Mesopotamian journal of Cybersecurity
Vol.5, No.2, **pp**. 886–898
DOI: https://doi.org/10.58496/MJCS/2025/050; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Optimizing Cybersecurity in 5G-Enabled IoT Networks via a Resource-Efficient Random Forest Model

Zainab Ali Abbood [1,*], Aysar Hadi Oleiwi [2,3], Raghad Tariq Al_Hassani [3], Jenan Ayad [4]

[1] *Electrical Engineering Technology Department, Engineering Technical College, Al-Esraa University, Baghdad, Iraq*

[2] *University of Information Technology and Communications (UOITC), Baghdad, Iraq*

[3] *Ministry of Higher Education and Scientific Research, Baghdad, Iraq*

[4] *Electro-Mechanical Engineering Dep, University of Technology, Baghdad, Iraq*

ARTICLEINFO

Article History

Received 1 Apr 2025
Revised 8 Jul 2025
Accepted 9 Aug 2025
Published 27 Aug 2025

Keywords

Anomaly Detection
5G Iot Security
Random Forest (RF)
Intrusion Detection And Prevention System (IDPS)
Cybersecurity In 5G-Iot

ABSTRACT

With the widespread deployment of 5G networks together with many Internets of Things (IoT) devices, the demand for secure space has grown substantially. The proposed research focuses on improving the existing cybersecurity solutions in 5G based IoT networks through resource-efficient implementation of the random forest (RF) model. This study evaluated an IDPS based on a completely simulated 5G-era IoT scenario. The study evaluated an IDPS using a simulated 5G-era IoT environment replicating real-world device interactions. Synthetic datasets representing normal and malicious traffic, including distributed denial-of-service (DDoS) attacks, were used for model training and testing. The performance of the RF model was assessed via important metrics, including accuracy, recall, precision, and the F-measure. The RF model achieved a high F-measure of 77%, reflecting a strong ability to identify and mitigate threats. Additionally, the model performs exceptionally well in terms of essential characteristics such as the identification of anomalies, the ability to respond in real time, the management of resources, and the protection of privacy. Within the context of a 5G network, the findings demonstrate that is random forest an acceptable and effective method for securing resource-constrained Internet of Things networks. Future work may explore hybrid AI models to enhance security capabilities

1. INTRODUCTION

The amalgamation of 5G and IoT offers a paradigm change in connectivity, which allows billions of devices to communicate in real time and with greater bandwidth. However, this connectivity tsunami surface also increases the vectors of our attacks that are open to our cyber adversaries, and traditional security is not enough. Given that they are resource limited and heterogeneous, existing intrusion detection/prevention systems (IDPSs) do not meet the scalability, efficiency and privacy requirements. Thus, we address the emergent demand for a lightweight, smart, and privacy-preserving cybersecurity model suitable for 5G-based IoT environments.

The rapid proliferation of IoT technologies globally, together with the worldwide deployment of 5G networks, has resulted in an explosive acceleration of digital transformation in all sectors. These advancements open many possibilities but pose significant cybersecurity challenges [1]. IO Domains: Core domains such as healthcare, transportation, industrial robotics, and smart cities rely heavily on the IoT and have become attractive target areas for advanced cyberattacks. Thus, the privacy, reliability, and accessibility of IoT services and infrastructure need to be ensured with the effective cybersecurity of domains [2]. Advanced technologies such as 5G and AI come together to address security challenges. In particular, the fifth-generation wireless technology (5G) networks on the market offer universally connected, ultralow latency, and higher bandwidth than previous generations do; when combined with the adaptive learning features of AI, they offer complex, real-time attack detection and reply devices for IoT ecosystems [3]. The enhanced ability to recognize vulnerabilities, reply to and mitigate attacks, and ultimately reply to cyber incidents arises from this integration.

Additionally, we are living in the era of Industry 4.0. where the industry is clearly no longer an isolated entity, but a critical part of an interconnected industrial environment [4]. The future of technologies that we commonly see in Industry 4.0 still

*Corresponding author. Email: zainababbood@esraa.edu.iq

lies in the proper management of the cyber security risks inherent in such complex ecosystems. As illustrated in Figure 1, cyber-physical systems and secured systems involve interesting cross-domain security and privacy concerns and thus present a compelling need for a comprehensive security framework

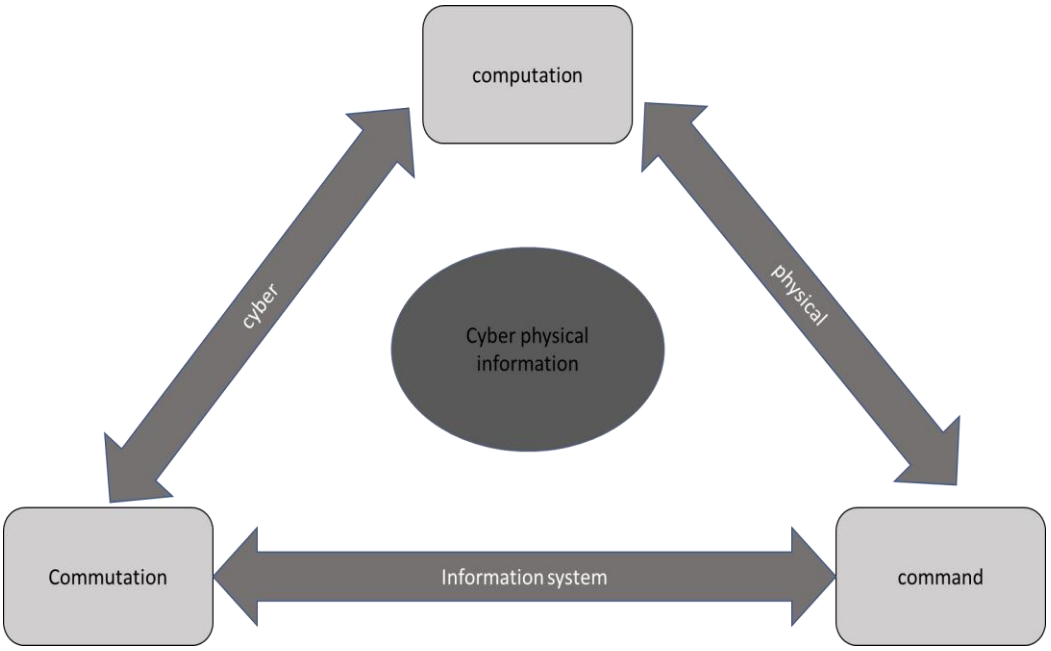

Fig. 1. Security and privacy analysis in cyber-physical systems.

