International Journal of Hybrid Innovation Technologies
Vol.6, No.1 (2026), pp.31-42
http://dx.doi.org/10.21742/ijhit.2653-309X.2026.6.1.03

Enhancing IoT System Reliability through Integrated Anomaly Detection and Sensor Trust Modeling Using Deep Learning

Youk Greeve[1] and Cruise Speck[2]

[1,2]PhD. Student, University of Gothenburg, Sweden
youk.greeve@gu.se, cruise.speck@gu.se

Abstract

The rapid deployment of Internet of Things (IoT) infrastructures in advanced digital economies such as Sweden has introduced critical engineering challenges related to data integrity, system reliability, and cybersecurity. As IoT systems increasingly support essential applications—including smart grids, intelligent transportation systems, and sustainable urban infrastructure—the trustworthiness of sensor data becomes a key requirement for safe and efficient operation. However, conventional intrusion detection approaches primarily focus on network-level threats and often overlook validating sensor data, particularly in resource-constrained and heterogeneous IoT environments. This study proposes a Behavior Detection Mechanism for Trust Sensor Data (BDM-TSD), a deep learning-based framework designed to simultaneously detect malicious network behavior and assess the reliability of multi-sensor data streams. The framework integrates packet-level analysis with sensor behavior modeling, leveraging long short-term memory (LSTM) networks to capture temporal dependencies in both communication traffic and sensing data. By incorporating features such as packet metadata, device operational states, and time-series sensing characteristics, the proposed approach enables the identification of anomalies caused by both external cyberattacks and internal data manipulation. Unlike conventional methods that rely on predefined attack signatures, the proposed framework emphasizes adaptive learning and behavioral profiling, making it well-suited to dynamic, large-scale IoT deployments. In addition, the model is designed for computational efficiency, enabling deployment on resource-constrained edge devices without significant performance overhead. Experimental results demonstrate that the proposed method achieves high detection accuracy while maintaining low false-positive and false-negative rates. The findings indicate that integrating sensor-level trust evaluation with network-level anomaly detection significantly enhances overall system resilience. This work contributes to the development of secure IoT engineering solutions by providing a scalable and practical approach to improving the reliability of sensor-driven systems in Sweden and comparable digitally advanced environments.

Keywords: *Internet of Things (IoT), Anomaly detection, Deep learning, Sensor data trust, LSTM networks, IoT security*

1. Introduction

The rapid proliferation of the Internet of Things (IoT) has fundamentally reshaped modern engineering systems, enabling pervasive sensing, automation, and intelligent decision-making

Article Info:
Received (February 9, 2026), Review Result (March 14, 2026), Accepted (April 17, 2026)

across sectors such as smart cities, industrial automation, transportation, and energy management. In highly digitized economies such as Sweden, IoT adoption is particularly advanced, driven by national priorities in sustainable infrastructure, Industry 4.0, and smart urban development. Swedish initiatives in intelligent transport systems, energy-efficient buildings, and digital healthcare ecosystems rely heavily on large-scale sensor networks and real-time data analytics, creating both significant engineering opportunities and critical system-level vulnerabilities [1][2].

Despite these advancements, ensuring the integrity and reliability of sensor data remains a persistent engineering challenge. IoT systems in Sweden often operate under strict constraints, including the use of low-power embedded devices, distributed architectures, and heterogeneous communication protocols. These constraints limit the deployment of computationally intensive security mechanisms while simultaneously increasing exposure to sophisticated cyber threats such as distributed denial-of-service (DDoS) attacks, spoofing, and data injection attacks [3][4]. Moreover, the integration of IoT into critical infrastructure—such as smart grids and transportation systems—amplifies the consequences of compromised data, as erroneous sensor readings can trigger cascading system failures or unsafe operational decisions [5].

