

Hybrid Intrusion Detection for IOT, 5G/6G, and Cloud Security: Trends, Challenges, and Future Directions.

Kamal Nayanam

HCL Technologies Ltd

knayanam@gmail.com

Abstract: Modern digital services have been transformed by scalable, networked, and data-driven applications made possible by the quick uptake of cloud computing including the Internet of Things (IoT). However, the growing quantity and diversity of cyberthreats have revealed significant security vulnerabilities in these environments, necessitating efficient intrusion detection. An enhanced hybrid intrusion detection framework with superior classification performance is suggested in this study to enhance the detection of hostile network activity. To improve data quality and reduce computational complexity, the suggested approach makes use of extensive data pre-processing, which includes feature selection, class imbalance correction using the Synthetic Minority Oversampling Technique (SMOTE), and data normalization. To take advantage of the deep feature learning capabilities of neural networks and the robust decision-making capabilities of gradient boosting, we use a hybrid classification model that combines a Multilayer Perceptron (MLP) and Extreme Gradient Boosting (XGBoost). Precision, recall, accuracy, F1-score, as well as receiver operating characteristic (ROC) analysis are among the performance criteria used to test the framework on the CICIDS2017 benchmark dataset. When compared to conventional machine learning techniques, the experimental results show that the suggested framework can detect both benign and malicious traffic and produce a better detection result at a lower false positive rate. These findings show that the suggested hybrid architecture is a scalable and effective way to defend cloud and IoT platforms against the constantly changing threats.

Keywords: 5G,6G, Cloud Security, DDoS attack, Federated Learning, IDS, IoT, Machine Learning, SMOTE

INTRODUCTION

The rapid proliferation of cloud-based network infrastructures and Internet of Things (IoT) devices has made it far more difficult to spot illicit network behavior in heterogeneous situations. Because they depend on pre-established attack information, conventional supervised intrusion detection methods are sometimes limited in their effectiveness on emergent or new assault patterns, but they frequently perform well on labeled attack data. The study looks into whether combining supervised classification with anomaly-aware sequence modeling can improve intrusion detection effectiveness in integrated IoT and business network systems. A hybrid intrusion detection method that uses TON IoT datasets and feature-aligned CICIDS2017 is suggested as a solution to this issue [1]. A common traffic-related characteristic, the destination port, the flow time, packet statistics, byte statistics, along with a domain indication were used to create a common cross-domain feature space. The proposed framework combines Random Forest and XGBoost as supervised learning models with an LSTM Autoencoder-based anomaly detection component.

Intrusion detection systems (IDS) are facing new and serious challenges due to the increasing volume of diverse data produced by the Internet of Things (IoT) including industrial cyber-physical devices. Numerous factors contribute to this, such as the massive volume of diverse data that is provided, the quick changes in attack patterns, expensive Edge deployments, and the growing demand for transparency in security assessments derived from AI. Traditional machine learning and deep learning-driven intrusion detection systems (IDSs) are not suitable for real-time, high-fidelity defense approaches because they cannot efficiently extrapolate across multiple domain datasets or capture reliance over time on the temporal dimension, in addition to being less understandable than other forms of defense [2]. Attacks on automated systems are becoming more frequent, sophisticated, intelligent, and widespread, which puts an Internet of Things (IoT) environment at serious risk and calls for costly solutions. In order to defend IoT environments against various kinds of attacks, intrusion detection systems (IDSs) are crucial. However, there are several serious issues

with standard IDS detection techniques, which primarily rely on signatures and rules. Prolonged reaction times, excessive false positive rates, and inadequate detection rates brought on by the incapacity to identify unknown threats are some of these issues. The authors of [3] use convolutional neural networks (CNNs) and feature selection methods for an intrusion detection system (IDS) to offer a new approach to deep learning for binary classification of network traffic (normal vs. attack) within anomaly detection conditions. NIDSs, or network intrusion detection systems, are essential for protecting computer networks. Intrusion detection systems need to get better and more efficient as networks grow and new attacks are created. Automated detection based on anomalies performs better than other detection methods. However, anomaly-based NIDS still struggles to manage enormous volumes of data due to the growing complexity along with frequency of intrusions. Therefore, an intrusion detection system that analyses massive volumes of traffic data must be implemented in order to find a workable solution through classification.