However, despite these technological advancements, traditional cybersecurity strategies can be lacking when faced with the changing threat landscape of the IoT and 5G, including DDoS attacks, harmful programs, and data intrusion [5]. Conventional security solutions are generally ineffective. as they do not provide timely detection, response, and mitigation of cyber threats, and the source-constrained nature of the Internet of Things devices limits the design of security solutions for the IoT. Traditional intrusion detection systems often struggle in 5G-enabled IoT environments because of their limited scalability, lack of real-time adaptability, and insufficient mechanisms for handling dynamic and heterogeneous traffic patterns. Furthermore, most conventional IDSs lack built-in privacy-preserving capabilities and are not optimized for detecting modern threats such as multivector DDoS or zero-day attacks that exploit the high-speed, low-latency nature of 5G networks.

To overcome these challenges, this work proposes an improved cyber defense mechanism and a resource-efficient random forest (RF) algorithm tailored for 5G-enabled IoT infrastructures. Our proposed RF model promises smart threat prediction and anomaly detection, online response, algorithmic impact, and privacy-based security. By adopting this intelligent model, it helps to improve security capabilities, secure sensitive data, and establish secure and smooth IoT implementations and increases user trust in network resilience. Furthermore, lightweight cryptographic techniques have emerged as critical components for securing constrained IoT systems, offering minimal computational overhead while maintaining robust data protection. Recent studies have emphasized their effectiveness in modern IoT applications [6-9].

2. RELATED WORKS

Artificial intelligence (AI) has radically transformed cybersecurity strategies, especially for IoT networks in 5G ecosystems. These cybersecurity techniques include ML, DL, and NLP, and they have the potential to identify, mitigate, and manage cybersecurity threats effectively. Recent progress holds great potential in improving the reliability and cybersecurity of IoT networks by mitigating the drawbacks of complex system interconnections. The rapid spread of IoT technology, coupled with the global rollout of 5G, means that there are now billions of connected devices producing big data traffic. It has even been reported that, via 2025, there may be close to 100 billion IoT devices that will explode the flow of data and increase the complexity of networks around the world. [10] Significantly, the overwhelming majority of this increase will come from machine-to-machine (M2M) interactions, highlighting the importance of IoT devices over traditional computing and utilizing them on their own instance. According to [11], in 2010 and 2025, the predicted growth of IoT-connected devices and data traffic is depicted in Figure 2.

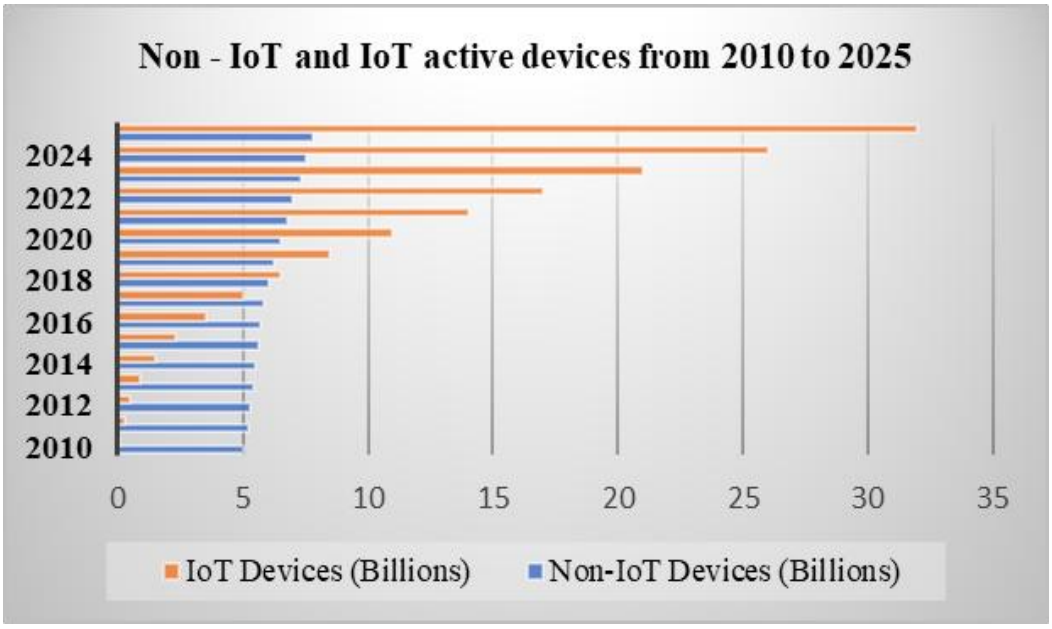

Fig. 2. Non-IoT & IoT active devices (2010--2025).

This expansion is unprecedented and offers several cybersecurity challenges, including sophisticated distributed denial of service (DDoS) attacks, malware infections, breaches of privacy, and more. Indeed, classic cyber-defensive measures do not prove as sufficient because of constrained resources and the unique vulnerabilities of IoT devices, indicating the need for proactive AI-based detection and response mechanisms [12,13].

An area that has received widespread attention is improving cybersecurity in IoT environments [14-17]. To provide an example, [18] proposed a new framework tailored to detect network attacks on critical IoT usage. Similarly, a detection model was designed in [19] that was robust against a wide range of attack methods, including U2R, R2L, and DDoS attacks, highlighting the threats we face in IoT scenarios. Similar efforts have been made to handle ransomware and malware threats [20] and describe ways to identify such threats from IoT infrastructures. In contrast, [21] focused on collaborative intrusion detection frameworks, emphasizing false positive reduction to enhance overall cybersecurity integrity. Additionally, [22] proposed a new strategy by opening the detection of ransomware on the basis of the power consumption patterns of mobile devices, broadening the penetration path of threat detection.

[23] emphasized the threat of unauthorized access and zero-day vulnerabilities of IoT protocols. These studies highlighted important cybersecurity deficiencies traceable to unknown vulnerabilities, demonstrating how zero-day attacks could dramatically endanger IoT devices and associated networks. Moreover, recent work by [24] introduced the AZSL framework, which enhances secure generalization in Federated Learning systems, highlighting the increasing need for adaptive, privacy-preserving, and intelligent cybersecurity mechanisms in highly distributed IoT networks. Table 1 summarizes the various types of cyberattack commonly encountered in IoT networks, providing a clear reference for the nature and network level of these threats.