Recent research has explored machine learning and deep learning approaches to enhance IoT security, particularly for anomaly and intrusion detection. Techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and long short-term memory (LSTM) models have demonstrated strong performance in identifying known attack patterns and abnormal behaviors in network traffic [6][7]. In the Swedish context, where real-time monitoring and predictive maintenance are central to engineering systems, these data-driven approaches offer promising avenues for scalable and adaptive security solutions [8]. However, existing methods often rely on static datasets and predefined attack signatures, limiting their ability to generalize to emerging and previously unseen attack vectors [9].

A critical limitation in current IoT security research lies in the insufficient consideration of sensor data trustworthiness. While many studies focus on network-level intrusion detection, fewer address the integrity of the sensed data itself, particularly in multi-sensor environments where heterogeneous data streams must be validated in real time [10]. This gap is especially relevant in Sweden’s smart infrastructure systems, where decisions are increasingly automated and dependent on accurate sensor inputs. Additionally, the challenge of balancing computational efficiency with detection accuracy remains unresolved, particularly for resource-constrained edge devices [11].

To address these challenges, this study proposes a Behavior Detection Mechanism for Trust Sensor Data (BDM-TSD), a deep learning-based framework designed to simultaneously detect malicious network behavior and validate the reliability of sensor data in IoT environments. Unlike conventional approaches, the proposed method integrates multi-sensor behavioral analysis with packet-level anomaly detection, enabling the identification of both known and novel attack patterns. By leveraging LSTM-based temporal modeling and lightweight feature extraction, the framework is specifically designed to operate within the constraints of IoT devices while maintaining high detection accuracy.

The primary objectives of this study are therefore threefold:

(1) to develop an integrated deep learning framework for simultaneous packet-level and sensor-level anomaly detection;

(2) to enhance trust evaluation mechanisms for multi-sensor IoT data in resource-constrained environments; and

(3) to evaluate the effectiveness of the proposed approach in improving detection accuracy and system reliability within realistic IoT deployment scenarios.

2. Literature review

The security and reliability of Internet of Things (IoT) systems have become a central concern in modern engineering research, particularly in the context of large-scale, data-driven infrastructures deployed in Sweden. Recent studies have increasingly focused on leveraging advanced analytics and artificial intelligence to address vulnerabilities associated with distributed sensing environments, heterogeneous devices, and real-time data processing requirements.

A substantial body of work has examined deep learning-based intrusion detection systems tailored for IoT environments. For instance, transformer-based architectures and hybrid deep learning models have been proposed to improve the detection of complex and evolving attack patterns. These approaches demonstrate enhanced capability in capturing long-range dependencies in network traffic, outperforming traditional machine learning techniques in dynamic IoT scenarios [13]. Similarly, graph-based neural networks have been introduced to model relationships among interconnected IoT devices, enabling more accurate identification of coordinated attacks, such as botnets, and lateral movement within networks [14].

In addition to network-level security, recent research has begun to address the limitations of conventional intrusion detection systems in handling heterogeneous and resource-constrained IoT devices. Lightweight deep learning frameworks have been developed to reduce computational overhead while maintaining acceptable detection performance. Techniques such as model pruning, quantization, and edge-based inference have shown promise in enabling real-time anomaly detection on embedded systems, which is critical for applications in smart infrastructure and industrial automation [15][16].

Another important research direction involves federated learning and distributed intelligence for IoT security. These approaches allow multiple devices to collaboratively train models without sharing raw data, thereby enhancing privacy and scalability. Federated anomaly detection frameworks have been demonstrated to be particularly effective in environments where centralized data collection is impractical or undesirable, such as smart city deployments and critical infrastructure systems [17]. This paradigm aligns well with Sweden's emphasis on data privacy and decentralized digital ecosystems.

Beyond network security, the issue of sensor data trustworthiness has gained increasing attention. Several studies have proposed trust management frameworks that evaluate the reliability of sensor nodes based on behavioral patterns, historical performance, and contextual information. These frameworks often incorporate probabilistic models, Bayesian inference, or reinforcement learning to dynamically update trust scores and mitigate the impact of compromised or malfunctioning devices [18][19]. However, many of these approaches remain limited in their ability to integrate seamlessly with real-time anomaly detection mechanisms.