The research conducted by the authors of [4] offers a novel method that uses both machine learning (ML) and deep learning (DL) to increase detection efficiency and ensure reliability. The method optimizes data preparation by utilizing SMOTE for effective data balance and Pearson's Correlation Coefficient (PCC) to feature selection. Machine learning-based intrusion detection systems addressed the expanding security requirements of Internet of Things (IoT) networks, where resource-constrained devices and heterogeneous networks offer an exponentially larger attack surface. Machine learning algorithms were used to train open-source secondary quantitative IoT intrusion traffic data. More than a million flow records with labels covering 34 attack categories, including benign traffic, make up the collection. To identify the various types of intrusions, three supervised machine learning (ML) classifiers—Decision Tree (DT), Random Forest (RF), and Support Vector Machine (SVM)—were trained after a thorough preprocessing that included handling missing values, encoding features, scaling, and eliminating redundancy. The precision, recall, accuracy, along with F1-score of the machine learning models were assessed. The Decision Tree model was judged to be the best, with a respectable performance in common attack classes and an overall accuracy of 99.36%. SVM trailed behind with an accuracy of 80.08% due to computational limitations when handling large volumes of big data, while ccy Random Forest followed closely behind with 99.27%. Using feature-importance analysis, inter-arrival time and total packet size were found to be significant discriminators in hazardous activity. In conclusion, tree-based models—Decision Trees in particular—offer incredibly efficient and comprehensible techniques for ongoing IoT intrusion detection. They also offer possible ways to manage class imbalance and investigate ensemble, lightweight, deep, and standard learning techniques for precise detection of uncommon and unanticipated threats.

By identifying and categorizing attacks in IoT devices for appropriate mitigation, this work advances cybersecurity [5]. These days, the breadth of cyberattacks on the internet of things has gone up dramatically due to the growth of devices connected to it. Therefore, in an internet of things context, it is imperative to create an accurate and efficient intrusion detection system that is quick, dynamic, and scalable. Conversely, fog computing offers a decentralized infrastructure that expands cloud computing to address its fundamental problems. Additionally, to guarantee safe and dependable communication between fog nodes and internet of things devices, a high degree of security is essential. In order to solve this problem, we offer an intrusion detection technique that effectively detects different kinds of network invasions on local fog nodes using artificial neural networks and genetic algorithms. Using this method, we optimized the network's linking weights and individual neuron's biases using evolutionary algorithms. As a result, it can build a back-propagation neural network model fast and efficiently. Additionally, the intrusion detection system can be distributed across local fog nodes with a centralized cloud thanks to the distributed design of fog computing, which results in faster attack detection than the cloud intrusion detection technique. The Raspberry Pi4 was used as a fog node in a number of experiments based on the binary-class classification UNSW-NB15 in addition to ToN_IoT data sets. The outcomes showed that the neural network with optimized biases and weights performed better than those without. The optimized model showed interoperability, scalability, and flexibility. Furthermore, it is reasonable to increase the true positive rate as well as minimize the neural network error rate in an effort to achieve a higher intrusion detection rate. The experiments demonstrate that the suggested approach produces superior outcomes in terms of processing speed and detection precision. In this case, the proposed solution improved convergence process acceleration as well as conserved processing power by reducing execution time for both data sets by 16.35% and 37.07%, respectively, when compared to other state-of-the-art methods [6]. Due to high-dimensional traffic data, extreme class imbalance, and resource constraints among IoT devices, edge gateways, and centralized servers, the fast growth of IoT ecosystems presents serious security challenges. This study presents two correlation-based feature selection models in an effort to improve the stability,

interpretability, and efficacy choices of anomaly-based intrusion detection systems (IDS) in Internet of Things environments. Model B favours non-redundant features with strong discriminative power that reflect network traffic behaviour, while Model A maintains consistent correlated feature clusters because of multicollinearity patterns. Both methods allow for effective IDS deployment under different computing conditions by automating the reduction of the data dimensionality through a correlation-guided thresholding mechanism. An experimental evaluation on the Bot-IoT dataset using a Decision Tree, k-Nearest Neighbors, and Random Forest classifiers with different feature configurations (10, 9, 6, and 3 features) revealed that the proposed models consistently beat baseline feature subsets produced using Principal Component Analysis, Genetic Algorithms, and K-best selection, especially in terms of ensuring balanced detection for typical IoT traffic. With six characteristics, Model A has an MCC of 0.9951 with a macro F1-score of 0.9975. Model B, on the other hand, achieves a macro F1-score of 0.9925 with an MCC of 0.9851 while maintaining good detection performance with just three characteristics. The suggested framework is appropriate for dependable and effective intrusion detection in resource-constrained IoT environments since Model B emphasizes highly differentiated behavioral traffic attributes in order to achieve near-perfect detection with just three features, while Model A is most helpful in intermediate feature spaces by maintaining stable correlated feature clusters [7].

