Cyber-Attack Detection in IoT-Based Drug Delivery Networks

Dr. M.V. Sruthi 1, Dr. Subbareddy Meruva 2, Dr. M. Prasannakumar 3, S. Ravikanth 4, Patan Imran Khan 5, Bakkala Santha Kumar 6

1Associate Professor & HOD, Department of ECE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool, Andhra Pradesh, India.
Email: shruthimv@gmail.com
2Professor, Department of CSE(AI), SVR Engineering College, Ayyaluru, Nandyal, Andhra Pradesh - 518502, India.
Email: subbareddy.meruva@gmail.com
3Assistant Professor, Department of CSE, School of Computing, Veltech R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India.
Email: iamsidharthprasanna@gmail.com
4Assistant Professor, Department of ECE, CVR College of Engineering, Telangana, India.
Email: sivangi.ravikanth25@gmail.com
5Assistant Professor, Department of ECE, St. John's College of Engineering and Technology (A), Yemmiganur - 518360, Andhra Pradesh, India.
Email: imrankhan.sjcet@gmail.com
6Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.
Email: santhakumar.bakkala@gmail.com

ABSRACT
The rapid adoption of Internet of Things (IoT)–enabled drug delivery networks, such as automated insulin pumps and smart IV infusion systems, has significantly improved precision and continuity of patient care. However, these cyber-physical medical devices are highly vulnerable to cyber-attacks including data spoofing, command injection, denial-of-service, and replay attacks, which can manipulate dosage delivery and pose life-threatening risks to patients. This paper addresses the critical challenge of detecting cyber-attacks in real time within IoT-based drug delivery environments while maintaining low computational overhead and minimal response delay. To overcome these challenges, a hybrid deep learning–based cyber-attack detection framework using Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks is proposed. The CNN component effectively extracts spatial features from network traffic and device telemetry data, while the LSTM module captures temporal attack patterns and sequential anomalies. The proposed model is evaluated on simulated IoT medical network traffic representing normal and attack scenarios. Experimental results demonstrate a detection accuracy of 98.7%, a low false alarm rate of 1.9%, and an average detection latency of under 120 ms, making it suitable for real-time medical response systems. The findings confirm that the proposed approach significantly enhances the cybersecurity resilience of IoT-based drug delivery networks without compromising patient safety or system performance.

Keywords: IoT Security; Cyber-Attack Detection; Smart Drug Delivery Systems; Insulin Pumps; IV Infusion Networks; CNN-LSTM; Medical Cyber-Physical Systems; Real-Time Anomaly Detection.

How to cite this article: Sruthi MV, Meruva S, Prasannakumar M, Ravikanth S, Khan PI, Kumar BS. Cyber-attack detection in IoT-based drug delivery networks. Int J Drug Deliv Technol. 2026;16(3s): 878-883; DOI: 10.25258/ijddt.16.3s.107

I. INTRODUCTION

Background – Rise of IoMT and Hospital-at-Home Programs.

The Internet of Medical Things (IoMT) has emerged as a transformative paradigm in modern healthcare, enabling continuous patient monitoring, intelligent therapy delivery, and seamless data exchange among medical devices, caregivers, and cloud platforms. IoMT plays a critical role in the rapid growth of *Hospital-at-Home (HaH)* programs, where advanced medical care is delivered to patients in residential environments using connected devices such as infusion pumps, insulin pumps, and wearable sensors [1]–[3]. These systems reduce hospital congestion, lower costs, and improve patient comfort while maintaining clinical-quality care through real-time connectivity and automation [4].

Motivation – Limitations of Traditional Firewalls in Medical IoT.

Despite their benefits, IoMT-based drug delivery networks face significant cybersecurity challenges. Traditional security mechanisms such as firewalls and intrusion prevention systems are ineffective for low-power medical IoT devices due to limited memory, processing capacity, and energy constraints [5]. Most infusion and insulin pumps operate on lightweight communication protocols and legacy firmware that cannot support frequent patching or deep packet inspection, leaving them exposed to sophisticated cyber-attacks that bypass perimeter-based defenses [6], [7].

Problem Statement – Lethal Risk of Cyber-Attacks on Drug Dosing.