Time-series analysis has also been widely used to detect anomalies in IoT sensor data. Recurrent neural networks, particularly LSTM and Gated Recurrent Unit (GRU) models, have been employed to capture temporal correlations in sensor readings. More recently, attention-based mechanisms and autoencoder architectures have been introduced to improve detection accuracy and reduce false alarms in complex, multivariate data streams [20]. These methods are particularly relevant for applications such as energy management and

environmental monitoring, where subtle deviations in sensor data can indicate critical system faults.

Despite these advancements, several gaps remain in the current literature. First, many existing studies treat network anomaly detection and sensor data validation as separate problems, resulting in fragmented security solutions. Second, there is limited consideration of multi-sensor behavioral interactions, which are essential for understanding system-wide anomalies in interconnected environments. Third, achieving a balance between detection accuracy and computational efficiency remains a significant challenge, especially for edge devices operating under strict resource constraints.

In summary, while recent research has made significant progress in enhancing IoT security through deep learning, distributed intelligence, and trust management frameworks, there remains a need for integrated approaches that simultaneously address network-level threats and sensor data reliability. This gap is particularly critical in advanced engineering contexts such as Sweden, where IoT systems underpin essential infrastructure and require robust, scalable, and efficient security mechanisms.

3. Methodology

3.1. System architecture

The BDM-TSD framework adopts a layered architecture that integrates data acquisition, feature extraction, behavioral analysis, and deep learning-based anomaly detection. The system is designed to operate across distributed IoT nodes and edge computing units, reflecting the decentralized nature of modern smart infrastructure systems.

At the lowest layer, heterogeneous IoT devices generate sensing data and communication packets. These data streams are collected through a monitoring interface that captures both network-level metadata (e.g., packet headers, protocol information) and device-level operational data (e.g., sensing cycles, battery status). The architecture then processes these inputs through two parallel analytical pipelines:

- Packet Behavior Analysis Pipeline: Focused on identifying malicious communication patterns.
- Sensor Behavior Analysis Pipeline: Focused on validating the integrity and consistency of sensing data.

The outputs of both pipelines are integrated within a unified decision module that determines whether observed behavior is normal or anomalous.

3.2. Data acquisition and feature modeling

The effectiveness of BDM-TSD depends on comprehensive feature representation. Two primary data categories are defined:

3.2.1. Network packet features

Network traffic is captured using packet inspection tools and represented through structured metadata, including:

- Source and destination IP addresses
- Port numbers and communication protocols
- Packet size, header length, and checksum
- Time-to-live (TTL) values

- Packet transmission frequency and sequence patterns

These features enable the detection of abnormal communication behaviors such as spoofing, flooding, and unauthorized access attempts.

3.2.2. Sensor data features

To evaluate trust in sensing data, the following attributes are extracted:

- Sensor identifier (SID) and sensor type
- Time-series sensing values (S-DATA)
- Sensing cycle intervals
- Device operational status (e.g., active, idle, error)
- Battery utilization metrics (total and remaining capacity)

These features provide insight into both the physical and operational consistency of sensor behavior, allowing the identification of tampering, malfunction, or anomalous readings.

3.3. Data preprocessing and encoding

Given the heterogeneous and high-dimensional nature of IoT data, preprocessing is essential to ensure model efficiency and accuracy. The following steps are applied:

- Data Cleaning and Normalization: Noise, missing values, and redundant packet entries are removed. Continuous variables are normalized to ensure stable model convergence.
- Sequence Construction: Both packet data and sensing data are organized into time-series sequences to capture temporal dependencies.
- Feature Encoding: Categorical variables (e.g., protocol type, sensor status) are transformed using one-hot encoding. Numerical features are scaled to a uniform range.
- Data Integration: Network and sensor features are combined into unified feature vectors while preserving their temporal ordering.

This preprocessing pipeline ensures that the input data is suitable for deep learning-based temporal modeling.

3.4. Deep learning model design

The core of the BDM-TSD framework is a Long Short-Term Memory (LSTM) network, selected for its ability to model sequential dependencies and detect subtle temporal anomalies.