LITERATURE REVIEW

Researchers have recently become more interested in cloud computing, a powerful technology that is mostly used for the distribution of computational resources and other remote services via the Internet. As the demand for cloud services increases, so do the risks, such as vulnerability to cybercrimes that steal private data. The most dangerous online attacks that can interrupt the availability of a service and pose a serious security risk are denial-of-service (DDoS) attacks [8]. There are many studies on data pre-processing techniques to counter DDoS attacks such as cross-correlation for removing redundancies and normalization for providing standardized characteristics. Based on these methods, this paper suggests new approaches using ensemble learning and Particle Swarm Optimization (PSO), which were created especially for DDoS mitigation [9]. The work introduces PSO-Stacking, bagging, and boosting techniques that make use of evolutionary algorithms and enhance machine learning models created on DDoS-related data sources. High-dimensional data typically requires the selection of attributes to minimize the quantity of the data, but it can be challenging to identify the most valuable features. This research uses evolutionary algorithms to optimize the models in order to solve this PSO challenge. PSO-Stacking yields remarkable results: 99.67% when using PSO-Bagging, 99.50% when using PSO-Boosting, and 99.99% when using PSO-Stacking Optimization. Lastly, this research helps identify DDoS attacks, which is a rigorous, precise technique that supports cybersecurity precautions and protects digital infrastructures from such a pervasive threat [10]. Smart environments, which encompass transportation, healthcare, smart buildings, public security, smart parking, smart traffic systems, smart agriculture, and other fields, have greatly improved urban surroundings and human quality of life [11]. They are fully capable of providing citizens with intelligent information and manipulating physical items in real-time. Smart city technologies have the ability to gather personal data. However, there are a number of architectural levels where security and privacy problems could occur [12]. Therefore, it is vital to take these security and privacy issues into account while building and implementing the applications. The article outlines the primary uses of smart cities and discusses the important concerns of security and privacy during the making of the apps. We have examined a number of potential IoT network assaults, shifted our focus to intrusion detection, and emphasized how communication technologies including 4G, 5G, and 6G affect the security and privacy of the IoT ecosystem [13]. Network security depends on intrusion detection, particularly in Internet of Things (IoT) environments where cyberthreats are on the rise. Conventional intrusion detection systems (IDSs) are challenging to identify novel attack types and may generate false alarms. Although metaheuristic optimization can improve feature selection, detection rate, and model complexity, it is not scalable or adaptable to changing circumstances [14]. Deep learning models can concentrate on important traits thanks to techniques inspired by nature. Current approaches struggle to protect the network from various forms of attacks, efficiently adjust to changing assault patterns, and accurately detect shifting attack patterns in IoT networks. The Whale Optimization Algorithm (WOA), Dipper Throated Optimization (DTO), as well as Ant Lion Optimization (ALO) for optimal feature selection are combined with Long Short-Term Memory and eXtreme Gradient Boosting for accurate anomaly detection in this new IoT-aware intrusion detection framework [15]. The proposed method effectively balances exploration and exploitation to select

informative features while the resulting learning models incorporate temporal as well as nonlinear trends in network data. The benchmark datasets NSL-KDD, KDDCup99, CICDDoS2019, as well as NF-UNSW-NB15-v2 are used to test the suggested framework. The suggested framework has been shown to have good detection effectiveness with fewer false alarms. Because it increases processing efficiency while guaranteeing robust detection capability for many threat categories, the suggested architecture is secure and scalable for real-time IoT intrusion detection [16].