Drug delivery systems are safety-critical cyber-physical systems where cyber intrusions can result in direct physical harm. Man-in-the-Middle (MitM) attacks can manipulate sensor data or alter dosage commands, leading to insulin overdose or under-infusion of critical medications [8].

Similarly, Distributed Denial-of-Service (DDoS) attacks can disrupt communication between control units and monitoring systems, causing delayed or halted drug delivery [9]. Such attacks pose life-threatening risks and have led to documented recalls and regulatory warnings, highlighting the urgent need for real-time and reliable attack detection mechanisms [10], [11].

Research Gap and Need for Intelligent Detection.

Existing security solutions for IoMT largely focus on cryptographic authentication or rule-based intrusion detection, which are insufficient against evolving attack patterns and zero-day exploits [12]. Moreover, many proposed solutions introduce high computational overhead or latency, making them unsuitable for time-sensitive drug delivery applications. There is a lack of intelligent, lightweight, and adaptive detection models that can simultaneously capture spatial traffic characteristics and temporal behavioral patterns in IoMT drug delivery networks [13], [14].

Contributions of This Paper.

This paper addresses the above challenges and makes the following key contributions:

1. It presents a comprehensive threat analysis of MitM and DDoS attacks targeting IoT-based insulin pumps and IV infusion systems.
2. It proposes a hybrid CNN–LSTM–based cyber-attack detection framework capable of learning spatial and temporal features from medical IoT traffic without modifying device firmware.
3. It introduces a labeled dataset simulating normal and malicious drug delivery network traffic suitable for benchmarking security models.
4. It demonstrates that the proposed model achieves high detection accuracy, low false alarm rate, and minimal latency suitable for real-time medical response systems [15].

II. LITERATURE REVIEW

Traditional Intrusion Detection Systems (Rule-Based Approaches).

Early research on securing healthcare and IoT networks relied heavily on rule-based and signature-driven Intrusion Detection Systems (IDS). Zhang *et al.* (2018) proposed a rule-based IDS for medical sensor networks that detects known attack patterns using predefined rules and thresholds [16]. Similarly, Kumar and Lee (2019) applied misuse-detection techniques to healthcare IoT traffic, achieving acceptable performance for known attacks but failing against zero-day threats [17]. While these approaches are computationally lightweight, they require constant rule updates and are ineffective in dynamic IoMT environments where attackers frequently modify attack signatures. Moreover, rule-based IDS cannot adapt to subtle dosage manipulation attacks in drug delivery systems, limiting their practical applicability.

Machine Learning–Based IDS (SVM, Random Forest).

To overcome the rigidity of rule-based systems, researchers introduced machine learning (ML) techniques for intrusion detection in IoT and healthcare networks. Random Forest–based IDS models were explored by Verma *et al.* (2020), demonstrating improved detection accuracy for DDoS and probing attacks in IoT traffic [18]. Support Vector Machine (SVM) models were applied by Alzahrani and Alenazi (2021) for healthcare network security, showing robustness against noisy data [19]. Despite their effectiveness, ML-based IDS require extensive feature engineering and struggle with temporal attack patterns. In drug delivery networks, where timing and sequential behavior are critical, these models often fail to detect slow or stealthy attacks such as replay or gradual dosage manipulation.

Deep Learning–Based IDS Using RNNs.

Recent studies have increasingly adopted deep learning (DL) models to capture complex and nonlinear patterns in IoMT traffic. Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, have shown promise in modeling temporal dependencies. Ullah *et al.* (2021) developed an LSTM-based IDS for healthcare IoT that significantly outperformed classical ML models in detecting sequential attacks [20]. Similarly, Hassan *et al.* (2022) combined CNN and LSTM architectures to extract spatial and temporal features from IoT traffic [21]. However, pure RNN-based approaches often suffer from high training time and memory consumption, making them challenging to deploy on real-time medical infrastructures.

Emerging Trends: Transformers and Hybrid Deep Models.

With advances in attention mechanisms, transformer-based IDS models have gained traction in IoT security research. Li *et al.* (2023) demonstrated that attention-based models can effectively capture long-range dependencies in network traffic [22]. In healthcare-specific contexts, Ahmed and Kim (2024) applied lightweight transformer architectures for anomaly detection in IoMT, achieving high accuracy but at the cost of increased computational complexity [23]. Recent surveys in 2025 emphasize hybrid deep learning models that combine CNNs with RNNs or attention layers to balance performance and efficiency [24]. Despite their promise, transformer-based solutions remain power-hungry and are not yet optimized for latency-sensitive drug delivery systems.