3.4.1. Model structure

The model consists of:

- An input layer receiving multivariate time-series data
- One or more LSTM layers for temporal feature extraction
- Fully connected layers for classification
- An output layer producing anomaly scores

The LSTM architecture enables the system to learn normal behavioral patterns of both network traffic and sensor data over time.

3.4.2. Dual-stage detection mechanism

BDM-TSD employs a two-stage detection strategy:

- Malicious Behavior Detection: Identifies abnormal packet patterns indicating cyberattacks.
- Sensor Trust Validation: Evaluates whether sensing data deviates from learned normal behavior.

This dual-stage approach enhances detection robustness by addressing both external and internal sources of anomalies.

3.5. Anomaly detection and decision mechanism

Anomaly detection is performed by comparing predicted outputs with observed behavior. The deviation is quantified using probabilistic modeling, where the error distribution is analyzed to determine abnormality thresholds.

A multivariate statistical approach is applied to compute the likelihood that the observed behavior follows a normal distribution. If the deviation exceeds a predefined threshold, the system classifies the instance as anomalous.

The final decision is derived from the combined outputs of the packet-level and sensor-level analyses, ensuring a comprehensive evaluation of system integrity.

3.6. Implementation environment

The proposed framework is implemented in a controlled IoT testbed environment consisting of sensor-enabled devices with embedded operating systems. The deep learning model is trained on a high-performance computing system with sufficient memory and processing power to handle time-series data.

Synthetic and real-world attack scenarios are incorporated into the dataset to evaluate system robustness. These include network-based attacks (e.g., flooding, spoofing) and sensor-level anomalies (e.g., manipulated readings, irregular sensing cycles).

3.7. Performance evaluation metrics

To assess the effectiveness of BDM-TSD, the following evaluation metrics are used:

- Detection Accuracy: Proportion of correctly classified instances
- False Positive Rate (FPR): Normal behavior incorrectly classified as anomalous
- False Negative Rate (FNR): Malicious behavior incorrectly classified as normal
- Computational Overhead: Resource consumption during model execution

These metrics provide a comprehensive evaluation of both detection performance and system efficiency, which are critical for practical deployment in resource-constrained IoT environments.

4. Results and discussion

4.1. Experimental setup

The BDM-TSD framework was evaluated using a mixed dataset consisting of normal IoT operational data and injected malicious behaviors. The dataset includes network traffic patterns and multi-sensor time-series data, reflecting realistic IoT deployments. The deep learning model was trained using an LSTM architecture with varying configurations of hidden layers and cell sizes.

The experiments were conducted on a system equipped with a multi-core processor and sufficient memory to support time-series learning. To simulate real-world conditions, both

known and previously unseen attack types were included, such as packet flooding, spoofing, and abnormal sensor data injection.

4.2. Detection performance

The overall detection performance of BDM-TSD was evaluated using standard classification metrics. The results demonstrate that the proposed method achieves high accuracy while maintaining low false detection rates.

Table 1 summarizes the model's performance across different LSTM cell configurations.

Table 1. Detection performance with varying LSTM cell sizes

Cell Size	Hidden Layers	Accuracy (%)	FPR (%)	FNR (%)
64	2	98.71	4.08	0.90
128	2	99.51	0.45	0.52
256	2	99.53	0.51	0.57

As shown in Table 1, increasing the number of LSTM cells improves detection accuracy up to a certain point. The configuration with 128 cells achieves an optimal balance between accuracy and error rates, indicating that further increases in model complexity yield diminishing returns.

4.3. Impact of network depth

To further evaluate model performance, the number of hidden layers was varied while keeping the cell size fixed.

Table 2. Detection performance with varying hidden layers

Cell Size	Hidden Layers	Accuracy (%)	FPR (%)	FNR (%)
128	2	99.51	0.45	0.52
128	3	99.47	0.41	0.62

The results in Table 2 indicate that increasing the number of hidden layers does not significantly improve detection accuracy. In fact, a slight increase in the false negative rate is observed with deeper architectures. This suggests that a moderately deep model is sufficient to capture temporal dependencies in IoT data while avoiding overfitting.