Federated learning-based solutions allow several businesses to use their pooled experience to create a machine learning model without sharing any participant's private raw data. The potential for training data spillage in federated learning models, which has been seen in systems employed in image processing, natural language processing, and tabular data, is the main obstacle to wider use. However, it is unclear how such privacy leakage issues can affect intrusion detection systems (IDS) based on federated learning [17]. The study addresses the issue of training data protection in federated learning-driven network intrusion detection systems for the first time by examining the implementations, methods, and constraints of current federated intrusion detection systems [18]. By conducting a thorough analysis of the current state of both federated learning and machine learning-driven network intrusion detection systems, we show that the research community has not thoroughly investigated data leakage attacks on intrusion detection systems derived from federated learning. Finally, the current defense against such attacks is examined, and it is speculated that these strategies might be applied to federated network intrusion detection systems in the future [19]. Privacy-Preserving Federated Learning (PPFL), a recently created approach to intrusion detection systems (IDS), allows cooperative threat detection while maintaining security and reducing direct data exposure. Despite the potential advantages, most FL-based intrusion detection systems are vulnerable to attacks like gradient leakage, poisoning, even model inversion because they lack strong privacy-preserving mechanisms [20].

Current approaches often ignore the need for strict privacy-enhancing techniques in favour of relying on data proximity as an implied privacy warranty. While a number of techniques, such as secure multi-party computation, homomorphic encryption, differential privacy, and safe aggregated data, can provide different levels of security, each has drawbacks with respect of communication costs, model accuracy, and computational efficiency [21]. Designing flexible privacy-preserving systems that solve these problems without compromising IDS responsiveness in real-world deployments is still a major challenge. The adversarial assessment of a privacy-preserving FL-derived IDS is a basic research gap that goes beyond enhancing privacy protections. Many studies assume that FL naturally improves privacy without specifically considering resistance against well-known threats including poisoning in addition to inference attacks. FL IDS technologies are still largely untested against these practical threats in the absence of thorough evaluation frameworks for measuring privacy leakage issues. To render PP-FL systems effective and secure, this gap must be closed [22].s

As the number of IoT devices connected to the cloud infrastructure increases rapidly, security has become more stringent, and traditional intrusion detection systems cannot cope with sophisticated cyberthreats. This research is aimed at designing an intrusion detection system (IDS) for enhancing the security of cloud-based IoT networks by integrating machine learning with traditional ML techniques [23].CNNs and long short-term memory (LSTM) networks are used in the system. Feature encoding, data division, and NSL-KDD dataset normalization were some of the preprocessing techniques used. DoS, Probe, R2L, along with U2R are the four types of assaults included in the dataset. The traffic is tagged as a result. The CNN-LSTM hybrid intrusion detection approach combines CNNs for spatial feature extraction with LSTMs for temporal sequence learning [24]. The approaches are summarised in a tabular format as shown in Table 1.

Table 1. Hybrid IDS methods for emerging 5G and 6G Networks.

Hybrid IDS	Purpose
MLP + XGBoost	Deep feature learning + robust classification
CNN + LSTM	Spatial and temporal feature extraction
CNN + GRU	Reduced complexity with sequential learning
Autoencoder+XGBoost	Feature extraction + attack classification

Autoencoder + MLP	Anomaly detection + classification
Random Forest + XGBoost	Ensemble-based intrusion detection
SVM + Random Forest	Improved decision boundaries
Decision Tree + XGBoost	Fast classification with boosting
CNN + BiLSTM	Bidirectional sequential learning

A Federated Learning-based Hybrid IDS (as shown in Algorithm 1) enables multiple edge devices, base stations, or cloud nodes to collaboratively train an intrusion detection model without exchanging raw network traffic data. Each participating device trains a local model using its own data and periodically sends only the updated model parameters to a central server. The server aggregates these updates to construct a global model, which is redistributed to all participating devices for further refinement. This decentralized learning approach preserves user privacy, reduces communication overhead, and supports real-time intrusion detection across geographically distributed IoT, cloud, and future 6G/7G networks.

Algorithm 1. Federated learning-based IDS.

Input: Local network traffic at edge nodes

Output: Global intrusion detection model

1. Initialize global model
 2. for each communication round do
 3. for each edge device do
 4. Train local IDS model
 5. Send model parameters to server
 6. end for
 7. Aggregate local models
 8. Update global model
 9. end for
 10. Detect intrusion using updated model
-