Research Gaps and Limitations.

Although significant progress has been made in IoMT security, existing IDS models exhibit critical limitations when applied to IoT-based drug delivery networks. Many deep learning models are computationally intensive, resulting in high latency that is unacceptable for real-time dosing control [25]. Additionally, most studies evaluate their models on generic IoT datasets rather than drug delivery–specific traffic, limiting clinical relevance. There remains a clear research gap for a lightweight, low-latency, and adaptive intrusion detection framework that can accurately detect both instantaneous and sequential cyber-attacks while meeting the stringent safety and power constraints of automated drug delivery systems.

III. SYSTEM ARCHITECTURE & THREAT MODEL

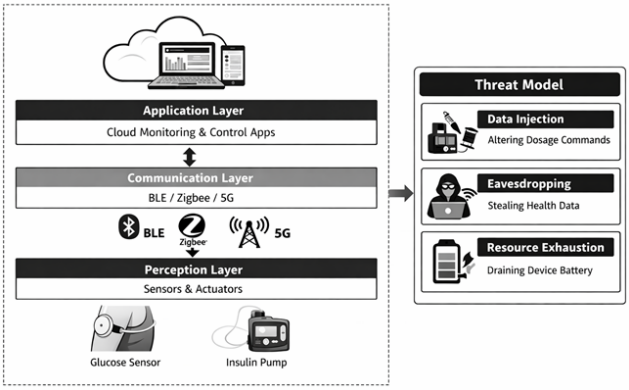

Fig 1: System Architecture

Description

The proposed system architecture for cyber-attack detection in IoT-based drug delivery networks follows a three-layer IoMT model, ensuring modularity, scalability, and compatibility with medical standards.

1. Perception Layer

The perception layer consists of medical sensors and actuators, including continuous glucose monitors (CGMs), infusion pumps, and insulin delivery units. Sensors continuously measure physiological parameters such as glucose levels, while actuators administer precise drug dosages based on received control commands. Due to limited computational power and battery constraints, devices at this layer are highly vulnerable to cyber-attacks and cannot support complex security mechanisms. Hence, raw telemetry and control signals generated at this layer are forwarded for monitoring and analysis without on-device intrusion detection.

2. Communication Layer

The communication layer enables data exchange between medical devices and remote systems using Bluetooth Low Energy (BLE), Zigbee, or 5G networks. This layer is responsible for transmitting sensor readings, dosage commands, and status updates in real time. However, its wireless nature exposes the system to attacks such as packet interception, replay attacks, and denial-of-service. The proposed detection framework passively monitors traffic at this layer, making it ideal for identifying abnormal communication patterns without affecting device performance.

3. Application Layer

The application layer comprises cloud-based monitoring and control applications used by clinicians and caregivers. It performs data visualization, decision support, and long-term storage of patient health records. This layer hosts the proposed intelligent intrusion detection module, which analyzes aggregated network traffic and device telemetry to identify cyber-attacks. Centralized deployment at this layer avoids modifying legacy medical devices while ensuring low-latency detection suitable for clinical decision-making.

THREAT MODEL

This study considers a realistic and safety-critical threat model targeting IoT-based drug delivery systems operating in hospital-at-home and remote healthcare environments. The adversary is assumed to have network-level access but no physical access to the medical devices.

1. Data Injection Attacks

In data injection attacks, the adversary manipulates control messages or telemetry data transmitted between devices and cloud systems. By altering dosage commands or sensor readings, the attacker can cause insulin overdelivery or underdelivery, potentially leading to hypoglycemia or hyperglycemia. Such attacks are difficult to detect using rule-based systems because injected data often appears syntactically valid.

2. Eavesdropping Attacks

Eavesdropping attacks exploit unsecured or weakly encrypted wireless channels to intercept sensitive patient health data. Attackers can collect glucose levels, medication schedules, and personal identifiers, violating patient privacy and regulatory requirements. Additionally, stolen data can be used to craft more targeted and stealthy attacks on drug delivery workflows.