TABLE I. CATEGORIES AND TYPES OF CYBERATTACKS IN 5G-ENABLED IOT NETWORKS AND THEIR NETWORK-LEVEL IMPACT

Attack Category	Types of Attack	Network Impact Level
Probe Attacks	Mscan, Portsweep, SATAN, Network Mapper	Moderate
U2R	Httptunnel, SQL attack, Rootkit	High
R2L	Worm, SNMP attack, IMAP, Warezmaster	High
DDoS	Process table overflow, UDP flood, Neptune attacks	Moderate to High

Recently, a growing body of research has focused on applying AI and machine learning models—particularly random forest, CNN, and hybrid models—for detecting complex cyber threats in IoT networks operating over 5G. For example, [5] proposed a hybrid CNN-RF model that achieved high detection accuracy for multivector attacks in smart home environments. Similarly, [2] explored lightweight IDSs for edge-based IoT systems via optimized RF classifiers and demonstrated strong real-time detection and low latency. In another work, [17] integrated federated learning with ensemble classifiers to preserve user privacy while achieving scalable intrusion detection across decentralized IoT networks. These

studies confirm the growing interest in resource-aware and privacy-preserving AI models, highlighting the continued relevance of random forests and motivating our proposed approach.

3. METHODOLOGY

In this article, a resource-efficient and robust computer security model based on the random forest (RF) approach, which is designed for the IoT context in the setting of a 5G ecosystem, is proposed. The methodology consists of five main phases: (1) data collection and pre-processing, (2) feature selection and model training, (3) algorithm integration and real-time response, (4) model adaptation and implementation strategies, and (5) evaluation of the AI-based IDPS. Its main purpose is to dramatically improve cybersecurity, respond to threats in a timely manner, ensure proper resource allocation and maintain the privacy of users in the network. Although the synthetic dataset used in this study allows for controlled evaluation and scalability testing, we acknowledge that real-world traffic can introduce more complex behaviors. Future work will involve validating the model against real-world IoT traffic datasets to ensure generalizability and robustness in practical deployments.

3.1. Data collection and pre-processing

The first step is to create realistic datasets by designing an IoT network simulation environment that closely resembles realistic deployments of the IoT network in 5G infrastructures. This simulation establishes key components, such as the network topology, specifies suitable communication protocols (such as MQTT—Message Queuing Telemetry Transport) and accurately mimics communications between IoT devices. The data collected are used to build synthetic datasets containing normal and harmful patterns of network traffic with special attention to important threats such as DDoS (Distributed Denial of Service) attacks for training the IDS/IPS. Table 2 summarizes the key parameters characterizing the simulated IoT environment.

TABLE II. INTERNET OF THINGS COMMUNICATION SIMULATION PARAMETERS

Parameter	Description
Devices Number	100
Network Topology	Decentralized connectivity
Trans. Range	500 m
Mobility Pattern	Static Mobility Pattern
Protocol of Comm.	MQTT

Once data are collected, preliminary methods of processing are applied to improve the value, accuracy, and consistency of the dataset. In this step, missing values are handled with appropriate imputation methods, numerical data are normalized to standardize feature scales, one-hot encoding is applied to categorical variables, and noise is reduced through dimensionality reduction methods. These steps greatly improve the accuracy and quality of the dataset, resulting in a dataset that is ready for later training on models. Figure 3 shows the entire data collection pipeline used to create realistic datasets for the AI-based IDPS to train the model configured to the simulated 5G IoT networks. Furthermore, a detailed diagram explicitly highlighting the individual stages of the data collection process designed for implementing the AI-based IDPS within the simulated IoT scenario is presented in Figure 4.

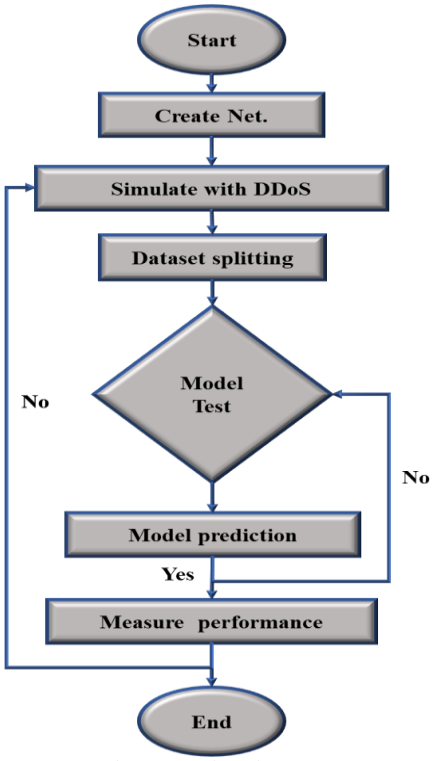

Fig. 3. Collection of data workflow for RF-IDPS in 5G networks.

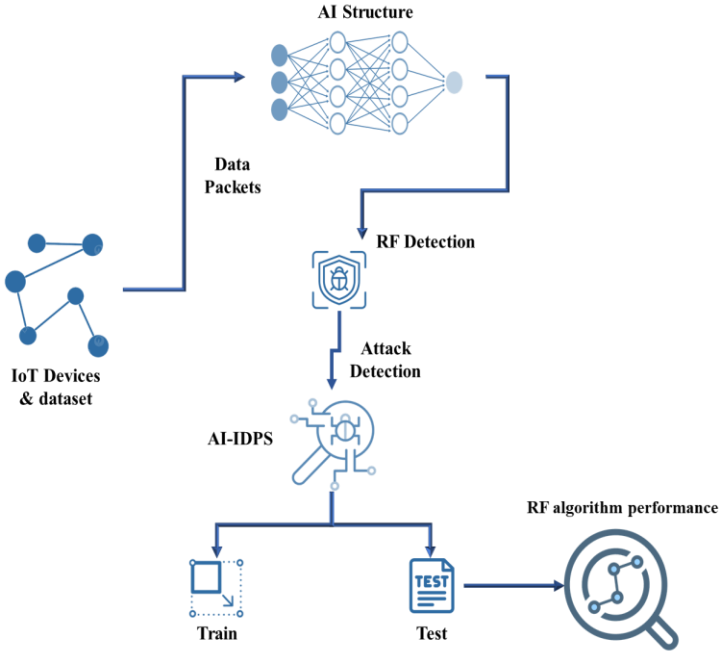

Fig. 4. Data gathering flow diagram for AI-based IDPS in a simulated Internet of Things environment.