Hybrid IDS for IoT, Cloud, and 5G/6G Environments

With their unparalleled data rates, low latency, along with multiple device connections, the Fifth Generation (5G) and upcoming Sixth Generation (6G) cellular networks are transforming contemporary wireless communication. Modern developments lead to toxic security scenarios where conventional intrusion detection in addition to defense systems are ineffective. In order to optimize high-speed network security, it suggests a new IDS and IPS system that uses deep learning artificial intelligence in conjunction with anomaly-detection along with signature-matching techniques [25]. Software-Defined Networking is the foundation of another strategy that allows for dynamic security policy enforcement and quick attack response. Based on benchmarks for processing speed and detection accuracy with the lowest false positive occurrence rate, the integrated solution is the most effective for safeguarding next-generation mobile networks [26]. Smart cities, autonomous cars, healthcare, including industrial automation can now connect seamlessly thanks to the development of 6G-equipped Internet of Things (IoT) networks, which have revolutionized communication [27]. 6G-IoT networks are vulnerable to a variety of cybersecurity risks, such as distributed denial-of-service (DDoS) attacks, malware propagation, high spoofing, because of their growing complexity and heterogeneity [28]. Due to their lack of flexibility, traditional intrusion detection systems (IDS) are unable to recognize changing attack patterns. The proposed study presented a novel Stacked-Hybrid Model for detecting attacks in 6G-IoT networks by using random forest (RF),

support vector machine (SVM), logistic regression (LR), and extreme gradient boosting (XGBoost) to improve detection accuracy and robustness. The proposed method reduces computational costs and improves classification performance by using ensemble learning along with feature selection [29]. The method's effectiveness is demonstrated by training and evaluating it using the RT-IoT dataset. The experimental results show that the proposed Stacked-Hybrid Model performs better than individual machine learning algorithms, with a detection accuracy of 99.90% [30]. The other performance metrics of the proposed model that have been evaluated are accuracy, sensitivity, specificity, along F1-score (99.56%, 99.56%, 99.93%, as well as 99.56%, respectively).

A comparison with other models reveals significant gains in identifying complicated and constantly changing cyber threats in 6G-IoT environments [31]. The Internet of Things has emerged as a significant innovation in harnessing the vast potential of wireless media in the real world. We can manage our environment by engaging with many autonomous smart applications operating on diverse platforms globally [32]. The Internet of Things, due to its widespread appeal, sometimes serves as a possible platform for the proliferation of malevolent organizations. By taking advantage of IoT vulnerabilities brought on by different limitations like scarce resources and insufficient security, these groups get access to permitted devices and may launch a variety of assaults [33]. By flooding the communication channel with bogus requests coming from a network of dispersed IoT devices, a Distributed Denial-of-Service (DDoS) attack in an IoT network seeks to jeopardize server availability. Due to recent events including the destruction of multiple well-known servers reported in recent years, defending against DDoS assaults in the Internet of Things has emerged as a crucial area of research. The notion of malware and botnets functioning within "Distributed" Denial of Service (DoS) in the Internet of Things (IoT) is examined in this paper [34].

The diverse DDoS defence strategies are comprehensively outlined and evaluated to discern the existing security vulnerabilities within them. Additionally, we enumerate the unresolved research concerns and obstacles that must be tackled to enhance DDoS defense mechanisms.[35] The significant increase in IoT botnet DDoS attacks in the past decade has become IoT security a paramount problem in the domain of network security. Numerous security strategies have been suggested in this domain; nonetheless, they remain inadequate in addressing newly emerging forms of IoT malware, referred to as Zero-Day Attacks. This study introduces a honeypot-based methodology employing machine learning strategies for malware detection. The data provided by the IoT honeypot serves as a dataset for the efficient and adaptive training of a machine learning model. This strategy serves as a constructive starting point for addressing Zero-Day DDoS Attacks, which have become a significant difficulty in safeguarding IoT against such threats.[36]. Worldwide deployment and regulation of the fifth generation (5G) of wireless communication networks is anticipated to begin in 2020. Massive machine type communications (mMTC), ultra-reliable low latency communications (uRLLC), particularly enhanced mobile broadband (eMBB) are the three main 5G communication possibilities [37]. When compared to fourth-generation (4G) wireless communication systems, the main characteristics include a peak data rate of 20 Gbps, a user-generated data rate of 0.1 Gbps, an end-to-end latency of 1 ms, support for mobility in excess of 500 km/h, a connection density of 1 million devices per km², an area traffic capacity of 10 Mbps/m², threefold spectrum efficiency, and a hundredfold energy efficiency. Several key technologies, including millimeter-wave (mmWave), massive multiple-input multiple-output (MIMO), and ultra-dense networks (UDN), have been proposed to achieve the goals of 5G [38]. 5G communications are now fully standardized, and the infrastructure is being deployed globally. With 86,000 5G base stations dispersed throughout roughly 85 cities, South Korea had emerged as a leader in 5G technology by April 2019. But six cities, notably Daegu, Busan, as well as Seoul, accounted for 85% of the 5G base stations. A standard distributed design using 3.5 GHz (sub-6) spectrum demonstrated data transmission speeds ranging from 193 to 430 Mbit/s [39]. Global connectivity has changed with the introduction of 5G and Wi-Fi networks, which offer faster speeds and lower latency. By promoting faster connectivity, Internet of Things (IoT) integration, real-time data processing, along with innovative applications like telemedicine, autonomous vehicles, and smart grids, these two access technologies are transforming a number of industries, including healthcare, manufacturing, transportation, retail, media, education, and smart cities. But as a result of this expansion, the attack surface has grown significantly, creating serious security problems [40].