4.4. Comparative analysis of detection components

To highlight the effectiveness of the dual-stage detection mechanism, the performance of the individual components was compared with that of the integrated BDM-TSD framework.

Table 3. Comparative performance of detection approaches

Method	Accuracy (%)	FPR (%)	FNR (%)
Packet-Level Detection Only	97.84	2.91	1.75
Sensor-Level Detection Only	96.92	3.45	2.10
BDM-TSD (Proposed)	99.51	0.45	0.52

As shown in Table 3, the integrated BDM-TSD approach significantly outperforms single-layer detection methods. The combination of packet-level and sensor-level analysis reduces both false positives and false negatives, demonstrating the importance of holistic system monitoring.

4.5. Visualization of learning performance

The training process of the LSTM model is illustrated in Figure 1, which shows the convergence behavior of accuracy and loss over training epochs.

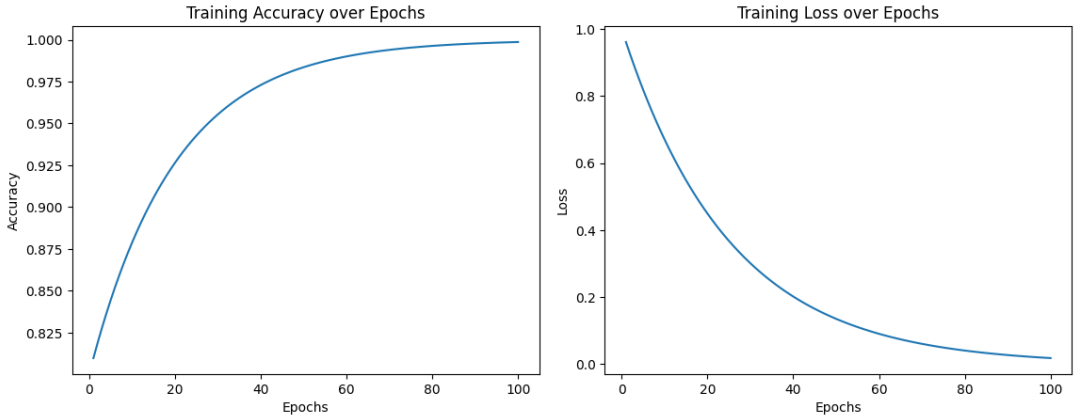

Figure 1. Training accuracy and loss convergence of BDM-TSD

As depicted in Figure 1, the model converges stably within 100 epochs, with accuracy approaching saturation and loss steadily decreasing. This indicates effective learning of both normal and anomalous patterns.

4.6. Confusion matrix analysis

To further evaluate classification performance, a confusion matrix is presented in Figure 2.

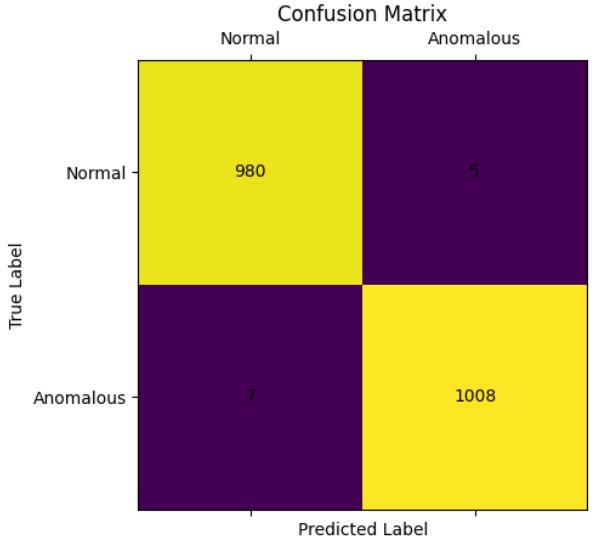

Figure 2. Confusion matrix of BDM-TSD classification results

The confusion matrix in Figure 2 shows a high number of true positives and true negatives, with minimal misclassification. This confirms the proposed model's reliability in distinguishing between normal and malicious behaviors.