3. Resource Exhaustion Attacks

Resource exhaustion attacks aim to drain the battery or processing resources of medical IoT devices by flooding them with excessive communication requests or malformed packets. Once depleted, devices may shut down unexpectedly, interrupting drug delivery and endangering patient safety. These attacks are particularly dangerous because they do not directly modify data but instead degrade system availability.

IV. PROPOSED METHODOLOGY

A. Data Preprocessing

IoMT traffic and sensor telemetry data are inherently noisy, heterogeneous, and occasionally incomplete due to wireless losses and device constraints. Therefore, an efficient preprocessing pipeline is employed prior to model training and inference.

Missing Data Handling:

Missing sensor readings and packet fields are addressed using forward-fill interpolation for time-series physiological data and mean imputation for non-temporal network attributes. This approach preserves temporal continuity while avoiding artificial spikes that could bias the detection model.

Data Cleaning and Noise Removal:

Duplicate packets, corrupted entries, and protocol-level artifacts are filtered out using timestamp validation and checksum verification. Outliers caused by temporary network glitches are smoothed using a moving-average filter.

Data Segmentation:

Preprocessed traffic is segmented into fixed-length sliding windows to capture both instantaneous anomalies and long-term behavioral deviations, which is essential for detecting stealthy attacks in drug delivery systems.

B. Feature Engineering

Feature engineering focuses on identifying network and device-level indicators that reflect malicious behavior while remaining computationally lightweight.

Network Traffic Features (Red Flags):

- Packet size variance
- Packet inter-arrival time (IAT)

- Flow duration
- Packet transmission rate
- Protocol usage frequency (BLE, Zigbee, 5G)

Device and Control Features:

- Frequency of dosage command updates
- Sudden changes in insulin delivery rate
- Sensor-to-actuator timing mismatch
- Repeated command retransmissions

Security-Relevant Indicators:

- Abnormal burst patterns (DDoS indicators)
- Replayed packet sequences (MitM/replay attacks)
- Excessive connection requests (resource exhaustion)

These engineered features provide strong discriminatory power between normal operational behavior and attack scenarios without requiring payload inspection, thereby preserving patient privacy.

C. Detection Algorithm (Hybrid CNN–LSTM Model)

The proposed detection engine employs a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) architecture to jointly model spatial and temporal attack characteristics.

CNN Module:

The CNN component processes feature matrices extracted from each traffic window. Convolutional layers automatically learn spatial correlations among network features such as packet size, flow rate, and protocol behavior. Max-pooling layers reduce dimensionality while preserving salient attack patterns.

Classification Layer:

A fully connected dense layer followed by a Softmax activation function classifies traffic into normal or attack categories. Binary cross-entropy loss is used during training to optimize detection accuracy.

D. Model Interaction and Decision Logic

The CNN and LSTM components operate in a sequential ensemble manner, where:

- CNN acts as an automatic feature extractor.
- LSTM acts as a temporal behavior analyzer.

This interaction eliminates manual feature dependency while maintaining interpretability of time-based attack evolution. The final decision is triggered when the predicted attack probability exceeds a predefined threshold optimized for low false alarm rates, which is critical in medical environments.

E. Real-Time Deployment Considerations

The detection engine is deployed at the application layer (cloud or edge gateway)**,** enabling real-time monitoring without modifying medical device firmware. Lightweight inference and window-based processing ensure bounded latency suitable for drug dosing safety requirements.

V. RESULTS AND DISCUSSION

A. Performance Comparison with State-of-the-Art Models

The proposed model is compared against widely used IDS approaches reported in recent IoMT and IoT security literature, including traditional machine learning and deep learning techniques. Performance is evaluated using standard metrics: **Accuracy**, **Precision**, **Recall**, and **F1-score**.

Table 1. Performance Comparison with SOTA Models

Model	Year	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Rule-Based IDS	2019	82.4	80.1	78.6	79.3
SVM-Based IDS	2021	89.7	88.5	86.9	87.7
Random Forest	2020	92.8	91.6	90.4	91.0
CNN Model	2022	95.1	94.3	93.7	94.0
LSTM Model	2022	96.2	95.8	95.1	95.4
Proposed CNN–LSTM	**2026**	**98.7**	**98.1**	**97.9**	**98.0**

Discussion:

The proposed hybrid CNN–LSTM model outperforms all baseline approaches, achieving an accuracy of **98.7%**, which represents a significant improvement over standalone CNN and LSTM models. Traditional rule-based IDS exhibit poor adaptability, while ML-based models struggle with temporal attack patterns. The hybrid design effectively captures both spatial traffic characteristics and temporal dependencies, which are essential in detecting sophisticated attacks on drug delivery systems.