Conclusion and Future work.

This article offers a comprehensive assessment of intrusion detection systems (IDS) with an emphasis on Wi-Fi and 5G-specific solutions to detect, contain, and combat new threats in upcoming convergent 5G and Wi-Fi networks. Manufacturers are investigating the intersection of cellular networks and Wi-Fi due of the significant standardized flexibility made about by the introduction of 5G networks. To guaranty that this convergence is achieved, a number of hypotheses have been put forth. These ideas are based on contemporary networking principles, which call for rearranging network components, dividing control and data planes, and deliberately moving resources toward or away from clients. Convergent architectures feature a number of security issues related to the architecture itself, the access norms, including networked models that support these designs, notwithstanding the possible advantages. The amount of data that flows through these networks and the emergence of zero-day infections that utilize the advantage of unknown signatures call for the creation of accurate, quick, and reliable solutions that can identify and stop threats before they spread throughout the network. However, attackers are increasingly using methods to trick IDS models and fabricate input data. Today's techniques are often resource-intensive and manipulable. Future study should focus on employing adversarial machine learning approaches to overcome these limitations. This provides promising avenues for enhancing IDS robustness and performance in combined 5G/Wi-Fi networks.

REFERENCES

- 1.Dunsin, D., Molla, R., & Esfahani, A. (2026). Hybrid Intrusion Detection System for IoT and Cloud Environments. <https://doi.org/10.21203/rs.3.rs-10144004/v1>
- 2.Gupta, S., Verma, D. K., Srivastava, S. K., & Joshi, C. (2026). An Explainable Latent-Attention Hybrid Deep Learning Framework for High-Fidelity Intrusion Detection in IoT and Industrial Cyber Systems. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2026.3701636>
3. Achbarou, O., Datsi, T., & Bourkougou, O. (2025). Enhanced Intrusion Detection System Using Feature Selection and Hybrid Learning Models for High Performance and Efficiency in an IOT environment. *Journal of Engineering Research*. <https://doi.org/10.1016/j.jer.2025.10.016>
4. Hakami, H., Faheem, M., & Ahmad, M. B. (2025). Machine learning techniques for enhanced intrusion detection in IoT security. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2025.3542227>
5. Sharma, V. (2026). A Literature Review For GPT-6 Astra.
- 6.Anand, N., & Kumar, M. (2013, July). Modeling and optimization of extraction-transformation-loading (ETL) processes in data warehouse: An overview. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE. <https://doi.org/10.1109/ICCCNT.2013.6726592>
7. Anand, N., & Sharma, P. (2014). Data Warehouse Security through Conceptual Models.
8. Anand, P. S. N. (2014). Framework for The Integrated And Validated Model of Data Warehouse. *American Journal of Engineering Research (AJER)*, e-ISSN, 2320-0847.
9. Agarwal, S., Singh, A. P., & Anand, N. (2013, July). Evaluation performance study of Firefly algorithm, particle swarm optimization and artificial bee colony algorithm for non-linear mathematical optimization functions. In *2013 fourth international conference on computing, communications and networking technologies (ICCCNT)* (pp. 1-8). IEEE. <https://doi.org/10.1109/ICCCNT.2013.6726474>
10. Anand, N., Singh, K.J. (2024). A Comprehensive Study of DDoS Attack on Internet of Things Network. In: Swain, B.P., Dixit, U.S. (eds) Recent Advances in Electrical and Electronic Engineering. ICSTE 2023. Lecture Notes in Electrical Engineering, vol 1071. Springer, Singapore. https://doi.org/10.1007/978-981-99-4713-3_56

