems," in *Security Issues and Solutions in 6G Communications and Beyond*, D. Pandey, B. Pandey, and T. Ahmad, Eds. Hershey, PA, USA: IGI Global Scientific Publishing, 2024, pp. 230–250, https://doi.org/10.4018/979-8-3693-2931-3.ch014.

[12] H. Alshahrani *et al.*, "Energy aware routing with optimal deep learning based anomaly detection in 6G-IoT networks," *Sustainable Energy Technologies and Assessments*, vol. 60, Dec. 2023, Art. no. 103494, https://doi.org/10.1016/j.seta.2023.103494.

[13] M. M. Kamruzzaman, "6G wireless communication assisted security management using cloud edge computing," *Expert Systems*, vol. 40, no. 4, May 2023, Art. no. e13061, https://doi.org/10.1111/exsy.13061.

[14] G. Han, J. Tu, L. Liu, M. Martínez-García, and Y. Peng, "Anomaly Detection Based on Multidimensional Data Processing for Protecting Vital Devices in 6G-Enabled Massive IIoT," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5219–5229, Apr. 2021, https://doi.org/10.1109/JIOT.2021.3051935.

[15] S. Zhang, Y. Yu, X. Tao, and L. Wang, "Towards Robust Video Anomaly Detection in 6G Networks: A Scene-Adaptive Framework," *IEEE Network*, 2025, https://doi.org/10.1109/MNET.2025.3535760.

[16] J. Shen, R. Tie, Z. Li, B. Liu, Z. Fan, and J. Lu, "Neural Network-Based Log Anomaly Detection Algorithm for 6G Wireless Integrated Cyber-Physical System," *Wireless Personal Communications*, June 2024, https://doi.org/10.1007/s11277-024-11218-9.

[17] S. Alsubai, M. Umer, N. Innab, S. Shiaeles, and M. Nappi, "Multi-scale convolutional auto encoder for anomaly detection in 6G environment," *Computers & Industrial Engineering*, vol. 194, Aug. 2024, Art. no. 110396, https://doi.org/10.1016/j.cie.2024.110396.

[18] N. Mishra and S. Mishra, "NSL-KDD Dataset Analysis: A Machine Learning Implementation to Detect Intrusions in the Computer Network," in *2024 2nd International Conference on Signal Processing, Communication, Power and Embedded System*, Odisha, India, 2024, pp. 1–6, https://doi.org/10.1109/SCOPES64467.2024.10990794.

[19] M. Jouhari, H. Benaddi, and K. Ibrahimi, "Efficient Intrusion Detection: Combining X2 Feature Selection with CNN-BiLSTM on the UNSW-NB15 Dataset," in *2024 11th International Conference on Wireless Networks and Mobile Communications*, Leeds, United Kingdom, 2024, pp. 1–6, https://doi.org/10.1109/WINCOM62286.2024.10658099.

[20] R. Singh and G. Srivastav, "Novel Framework for Anomaly Detection Using Machine Learning Technique on CIC-IDS2017 Dataset," in *2021 International Conference on Technological Advancements and Innovations*, Tashkent, Uzbekistan, 2021, pp. 632–636, https://doi.org/10.1109/ICTAI53825.2021.9673238.

[21] D. Kapil, V. Mittal, and D. Gangodkar, "Evaluating Machine Learning Approaches for DDoS Attack Detection Using CIC-DDoS2019," in *2024 Second International Conference on Advanced Computing &*

Communication Technologies, Sonipat, India, 2024, pp. 762–767, https://doi.org/10.1109/ICACCTech65084.2024.00127.

[22] S. Alqaraleh, "An Efficient Ensemble Network Anomaly Detection System for Cyber-Attacks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 25549–25554, Aug. 2025, https://doi.org/10.48084/etasr.11920.

[23] S. A. Ahmed, E. H. Khalifa, M. Nawaz, F. A. Abdalla, and A. F. A. Mahmoud, "Enhancing Cloud Data Center Security through Deep Learning: A Comparative Analysis of RNN, CNN, and LSTM Models for Anomaly and Intrusion Detection," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 20071–20076, Feb. 2025, https://doi.org/10.48084/etasr.9445.