Anomaly-Driven Jamming Attack Identification Using Hybrid Deep Neural Networks

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Ambeth Raja, A., et al. "Anomaly-Driven Jamming Attack Identification Using Hybrid Deep Neural Networks." *Shanlax International Journal of Arts, Science and Humanities,* vol. 13, no. 3, 2026, pp. 366–76.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i2-Feb.10307

Dr. A. Ambeth Raja
Associate Professor, PG & Research Department of Computer Science)
Thiruthangal Nadar College (Affiliated to University of Madras) Chennai, India

Mr. R. Sureshkumar
Ph.D Research Scholar
PG & Research Department of Computer Science)
Thiruthangal Nadar College (Affiliated to University of Madras) Chennai, India

Dr. V. Devi
Professor, PG & Research Department of Computer Science
Thiruthangal Nadar College (Affiliated to University of Madras) Chennai, India

Abstract

Healthy life enhances the quality of life by allowing individuals in engage able Wireless communication systems supporting Internet of Things (IoT), cyber-physical systems, and next- generation networks are increasingly vulnerable to sophisticated jamming attacks that degrade spectrum availability and service reliability. Conventional anti-jamming techniques based on fixed thresholds and handcrafted signal features fail to adapt to dynamic and intelligent interference behaviors. In this paper, an Anomaly-Driven Jamming Attack Identification Framework (AD-JAIF) is proposed using a hybrid deep neural network architecture that integrates convolutional neural networks (CNNs) and bidirectional long short-term memory (BiLSTM) networks. Time–frequency spectrogram representations of received signals are employed to enable effective spatial–frequency feature extraction through CNNs and temporal dependency modeling through BiLSTMs. To address the challenge of limited labeled attack data and zero- day jamming scenarios, an anomaly-driven learning mechanism is incorporated to model normal communication behavior and detect deviations indicative of jamming attacks. Extensive simulations were conducted under realistic wireless channel conditions considering constant, reactive, and adaptive jamming strategies over a wide signal-to-noise ratio range. Experimental results demonstrate that the proposed framework achieves superior detection performance, exceeding 98% accuracy with reduced false alarm rates and low detection latency compared to traditional machine learning and standalone deep learning models. The proposed AD-JAIF offers a robust, scalable, and real-time solution for securing emerging wireless communication systems against modern jamming threats.

Keywords: Jamming Attack Detection, Anomaly Detection, Hybrid Deep Learning, CNN-BiLSTM, Wireless Security

Introduction

The rapid evolution of wireless communication technologies has enabled large-scale deployment of Internet of Things (IoT)

devices, cyber-physical systems, unmanned aerial vehicles, and next-generation 5G/6G networks supporting mission-critical applications such as smart healthcare, intelligent transportation, industrial automation, and emergency response systems. Despite their transformative benefits, these wireless infrastructures remain highly susceptible to jamming attacks, a form of denial-of-service threat in which adversaries intentionally interfere with radio frequency transmissions to disrupt network availability, degrade quality of service, and compromise system reliability [1-3]. Unlike conventional cyber intrusions, jamming attacks exploit the broadcast nature of wireless channels, making them difficult to prevent using traditional cryptographic or access control mechanisms.

Existing anti-jamming solutions predominantly rely on signal processing-based techniques, including energy detection, spectrum sensing, spread spectrum communication, frequency hopping, and adaptive power control. While these approaches offer basic resilience against static and low-complexity jammers, they often fail to cope with intelligent and adaptive jamming strategies that dynamically alter attack patterns based on network behavior [4-6]. Furthermore, threshold-based detection methods are highly sensitive to environmental noise, channel fading, and mobility-induced variations, resulting in high false alarm rates and limited generalizability across diverse deployment scenarios.

In recent years, machine learning (ML) and deep learning (DL) have emerged as promising tools for wireless security, enabling data-driven detection of abnormal signal behaviors and network disruptions. Supervised learning approaches such as support vector machines, random forests, and deep neural networks have been explored for classifying jamming and non-jamming conditions using extracted spectral and temporal features [7-9]. However, these models typically require large volumes of labeled attack data, which is often impractical to obtain in real-world wireless environments. Moreover, single- architecture models struggle to capture the complex multi-dimensional characteristics of wireless signals that exhibit both spatial-frequency correlations and long-term temporal dependencies[10-12].