11. Anand, N., Singh, K.J. (2023). An Overview on Security and Privacy Concerns in IoT-Based Smart Environments. In: Rao, U.P., Alazab, M., Gohil, B.N., Chelliah, P.R. (eds) Security, Privacy and Data Analytics. ISPDA 2022. Lecture Notes in Electrical Engineering, vol 1049. Springer, Singapore. https://doi.org/10.1007/978-981-99-3569-7_21
12. Kumar, M., Lal, I.B., Ranjan, R., Kumar, N., Kumar, N., Anand, N. (2025). Optimizing Modulation Schemes for 5G Efficiency Networks. In: Ghonge, M.M., Liu, H., Khan, M., Tran, T.A. (eds) Advances in Emerging Technologies and Computing Innovations. ICETCI 2025. Sustainable Artificial Intelligence-Powered Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-92854-3_39
13. Kumar, N., Asmita, Kaushik, S., Soni, R.S., Verma, R., Anand, N. (2026). Experimental Results Region-Based Convolutional Neural Network Algorithm for Deep Face Detection. In: Udgata, S.K., Mohapatra, D., Sethi, S., Rana, M.E. (eds) Intelligent Systems. ICMIB 2025. Lecture Notes in Networks and Systems, vol 1624. Springer, Cham. https://doi.org/10.1007/978-3-032-05117-2_26
14. Singh, P., Sharma, V., Anand, N., Kundu, R. (2027). A Systematic Analysis of Learning Methods for Privacy Preservation in IoT Environments. In: Roy, N.R., Panda, B., Halgamuge, M.N. (eds) Proceedings of International Conference on Artificial Intelligence and Cyber Security. ICAICS 2025. Lecture Notes in Networks and Systems, vol 2024. Springer, Cham. https://doi.org/10.1007/978-3-032-28379-5_28
15. Nayak, D. *et al.* (2026). A Metaheuristic-Tuned Hybrid IDS for Detecting DDoS Attacks in IoT Networks. In: Swaroop, A., Virdee, B., Correia, S.D., Valicek, J. (eds) Data Processing and Networking. ICDPN 2025. Lecture Notes in Networks and Systems, vol 2005. Springer, Cham. https://doi.org/10.1007/978-3-032-27691-9_11
16. Khan, S., Luo, S., Khan, M. A. A., Munna, M. M. I., Masele, M. P., Zaman, R. S., & Al Shakil, S. (2026). Integrated Fuzzy Trust Management with Federated Machine Learning Approaches for Enhancing Intrusion Detection in IoT Networks. *Internet of Things*, 102013. <https://doi.org/10.1016/j.iot.2026.102013>
17. Kumar, N., Sharma, P., Anand, N., & Dash, J. (2025, April). Frame Encoding Technique by Different Stuffing Approaches. In *Proc. Int. Conf. Advances in Computing, Communication & Networks (ICACCN)*, Bhubaneswar, India.
18. Khraisat, A., Alazab, A., Singh, S., Jan, T., & Jr. Gomez, A. (2024). Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. *ACM Computing Surveys*, 57(1), 1-38. <https://doi.org/10.1145/3687124>
19. Kalodanis, K., Papapavlou, C., & Feretzakis, G. (2025). Enhancing security in 5G and future 6G networks: Machine learning approaches for adaptive intrusion detection and prevention. *Future Internet*, 17(7), 312. <https://doi.org/10.3390/fi17070312>
20. Buyuktanir, B., Altinkaya, Ş., Karatas Baydogmus, G., & Yildiz, K. (2025). Federated learning in intrusion detection: advancements, applications, and future directions. *Cluster Computing*, 28(7), 473. <https://doi.org/10.1007/s10586-025-05325-w>
21. Bunko, T., Johnstone, M.N., Yang, W. *et al.* A survey of privacy-preserving federated learning for intrusion detection systems. *Artif Intell Rev* **59**, 125 (2026). <https://doi.org/10.1007/s10462-026-11519-4>
22. Anand, N., & Kumar, N. Jnyanaranjan Dash. *Dipa Patra: Using ETL for Optimizing Business Intelligence Success in Multiple Investment Combinations*, published in *International Journal of Applied Engineering Research* ISSN, 0973-4562.
23. Anand, N. (2014). The Conceptual Modeling of ETL Processes. *Journal of Global Research in Computer Science*, 5(1), 16-18.
24. Anand, N. (2012). Application of ETL tools in business intelligence. *International Journal of Scientific and Research Publications*, 2(11), 1-4.
25. Anand, N., & Kumar, M. (2013, June). An overview on data quality issues at data staging etl. In *Proceedings of the International Conference on Advances in Computer Science and Application*, Lucknow, India (pp. 21-22).