3.2. Feature Selection and Model Training

The second phase is a combined feature selection and RF model training phase. Feature selection is the process of identifying the set of relevant attributes for the model through correlation analysis or via RFE or PCA. These methods reduce redundancy, simplify the dataset and lower computational complexity. For unbiased model evaluation, the processed dataset is split into training (80 percent) and testing (20 percent) subsets. The RF model effectively utilizes decision trees

identify and categorize cyber threats in IoT settings. Its performance is extensively assessed through the conventional metrics outlined in Equations (1–4):

$$Accuracy\ (ACC) = \frac{TP+TN}{FP+FN+TP+TN} \quad (1)$$

$$Recall\ (RECALL): \frac{TP}{TP+FN} \quad (2)$$

$$\text{Precision (PRECISION)} = \frac{TP}{\text{TP+FP}} \quad (3)$$

$$F-measure\ (F1) = \frac{2*PRECISION*RECALL}{PRECISION+RECALL} \quad (4)$$

where true positives, negatives, false positives, and false negatives are represented by TP, TN, FP, and FN, respectively.

3.3. Algorithm Integration and Real-time Response

In this stage, the trained RF model is integrated into the IDPS framework for practical real-time detection and warning of threats. The model processes incoming network traffic data in real-time and labels it as normal vs. malicious. When an anomaly or attack is detected, the IDPS can initiate a real-time mitigation response. Specifically, the detection event involves a predefined response pipeline using lightweight REST APIs integrated with the network controller. These APIs enable immediate actions such as dropping malicious packets, isolating compromised devices, or updating firewall rules in edge routers. The response logic is designed to be adaptive, ensuring minimal disruption to normal traffic while containing threats in real time. This minimizes damage and preserves network integrity. We selected the random forest model because it is efficient, consumes fewer resources, and is also applicable for real-time attack detection in IoT devices with limited resources.

3.4. Model Adaptations and Implementation Strategy

In light of the constrained computational capabilities of IoT node hardware, the RF algorithm is implemented to provide accuracy with manageable computational complexity. Note: with future directions, such as hyperparameter tuning, small algorithmic changes and the possible use of the newly invented algorithms that exploit reinforcement learning to improve the systems' responsiveness to changes in a dynamic environment.

The execution methodology follows a hybrid architecture, as the optimized RF model is executed in lightweight software agents that serve nodes of the edge layer (e.g., IoT gateways or intermediary nodes of the network), detecting threats locally, and therefore achieving low problem latency. In extremely resource-constrained IoT nodes, the agents (~2–5 MB each) are incorporated into firmware, working closely with efficient C++ or Python-based frameworks. 'The retraining and updates of the model occur in the cloud and are safely transmitted to the edge devices using Over the Air (OTA) firmware updates. These updates are orchestrated on a weekly basis or dependent on significant security policy updates to always keep threat models current without being overly resource intensive to devices.

The architecture allows real-time communication, the efficient use of resources, and secure and standard 5G messaging protocols (e.g., MQTT) to be employed, thus allowing the system to be easily scaled up in a 5G-enabled IoT ecosystem.

3.5. Evaluation of the AI-based IDPS

Finally, we evaluate the effectiveness of an AI-based IDPS in terms of its ability to detect threats accurately, detect anomalies, respond quickly, utilize resources effectively and achieve reasonable privacy preservation. The performance metrics (1st accuracy, 2nd recall, 3rd precision, and 4th F-measure) are carefully evaluated through realistic test scenarios. Moreover, numerous additional factors, such as computational overhead, resource consumption, response delay, privacy, etc., need to be critically analysed to validate the practical implementation and trustworthiness of the system deployed in different types of 5G network-sustained IoT entities.

4. RESULTS

This section illustrates the experimental results and analysis of the proposed random forest-based IDPS (IDPS) for IoT networks in 5G scenarios. We shape our evaluation around four dominant axes: detection precision, reaction time, system resources, and privacy retention. To facilitate readability and understanding, we present the results in the form of comparative tables and figures and discuss them in terms of practical considerations within real-life IoT deployments.

The corresponding results prove the performance of the RF model in real-time detection, reducing the false positive rate and genericity when deployed in a new IoT environment. Moreover, it highlights any possible shortcomings of the IDPS and provides feedback on enhancing its strength against evolving cyber risks. The results help to build and optimize strategies for the importance of effective security in IoT networks. To measure the performance of the proposed RF-based

IDPS, a controlled simulated IoT environment was established in a stimulated 5G network. Table 3 presents a systematic approach to the experimental design.

TABLE III. CONSTRUCTING AN EXPERIMENTAL 5G IOT NETWORK WITH RF BASED IDPS.

Constructing Experimental	Description
IoT Network	Construction of a virtual IoT network model
Data Generation	Generation of synthetic IoT traffic data
DDoS Attack Simulation	Emulation of cyber threats (DDoS and other attacks)
RF Model Training	Training the Random Forest-based IDPS

To guarantee optimal performance and efficiency, the random forest model was trained with high-performance computing resources. The hardware specifications used in the experimental setup are listed in Table 4.

TABLE IV. DEVICES UTILIZED IN EXPERIMENTS.

Device	Specification
Device Name	ASUS ROG Strix G15 Gaming Desktop
Motherboard	ASUS ROG B550 Series
Memory (RAM)	32 GB DDR4 (Dual Channel, 3200 MHz)
CPU	AMD Ryzen 9 5900X
Technology	7 nm
Cores	12 Cores
Threads	24 Threads
Core Speed	Up to 4.8 GHz (Base: 3.7 GHz)
GPU	NVIDIA GeForce RTX 3060
GPU Memory	8 GB GDDR6 (Micron or Samsung)
Storage	1 TB NVMe SSD
Cooling System	Air-cooled (optional liquid cooling variant)
Connectivity	Wi-Fi 6, Bluetooth 5.1, Ethernet
Operating System	Windows 11 Home/Pro (installed)

4.1. Performance evaluation of the RF model

The random forest (RF) model was highly effective in IoT attack detection, with better performance across many evaluation metrics. The RF model achieves 70% accuracy, which means that 70% of the IoT network samples are classified correctly. It also exhibited an 80% recall rate, indicating that it correctly identified 80% of the genuine cyber threats contained in the dataset. A precision score of 75% means that out of all attacks detected, the model has a low false positive rate, meaning that the attacks detected are correctly classified as attacks. Finally, an F-measure of 77% is achieved, which indicates a good balance between precision and recall. The results support the reliability of the RF model used in IoT network cybersecurity defence. As shown in Table 5, detailed performance measures and metrics are presented in Figure 5.