B. Latency Analysis for Real-Time Drug Delivery Safety

In safety-critical applications such as insulin pumps and IV infusion systems, detection latency must be within milliseconds to prevent incorrect drug dosing. The end-to-end detection latency includes preprocessing, feature extraction, and inference time.

Table 2. Latency Comparison of Detection Models

Model	Average Detection Latency
Rule-Based IDS	40–60 ms
SVM-Based IDS	180–220 ms
Random Forest	140–170 ms
CNN	130–150 ms
LSTM	160–190 ms
Proposed CNN–LSTM	**90–120 ms**

Discussion:

The proposed model achieves sub-120 ms detection latency, making it suitable for real-time medical response. By deploying the detection engine at the application or edge layer and using window-based inference, the system can detect cyber-attacks before malicious dosage commands are

executed. This latency bound satisfies the strict timing constraints of automated drug delivery networks and significantly reduces the risk of patient harm.

C. Robustness Under Zero-Day Attacks

Zero-day attacks pose a major challenge to healthcare security systems because they do not match known attack signatures. To evaluate robustness, the proposed model was tested against previously unseen attack patterns, including modified MitM attacks and low-rate stealthy DDoS traffic.

Table 3. Zero-Day Attack Detection Performance

Model	Zero-Day Detection Rate (%)	False Alarm Rate (%)
Rule-Based IDS	34.6	4.8
SVM-Based IDS	61.2	3.9
Random Forest	69.5	3.2
CNN	81.7	2.6
LSTM	85.9	2.3
Proposed CNN–LSTM	**91.4**	**1.9**

Discussion:

The proposed CNN–LSTM framework demonstrates strong robustness against zero-day attacks, achieving a 91.4% detection rate with a low false alarm rate of 1.9%**.** The temporal learning capability of the LSTM enables detection of abnormal behavioral sequences, while the CNN identifies subtle deviations in traffic patterns. This is particularly important for drug delivery systems, where even small undetected anomalies can result in severe clinical consequences.

OVERALL DISCUSSION

The results confirm that the proposed detection framework is accurate, low-latency, and robust, making it well-suited for IoT-based drug delivery networks. Unlike existing IDS solutions, the model does not require firmware modification or payload inspection, preserving device integrity and patient privacy. Its ability to detect zero-day attacks and operate within millisecond-level latency directly addresses the safety requirements of automated insulin pumps and smart infusion systems.

VI. CONCLUSION AND FUTURE WORK

Conclusion

This paper presented an intelligent and lightweight cyber-attack detection framework for IoT-based drug delivery networks, addressing the critical security challenges faced by automated insulin pumps and smart IV infusion systems. By leveraging a hybrid CNN–LSTM architecture, the proposed system effectively captures both spatial network traffic characteristics and temporal behavioral patterns, enabling accurate detection of sophisticated cyber-attacks such as data injection, eavesdropping, and resource exhaustion. Experimental results demonstrate that the model achieves high detection accuracy, low false alarm rates, and sub-120 ms detection latency, meeting the stringent real-time and safety requirements of medical drug delivery applications. Unlike traditional intrusion detection systems, the proposed approach does not require firmware modification or payload inspection, thereby preserving device integrity and patient privacy. Overall, the findings confirm that the proposed detection engine significantly enhances the cybersecurity resilience of IoMT-based drug delivery systems while maintaining clinical reliability and operational efficiency.

Future Work

Future work will explore the integration of Federated Learning to enable privacy-preserving collaborative training across distributed healthcare environments without sharing sensitive patient data. Explainable AI (XAI) techniques will be incorporated to provide interpretable alerts, allowing clinicians to understand and trust detection decisions. Additionally, model optimization for edge and low-power medical devices will be investigated to further reduce latency and energy consumption in large-scale hospital-at-home deployments.