26. Zitouni, M., Barouni, Y., & Ltifi, H. (2025, October). Intrusion Detection System Based on Federated Learning for Distributed 5G/6G Network Architectures. In *2025 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)* (pp. 1-6). IEEE.
27. Nayak, D., Anand, N., Prusty, T., & Das, S. Transfer learning for corn leaf disease detection: experimental comparison of MobileNetV2 and EfficientNetBO. In *Connecting Intelligence* (pp. 408-412). CRC Press. <https://doi.org/10.1201/9781003773504-69>
28. Verma, R., Kumar, V., Sharma, A., Anand, N., Raj, K., & Kumar, N. (2025, December). Artificial Intelligence Based Image Classification and Compression Technique. In *2025 IEEE International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)* (pp. 1-5). IEEE. <https://doi.org/10.1109/ELEXCOM67950.2025.11451667>
29. Kumari, A., Kumar, P., Nath, T., Mondal, B., Hazra, K., Anand, N., & Kumar, N. (2026). Evaluating a Novel Hybrid Deep Learning Model for Brain Tumor Diagnosis. *Available at SSRN 6062834*. <https://dx.doi.org/10.2139/ssrn.6062834>
30. Sharma, V., Anand, N., Sakshi, S., & Kundu, R. (2026). A Review on Security Challenges in Next-Gen IoT Networks. <https://dx.doi.org/10.2139/ssrn.6729878>
31. Anand, N., Raj, P., Shivam, S., & Sharma, V. (2025, August). A Layer based Aspect of the Security Issues in Internet of Things: An Analytical Survey. In *2025 International Conference on Intelligent and Secure Engineering Solutions (CISES)* (pp. 34-40). IEEE. <https://doi.org/10.1109/CISES66934.2025.11265603>
32. Scalise P, Boeding M, Hempel M, Sharif H, Delloiacovo J, Reed J. A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas. *Future Internet*. 2024; 16(3):67. <https://doi.org/10.3390/fi16030067>
33. Rajesh, K., Vetrivelan, P. Comprehensive analysis on 5G and 6G wireless network security and privacy. *Telecommun Syst* **88**, 52 (2025). <https://doi.org/10.1007/s11235-025-01282-2>
34. Bodade, N. (2023). Security Challenges and Solutions in 5G and 6G Networks. *Available at SSRN 6992939*. <https://dx.doi.org/10.2139/ssrn.6992939>
35. Vishwakarma, R., Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun Syst* **73**, 3–25 (2020). <https://doi.org/10.1007/s11235-019-00599-z>
36. R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1019-1024, <https://doi.org/10.1109/ICOEI.2019.8862720>
37. Mavale, K., Ingle, A., Kshirsagar, K. P., Reddy, C. M., Honawadajkar, P. D., & Marathe, V. M. (2025, August). An Intelligent Hybrid Intrusion Detection and Prevention System for Threat Mitigation in High Bandwidth 5G/6G Network. In *2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 1888-1893). IEEE. <https://doi.org/10.1109/ICSCDS65426.2025.11167585>
38. Sharma, V., Kumari, P., Das, S., Anand, N., & Kundu, R. Energy efficient IoT enabled smart irrigation system leveraging LoRa technology. In *Connecting Intelligence* (pp. 413-418). CRC Press. <https://doi.org/10.1201/9781003773504-70>
39. Nitin Anand, Vatsala Sharma, Pardeep Singh (2025); ETL and Data Warehousing: Architecture, Vulnerabilities, and Security Mechanisms; International Journal of Scientific and Research Publications (IJSRP) 15(10) (ISSN: 2250-3153), DOI: <http://dx.doi.org/10.29322/IJSRP.15.10.2025.p16612>
40. Hamroun, C., Fladenmuller, A., Pariente, M., & Pujolle, G. (2025). Intrusion detection in 5G and Wi-Fi networks: A survey of current methods, challenges, and perspectives. *IEEE Access*, **13**, 40950-40976. <https://doi.org/10.1109/ACCESS.2025.3546338>