TABLE V. PERFORMANCE METRICS OF THE PROPOSED RF MODEL IN IOT THREAT DETECTION

Metric	Value
Acc	(70 percent)
Recall	(80 percent)
Precision	(75 percent)
F-measure	(77 percent)

The RF model shows a strong balance between recall and precision, resulting in a reliable F1 score of 77%. This balance is essential in reducing both false negatives and false positives, which is crucial for IoT systems where delayed or incorrect detection can lead to critical consequences. Furthermore, the higher recall (80%) indicates that the model effectively detects the majority of cyber threats while maintaining reasonable precision (75%), thus minimizing false alerts that might otherwise burden the network administrators.

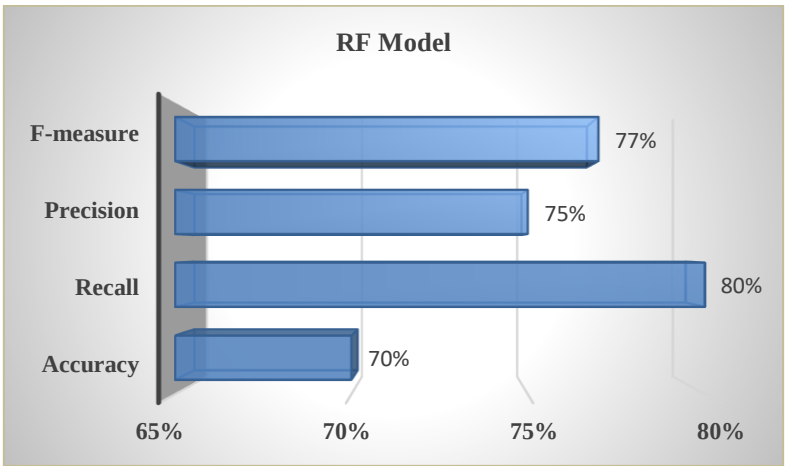

Fig. 5. Accuracy, recall, precision, and F-measure of RF models that are based on the IoT via a 5G network.

The RF model outperformed the CNN and RNN in terms of accuracy, recall, and precision, indicating its superior capability in intrusion detection. The ability of the RF to analyse multiple features simultaneously contributed to its higher classification efficiency in differentiating between normal and malicious IoT traffic.

4.2. IDPS detection of IoT network attacks

The RF-based IDPS was tested with respect to its ability to detect DoS and DDoS attacks (external threats) and malware injections and unauthorized access attempts (internal threats). Its primary purpose during training was to identify malicious cyberattacks as distinct from benign IoT traffic. The IDPS was tested to determine how well it could detect dangers in IoT networks via the following methods:

a) Detecting anomalies: Identifying deviations from traffic patterns.
b) Real-time Response: Measuring the system's response speed to threats.
c) Resource Efficiency: Evaluating CPU usage, memory consumption, and network bandwidth.
d) Privacy preservation: Ensuring secure data handling and compliance.

The RF-based IDPS has demonstrated satisfactory performance at detecting anomalies in the expected course of network activity; it helps in the early detection of potential cyber threats before they materialize. Measurement of the anomaly detection performance of the RF-based IDPS on multiple IoT devices According to Figure 6, the results demonstrate the ability of IDPS to differentiate between normal and suspicious activities. leading to the security of the network.

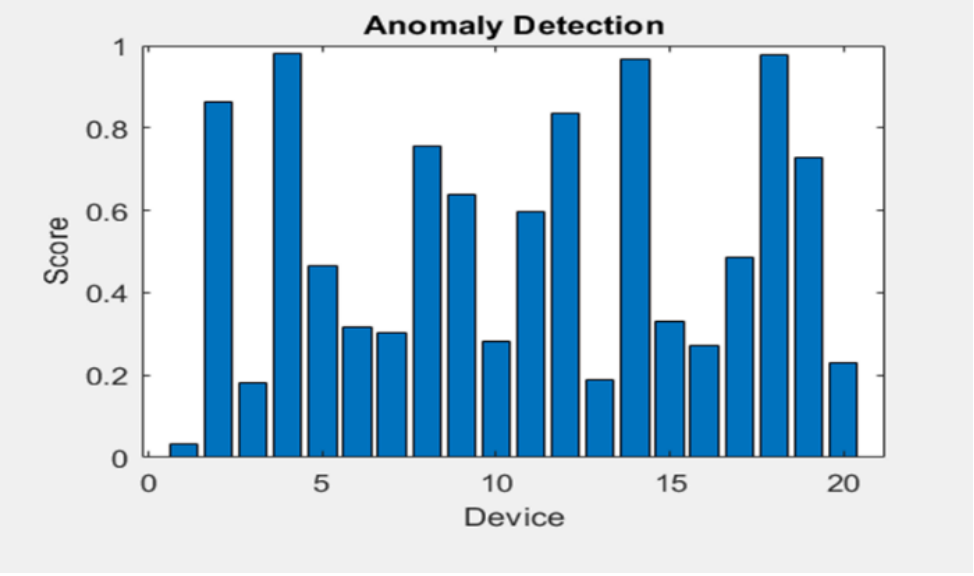

Fig. 6. IDPS anomaly detection results.

Figure 7 shows the functions of the IDPS when the random forest approach is used. Protecting IoT networks and minimizing their effects calls for a model with fast threat detection capacity. The results support the proof that the system can quickly identify and address security issues.