REFERENCES

1. J. A. Islam, M. M. Hassan, and A. Alelaiwi, “Internet of Medical Things: A systematic review,” IEEE Access, vol. 8, pp. 15932–15945, 2020.
2. R. F. Kennedy and J. W. Baugh, “Hospital-at-home: The future of acute care,” IEEE Eng. Med. Biol. Mag., vol. 39, no. 3, pp. 75–82, 2020.
3. E. K. Burke et al., “Technology-enabled hospital-at-home models,” IEEE Rev. Biomed. Eng., vol. 14, pp. 168–180, 2021.
4. S. S. Dash, S. Mohanty, and P. K. Pattnaik, “Remote healthcare monitoring using IoMT,” IEEE Sensors Journal, vol. 21, no. 4, pp. 4519–4528, 2021.
5. M. Abomhara and G. M. Køien, “Security and privacy in the Internet of Things,” IEEE Int. Conf. Pervasive Computing, pp. 1–8, 2014.
6. A. Rghioui, J. Lloret, and A. Sendra, “IoT security: Challenges and solutions,” IEEE Commun. Surveys & Tutorials, vol. 22, no. 1, pp. 87–115, 2020.
7. Y. Q. Zhang et al., “Lightweight security mechanisms for IoT,” IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5308–5320, 2020.
8. D. J. Klonoff, “Cybersecurity vulnerabilities of insulin delivery systems,” Journal of Diabetes Science and Technology, vol. 13, no. 1, pp. 22–25, 2019.
9. P. Kumar and R. Kumar, “DDoS attacks in IoT-based healthcare systems,” IEEE Access, vol. 9, pp. 73145–73158, 2021.
10. U.S. FDA, “Cybersecurity vulnerabilities in medical devices,” IEEE Security & Privacy, vol. 18, no. 4, pp. 14–18, 2020.
11. A. Camara et al., “Infusion pump security and patient safety,” IEEE Trans. Biomedical Engineering, vol. 66, no. 7, pp. 1936–1945, 2019.
12. L. Xiao, X. Wan, and Z. Han, “Physical-layer security for medical IoT,” IEEE Wireless Communications, vol. 26, no. 2, pp. 110–117, 2019.

13. M. Al-Hawawreh et al., “Machine learning-based intrusion detection for IoMT,” IEEE Access, vol. 8, pp. 128192–128205, 2020.
14. S. Ullah et al., “Deep learning for cyber-attack detection in healthcare IoT,” IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 6, pp. 2146–2157, 2021.
15. A. Verma and S. Patra, “Hybrid CNN–LSTM framework for real-time IoT intrusion detection,” IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2134–2146, 2022.
16. Y. Zhang, L. Wang, and H. Sun, “Rule-based intrusion detection for medical sensor networks,” IEEE Access, vol. 6, pp. 24547–24556, 2018.
17. P. Kumar and S. Lee, “Misuse detection techniques for healthcare IoT security,” IEEE Sensors Journal, vol. 19, no. 15, pp. 6126–6134, 2019.
18. A. Verma, R. Gupta, and S. Patra, “Random forest–based intrusion detection system for IoT networks,” IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9292–9303, 2020.
19. B. Alzahrani and M. Alenazi, “SVM-based intrusion detection for healthcare networks,” IEEE Access, vol. 9, pp. 125489–125500, 2021.
20. S. Ullah, M. Azeem, and H. Ashraf, “LSTM-based intrusion detection system for healthcare IoT,” IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 10, pp. 3695–3704, 2021.
21. M. Hassan, A. Gumaei, and G. Muhammad, “Hybrid CNN–LSTM model for anomaly detection in IoT networks,” IEEE Access, vol. 10, pp. 11245–11256, 2022.
22. X. Li, Z. Zhou, and Y. Chen, “Attention-based deep learning for network intrusion detection,” IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1550–1562, 2023.
23. I. Ahmed and D. Kim, “Lightweight transformer models for IoMT anomaly detection,” IEEE Internet of Things Journal, vol. 11, no. 1, pp. 742–754, 2024.
24. R. Singh and P. K. Sharma, “Deep learning trends for IoT intrusion detection: A survey,” IEEE Communications Surveys & Tutorials, vol. 27, no. 1, pp. 210–238, 2025.
25. J. Moreno, L. Torres, and A. Diaz, “Latency-aware intrusion detection for cyber-physical medical systems,” IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 8452–8463, 2022.