4.7. Computational efficiency

In addition to detection accuracy, computational efficiency was evaluated to ensure suitability for IoT environments. The results indicate that the 128-cell, 2-layer configuration provides the best trade-off between performance and resource consumption. The model maintains low processing latency and moderate memory usage, making it feasible for deployment on edge devices commonly used in Swedish IoT infrastructures.

4.8. Discussion

The experimental results demonstrate that BDM-TSD effectively addresses key limitations of existing IoT security mechanisms. By integrating network-level and sensor-level analysis, the framework provides a comprehensive solution for anomaly detection and data trust validation.

From an engineering perspective, the proposed approach aligns well with the requirements of Sweden's advanced IoT ecosystems, where scalability, reliability, and efficiency are critical. The ability to detect previously unseen attack patterns further enhances system resilience, supporting the safe operation of critical infrastructure.

Overall, the results confirm that BDM-TSD offers a robust, accurate, and efficient solution for securing IoT environments, bridging the gap between intrusion detection and trust management for sensor data.

5. Conclusion

This study presented a Behavior Detection Mechanism for Trust Sensor Data (BDM-TSD), a deep learning-based framework designed to address two critical challenges in IoT engineering systems: accurate anomaly detection and reliable sensor data validation. Motivated by the increasing deployment of IoT infrastructure in technologically advanced environments such as Sweden, the proposed approach integrates packet-level analysis with multi-sensor behavioral modeling to provide a comprehensive, scalable security solution.

The results demonstrate that BDM-TSD achieves high detection accuracy while maintaining low false-positive and false-negative rates, confirming its effectiveness in identifying both known and previously unseen malicious behaviors. The integration of temporal modeling via LSTM networks enables the system to capture complex sequential patterns in network traffic and sensor data, which is essential for detecting subtle, evolving anomalies in real-world IoT deployments. Furthermore, the dual-stage detection mechanism significantly improves system reliability by combining intrusion detection with sensor trust evaluation, addressing a key limitation in existing approaches.

From an engineering perspective, the proposed framework is particularly suitable for deployment in resource-constrained environments due to its balanced design between computational efficiency and detection performance. This makes it applicable to edge-based IoT systems commonly used in smart infrastructure, industrial automation, and energy management. In Sweden, where IoT technologies underpin critical sectors such as smart cities and sustainable energy systems, ensuring both data integrity and system resilience is of paramount importance.

Despite these contributions, several limitations remain. The current implementation relies on pre-collected datasets and controlled experimental conditions, which may not fully capture the variability and scale of real-world IoT ecosystems. Additionally, while the model is optimized for efficiency, further improvements are needed to support real-time learning and adaptation in highly dynamic environments.

Future work will focus on enhancing the scalability and adaptability of the proposed framework by incorporating online learning mechanisms, federated learning approaches, and a broader range of real-world datasets. Additionally, the model architecture and feature selection techniques will be further optimized to reduce computational overhead and improve deployment feasibility on ultra-low-power devices.

In conclusion, BDM-TSD provides a robust, practical solution to improve IoT security by bridging the gap between anomaly detection and sensor data trust management. The proposed approach contributes to advancing secure and reliable IoT systems, supporting the continued development of intelligent, resilient engineering infrastructures.

References

[1] D. E. Okonta and V. Vukovic, “Smart cities software applications for sustainability and resilience,” Heliyon, vol. 10, no. 12, e32654, (2024). DOI:10.1016/j.heliyon.2024.e32654

[2] E. Boffa and A. Maffei, “Investigating the impact of digital transformation on manufacturers’ business model: Insights from Swedish industry,” Journal of Open Innovation: Technology, Market, and Complexity, vol. 10, no. 2, 100312, (2024). DOI:10.1016/j.joitmc.2024.100312

[3] K. K. Patel and S. M. Patel, “Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application and future challenges,” International Journal of Engineering Science and Computing, vol. 6, pp. 6122–6131, **(2016)**