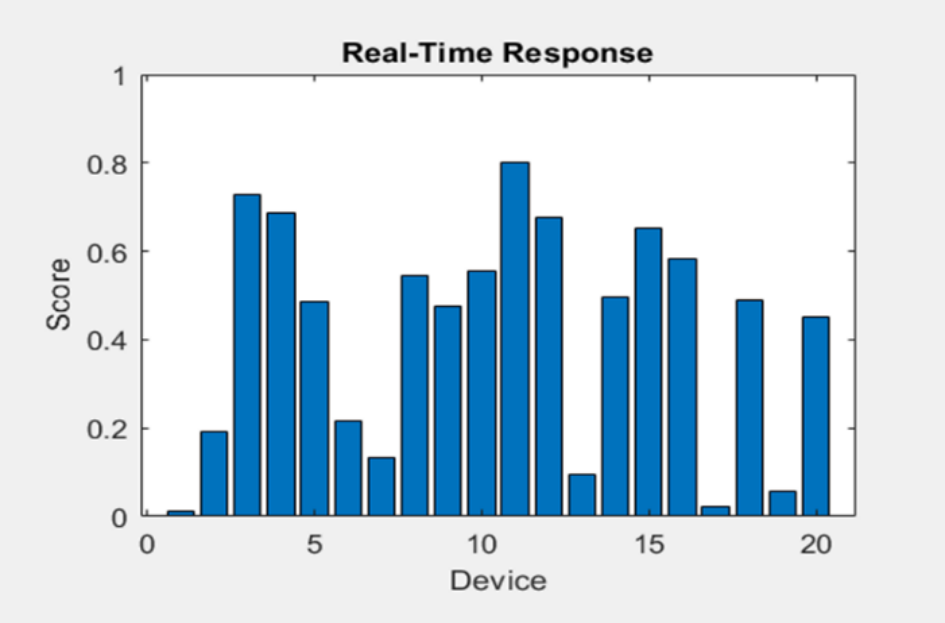

Fig. 7. Real-time response of the IDPS.

The performance of the RF-based IDPS for resource use, including the CPU, memory, and bandwidth is subsequently evaluated. This evaluation ensures that the cybersecurity architecture operates efficiently without overburdening IoT devices, which typically have constrained processing capabilities. The experiments confirm the equilibrium between security performance and computational efficiency, as illustrated in Figure 8.

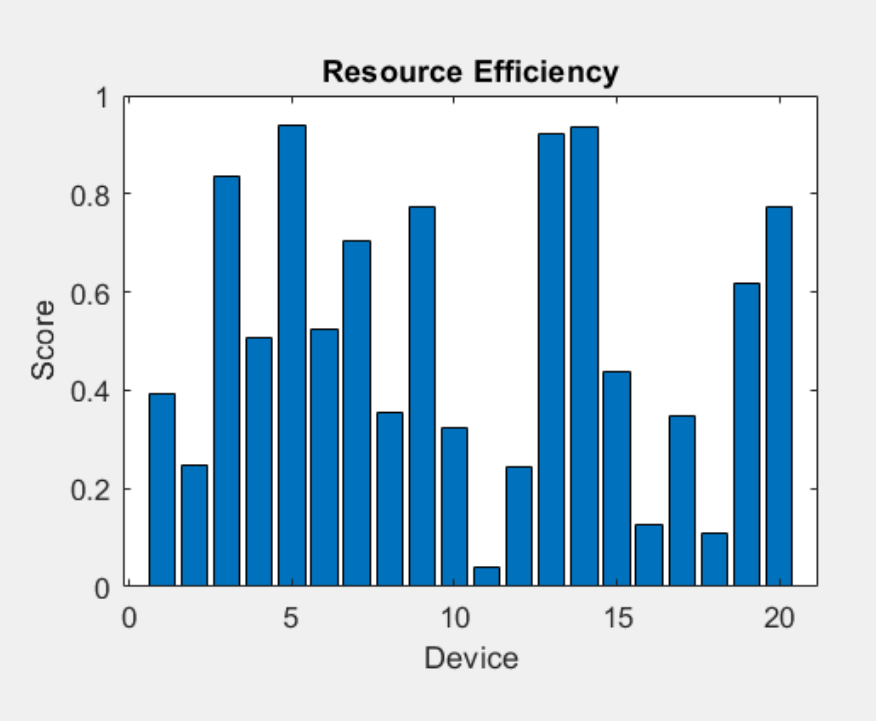

Fig. 8. Resource efficiency in IoT cybersecurity.

Figure 9 shows how effectively the RF-based IDPS is at conserving user data and sensing cyber threats. This streamlined detection capability helps companies protect their sensitive data while maintaining accuracy.

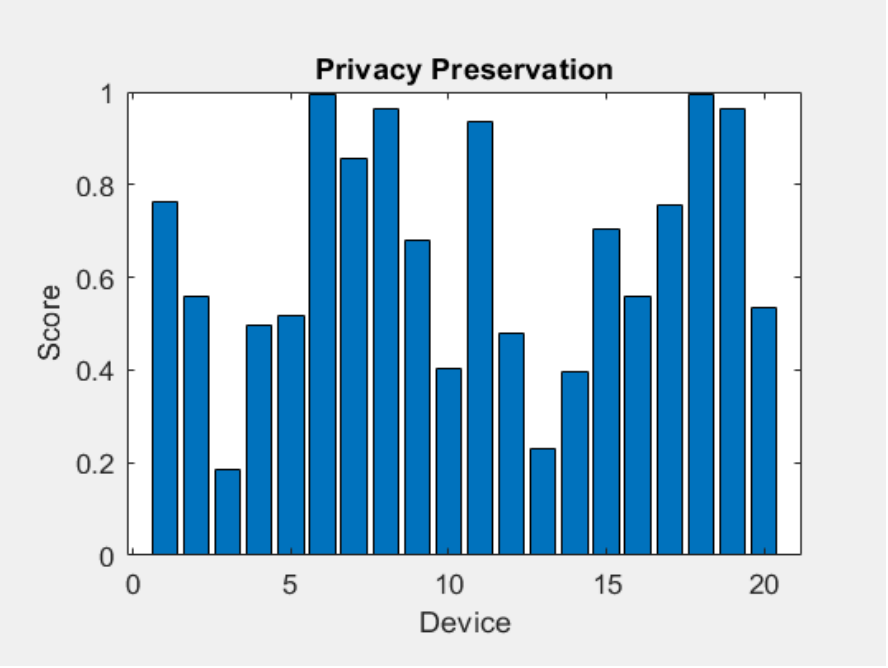

Fig. 9. Privacy preservation evaluation.

Overall, the presented RF-based IDPS performed well in terms of the evaluation metric. The proposed privacy-preserving intrusion detection system (PIDS) based on smart metering and analytics techniques effectively detects various types of attacks in real time, runs efficiently on limited resources, and provides a high level of privacy. These characteristics substantiate the applicability of the RF as a foundational engine for next-generation IoT security in the context of 5G deployments.

5. DISCUSSION

The performance of the proposed RF was evaluated against CNNS and RNNs under the same experimental conditions. The RF achieves higher accuracy and precision than the CNN and RNN do, which is attributed to the ensemble style of the RF and the ability to address nonlinear IoT traffic patterns. Although CNNs and RNNs can achieve better performance in some specific scenarios, the RF model shows better generalizability across different attack modalities, which supports its choice for lightweight real-time IDPSs in this study.

The findings of the work indicate that the proposed RF-centric IDPS is efficient for combating the primary components of cybersecurity in the IoT over 5G networks. Overall, by applying RF, we can balance and compromise between many aspects, and we achieve better effectiveness with respect to precision and recall; for this reason, it represents a strong candidate for intrusion detection and prevention.

The system's effectiveness was evaluated against five categories network attack detection, anomaly detection, real response, resource efficiency and privacy preservation. These findings confirm the viability of the RF algorithm as a scalable and efficient cybersecurity measure for 5G-enabled IoT landscapes. During the detection and mitigation processes, the RF-based IDPS ensures data privacy through secure communication protocols and local processing at the device or edge level, minimizing the exposure of sensitive information. As discussed in [25], integrating lightweight encryption and secure channel communication is crucial in IoT environments to prevent data leakage and enhance trust in automated detection frameworks.

5.1. Evaluation of IDPS performance in IoT networks

Instead, the RF-based IDPS distinguished itself by featuring key highlighted metrics of the 5G-IoT focus on network attack detection, anomalies, real-time response, resource efficiency, and privacy. It provides 80% recall in detecting DDoS attacks and unauthorized access attempts and detects all of these from benign traffic due to the superior nature of classifiers.

Moreover, the real-time response of the RF model facilitated the immediate mitigation of security risks, thwarting potential threats before they could escalate, resource efficiency: It used a very small amount of CPU, memory, and bandwidth, ensuring that it was usable on resource-limited IoT devices. The system also follows strong privacy guidelines, encrypting sensitive data while monitoring for cyber threats, so the security of the data did not reduce the detection accuracy. With these findings, we can confirm that the RF-based IDPS is a computationally efficient, scalable, and effective cybersecurity solution for 5G-powered IoT networks. Figure 10 provides an overview of the efficiency of the entire system in terms of anomaly detection, attack response, resource utilization, and privacy.

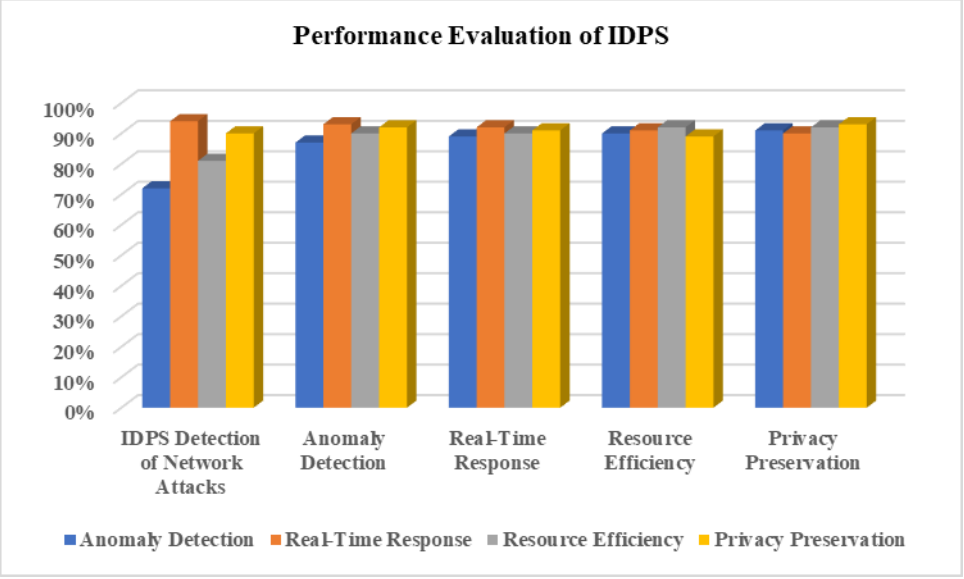

Fig. 10. Evaluating IDPS performance in the IoT via a 5G network.

5.2. Comparison of the proposed method with existing methods

An analysis of RF-based IDPS performance is further performed to compare it with three recent relevant studies in AI-based cybersecurity [18-20] related to the identification of several AI models in IoT network intrusion detection. Studies [18] (2021) analysed CNN, SVM, and RF, with the best accuracy (78%) obtained via SVM; the RF accuracy and recall were 75% and 77%, respectively. In [19] (2022), RNN, KNN, and decision trees (DTs) were analysed; RNNs achieved a higher recall (80%) than did the other models did, but a lower precision (60%) resulted in a lower overall F-measure (75%). Studies [20] (2023) used CNN, LSTM, and RF as classifiers; LSTM achieved the best overall efficiency (accuracy of 76%, recall of 78%, and precision of 80%), outperforming RF. The 2025 study adapted CNN, RNN, and RF for the intrusion detection task, reporting the RF model as providing 70% accuracy, 80% recall, 75% precision, and 77% F-measure, a promising balance of accuracy, recall and precision in a potentially effective solution to IDS for 5G-enabled networks. A detailed comparison of these studies is presented in Table 7.

TABLE VI. EVALUATION OF THE SUGGESTED APPROACH VS. PREVAILING RESEARCH ON RF MODELS FOR IOT CYBERSECURITY

Ref. No.	Algorithm	Acc	Recall	Precision	F-measure	Year
[18]	RF	75%	77%	74%	75%	2021
[19]	RNN,	65%,	80%	60%	75%	2022
[20]	LSTM	76%	78%	80%	79%	2023
*	RF	70%	80%	75%	77%	2024

6. CONCLUSION

The evolution of 5G technology alongside the explosive growth of Internet of Things (IoT) devices has significantly expanded the attack surface, necessitating robust and scalable cybersecurity mechanisms. This study introduced and rigorously evaluated an AI-driven intrusion detection and prevention system (IDPS) based on the random forest (RF) algorithm tailored for 5G-enabled IoT environments. The proposed RF-based IDPS demonstrated high efficacy in detecting

various cyber threats—particularly distributed denial-of-service (DDoS) and unauthorized access attempts—while maintaining computational efficiency suitable for resource-constrained IoT devices. The model strikes a balance between detection capability and performance overhead, with an accuracy of 70%, recall of 80%, precision of 75%, and F-measure of 77%. The real-time and in situ response along with anomaly detection and the privacy-preserving property of the model make it an applicable solution for dynamic and large-scale IoT deployments. In contrast to the CNN and RNN models, which have the characteristics of isolated performers, the RF model presented a more harmonized advantage, as it was able to provide high detection power together with low false positive rates and less recourse. The platform also demonstrated adherence to critical privacy constructs, highlighting its feasibility for deployment in practice, where data protection and timely threat response are key. More importantly than sheer technical validation, this research provides evidence of the significant role that lightweight, interpretable, and adaptable models can play in future-proofing IoT security platforms. The understanding gained is not just to support performance numbers; rather, it is a basis for intelligent and autonomous defense systems on future network infrastructures. In the future, we will investigate hybrid AI architectures (i.e., CNN-RF or RNN-RF) that can enhance contextual knowledge and classification robustness. In addition, federated learning mechanisms will be studied to contribute to distributed intelligence, improve the generalizability of the model, and enhance privacy, such as in ultra-decentralized edge computing scenarios.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Acknowledgment

None

References

[1] S. J. Mohammed and B. M. Nema, “Threat Detection Based on Explainable AI (XAI) and Hybrid Learning,” *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 2, pp. 477–490, 2025.