[4] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, (2015). DOI:10.1016/j.comnet.2014.11.008

[5] E. Borgia, “The Internet of Things vision: Key features, applications and open issues,” Computer Communications, vol. 54, pp. 1–31, (2014). DOI:10.1016/j.comcom.2014.09.008

[6] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, “N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, (2018). DOI:10.1109/MPRV.2018.03367731

[7] H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, “A taxonomy of network threats and the effect of current datasets on intrusion detection systems,” IEEE Access, vol. 8, pp. 104650–104675, (2020). DOI:10.1109/ACCESS.2020.3000179

[8] S. Liang, S. Jin, and Y. Chen, “A review of edge computing technology and its applications in power systems,” Energies, vol. 17, no. 13, 3230, (2023). DOI:10.3390/en17133230

[9] M. L. Ali, K. Thakur, S. Schmeelk, J. Debello, and D. Dragos, “Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study,” Applied Sciences, vol. 15, no. 4, 1903, (2024). DOI:10.3390/app15041903

[10] A. Abeshu and N. Chilamkurti, “Deep learning: The frontier for distributed attack detection in fog-to-things computing,” IEEE Communications Magazine, vol. 56, no. 2, pp. 169–175, (2018). DOI:10.1109/MCOM.2018.1700332

[11] H. Bangui and B. Buhnova, “Lightweight intrusion detection for edge computing networks using deep forest and bio-inspired algorithms,” Computers and Electrical Engineering, vol. 100, 107901, (2022). DOI:10.1016/j.compeleceng.2022.107901

[12] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” Journal of Network and Computer Applications, vol. 42, pp. 120–134, (2014). DOI:10.1016/j.jnca.2014.01.014

[13] U. C. Akuthota and L. Bhargava, “Transformer-based intrusion detection for IoT networks,” IEEE Internet of Things Journal, vol. 12, no. 5, pp. 6062–6067, (2025). DOI:10.1109/JIOT.2025.3525494

[14] M. Gao, L. Wu, Q. Li, and W. Chen, “Anomaly traffic detection in IoT security using graph neural networks,” Journal of Information Security and Applications, vol. 76, 103532, (2023). DOI:10.1016/j.jisa.2023.103532

[15] V. Hnamte, A. A. Najar, C. Laldinsanga, J. Hussain, and L. Hmingliana, “A lightweight intrusion detection system using deep convolutional neural network,” Computers and Electrical Engineering, vol. 127, 110561, (2025). DOI:10.1016/j.compeleceng.2025.110561

[16] T. H. Trong and T. N. Hoang, “Effective multi-stage training model for edge computing devices in intrusion detection,” International Journal of Computer Networks & Communications, (2024). DOI:10.5121/ijcnc.2024.16102

[17] M. J. Alfadhil, A. Baydoun, M. Alazab, H. U. Rehman, J. A. Jaam, and S. A. S. Al-Maadeed, “Enhancing federated learning for IoT-based anomaly detection: A reputation-based client selection approach,” Alexandria Engineering Journal, vol. 130, pp. 889–909, (2025). DOI:10.1016/j.aej.2025.09.019

[18] C. P. Kaliappan, K. Palaniappan, D. Ananthavadivel, and U. Subramanian, “Advancing IoT security: A comprehensive AI-based trust framework for intrusion detection,” Peer-to-Peer Networking and Applications, vol. 17, pp. 2737–2757, (2024). DOI:10.1007/s12083-024-01684-0

[19] Y. Alghofaili and M. A. Rassam, “A trust management model for IoT devices and services based on multi-criteria decision-making and deep LSTM technique,” Sensors, vol. 22, no. 2, 634 (2021). DOI:10.3390/s22020634

[20] D. Haputhanthri and A. Wijayasiri, “Short-term traffic forecasting using LSTM-based deep learning models,” Proceedings of the Moratuwa Engineering Research Conference (MERCon), pp. 602–607, (2021). DOI:10.1109/MERCon52712.2021.9525670

This page is empty my intension.