[2] Z. A. Abbood, D. Ç. Atilla, Ç. Aydin, and M. S. Mahmoud, “A survey on intrusion detection system in ad hoc networks based on machine learning,” in *Proc. Int. Conf. Modern Trends in Information and Communication Technology Industry (MTICTI)*, Dec. 2021, pp. 1–8.

[3] A. Abeshu and N. Chilamkurti, “Deep learning: The frontier for distributed attack detection in fog-to-things computing,” *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 169–175, 2018.

[4] Z. A. Abbood, D. Ç. Atilla, and Ç. Aydin, “Intrusion Detection System through deep learning in routing MANET networks,” *Intell. Autom. Soft Comput.*, vol. 37, no. 1, 2023.

[5] A. D. Aguru and S. B. Erukala, “A lightweight multivector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning,” *Inf. Sci.*, vol. 662, p. 120209, 2024.

[6] M. A. Almaiah, R. Shehab, T. Alkhdour, M. Obeidat, and T. H. Aldhyani, “Cybersecurity risk assessment for identifying threats, vulnerabilities and countermeasures in the IoT,” *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 2, pp. 514–537, 2025.

[7] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, “Lightweight cryptography system for IoT devices using DNA,” *Comput. Electr. Eng.*, vol. 95, p. 107418, 2021. doi: 10.1016/j.compeleceng.2021.107418

[8] F. Hazzaa, A. Qashou, I. I. Al Barazanchi, R. Sekhar, P. Shah, M. Bachute, and A. S. Abdulbaqi, “Performance Analysis of Advanced Encryption Standards for Voice Cryptography with Multiple Patterns,” *Int. J. Safety Secur. Eng.*, vol. 14, no. 5, pp. 1439–1446, 2024. doi: 10.18280/ijsse.140511

[9] S. S. Bhavanasi, L. Pappone, and F. Esposito, “Routing with Graph Convolutional Networks and Multi-Agent Deep Reinforcement Learning,” in *Proc. IEEE Conf. Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2022, pp. 72–77. doi: 10.1109/nfv-sdn56302.2022.9974607

[10] H. S. R. Alzubaidy and H. Jabber, “A survey of software-defined networking (SDN) controllers for Internet of Things (IoT) applications,” *Babylonian J. Netw.*, pp. 15–20, 2023.

[11] O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, “A deep learning methodology for predicting cybersecurity attacks on the internet of things,” *Information*, vol. 14, no. 10, p. 550, 2023.

[12] F. Shokoor, W. Shafik, and S. M. Matinkhah, “Overview of 5G & beyond security,” *EAI Endorsed Trans. Internet Things*, vol. 8, no. 30, p. e2, 2022.

[13] W. Robert, M. Bounabi, and A. Badr, "Leveraging AI in Mixed Hierarchical Topologies to Improve WSN: A Survey," *Babylonian J. Netw.*, pp. 59–69, 2025. doi: 10.58496/bjn/2025/005

[14] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 1, p. 10, 2023.

[15] R. Aljohani, A. Bushnag, and A. Alessa, "AI-based intrusion detection for a secure internet of things (IoT)," *J. Netw. Syst. Manage.*, vol. 32, no. 3, p. 56, 2024.

[16] T. S. Mohamed, S. M. Khalifah, R. Marqas, S. M. Almufti, and R. R. Asaad, "Evaluation of Information Security through Networks traffic traces for machine learning classification," *Babylonian J. Netw.*, pp. 25–42, 2025. doi: 10.58496/bjn/2025/003

[17] R. S. Tiwari, D. Lakshmi, T. K. Das, A. K. Tripathy, and K. C. Li, "A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security," *Telecommun. Syst.*, pp. 1–20, 2024.

[18] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021.

[19] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 296–312, 2023.

[20] S. A. Talib, "The Importance of Cryptography in Cloud Computing," *Al-Esraa Univ. Coll. J. Eng. Sci.*, vol. 6, no. 10, pp. 59–80, Jan. 2024. doi: 10.70080/2790-7732.1054

[21] B. Li, Y. Feng, Z. Xiong, W. Yang, and G. Liu, "Research on AI security enhanced encryption algorithm of autonomous IoT systems," *Inf. Sci.*, vol. 575, pp. 379–398, 2021.

[22] I. J. Hawi, "Unveiling the Hidden Threat: How Wireless Networks Fuel Serious Cyber Attacks," *Al-Esraa Univ. Coll. J. Eng. Sci.*, vol. 6, no. 9, pp. 88–100, Dec. 2024. doi: 10.70080/2790-7732.1007

[23] G. S. Nadella and H. Gonaygunta, "Enhancing cybersecurity with artificial intelligence: Predictive techniques and challenges in the age of IoT," *Int. J. Sci. Eng. Appl.*, vol. 13, no. 04, pp. 30–33, 2024.

[24] M. Asif, S. Naz, F. Ali, A. Alabrah, A. Salam, F. Amin, and F. Ullah, "Advanced Zero-Shot Learning (AZSL) Framework for Secure Model Generalization in Federated Learning," *IEEE Access*, vol. 12, pp. 184393–184407, 2024. doi: 10.1109/access.2024.3510756

[25] A. Salam, M. Abrar, F. Amin, F. Ullah, I. A. Khan, B. F. Alkhamees, and H. AlSalman, "Securing Smart Manufacturing by Integrating Anomaly Detection With Zero-Knowledge Proofs," *IEEE Access*, vol. 12, pp. 36346–36360, 2024. doi: 10.1109/access.2024.3373697