To overcome these limitations, hybrid deep learning architectures that combine complementary neural network models have gained increasing attention. Convolutional neural networks (CNNs) are particularly effective in learning localized spectral and spatial features from time-frequency representations of wireless signals, while recurrent neural networks such as long short-term memory (LSTM) and bidirectional LSTM (BiLSTM) networks excel at modeling sequential dependencies and temporal dynamics. Nevertheless, most existing hybrid approaches focus primarily on supervised classification and remain vulnerable to previously unseen or evolving jamming behaviors.

Anomaly-driven learning paradigms provide a powerful alternative by modeling normal communication patterns and identifying deviations that indicate potential attacks. By reducing dependence on labeled attack samples, anomaly detection frameworks enhance adaptability and robustness against zero-day jamming strategies [13-15]. However, current anomaly-based methods often employ shallow models or isolated feature spaces, limiting their ability to capture the high-dimensional and non-linear nature of wireless signal disruptions.

Motivated by these challenges, this paper proposes an Anomaly-Driven Jamming Attack Identification Framework (AD-JAIF) utilizing a hybrid deep neural network architecture that synergistically integrates CNN-based spectral-spatial feature extraction with BiLSTM-based temporal sequence learning. An unsupervised anomaly scoring mechanism is incorporated to identify subtle behavioral deviations from normal transmission patterns, enabling early and reliable detection of diverse jamming attacks without extensive labeled data. The proposed framework is designed to operate in real time and adapt to dynamic wireless environments.

The main contributions of this work are summarized as follows:

1. A hybrid deep learning architecture combining CNN and BiLSTM networks to jointly model spectral, spatial, and temporal characteristics of wireless signal behavior under jamming conditions.
2. An anomaly-driven detection mechanism that learns normal communication patterns and identifies novel jamming strategies with minimal reliance on labeled attack data.
3. A comprehensive experimental evaluation across multiple jamming scenarios, including constant, reactive, and adaptive intelligent jammers, demonstrating superior detection accuracy and robustness compared to traditional ML and standalone DL models.
4. A scalable and resilient security framework suitable for IoT, cyber physical systems, and next-generation wireless networks.

The remainder of this paper is organized as follows. Section 2 reviews related work on jamming detection and deep learning-based wireless security. Section 3 describes the proposed anomaly-driven hybrid framework and system architecture. Section 4 presents the experimental setup and performance metrics. Section 5 discusses the results and comparative analysis. Finally, Section 6 concludes the paper and outlines future research directions.

Related Work

Anomaly detection has become a central paradigm in modern cybersecurity due to its capability to identify previously unseen attack behaviors without relying exclusively on labeled intrusion data. Recent research has increasingly leveraged deep learning and hybrid intelligence frameworks to model complex system dynamics and improve detection robustness across cyber-physical and networked environments.

Mitikiri et al. (2025) investigated anomaly-based detection of adversarial cyberattacks in electric vehicle (EV) charging infrastructures, emphasizing the vulnerability of critical cyber-physical systems to coordinated disruptions. Their framework modeled normal operational behavior and identified deviations indicative of attack activities, achieving high detection sensitivity under adversarial conditions. The study demonstrated the effectiveness of anomaly-driven approaches in dynamic environments but primarily relied on structured operational data rather than high-dimensional temporal-spectral patterns commonly observed in wireless communication disruptions such as jamming.

Hybrid neural architectures have also gained prominence for real-time anomaly detection. Jain et al. (2025) proposed a hybrid deep learning framework integrating multiple neural network layers to enhance cybersecurity threat recognition in streaming environments. Their model combined feature abstraction with temporal pattern learning to improve detection accuracy and latency performance. Although the hybrid strategy improved adaptability, the approach remained focused on traditional network traffic anomalies and did not address signal-level disruptions or adaptive interference attacks present in wireless systems.

Architectural perspectives on multi-stage anomaly detection were presented by Grekov (2022), who introduced a layered detection pipeline that sequentially performs traffic preprocessing, anomaly scoring, and attack classification. This modular structure enabled early threat filtering and scalable deployment across network infrastructures. However, the framework primarily employed classical detection mechanisms and lacked deep feature representation learning, limiting its effectiveness against sophisticated and evolving attack strategies.

Optimization-driven intrusion detection systems have further enhanced anomaly classification performance. Albasheer et al. (2024) developed an IDS incorporating the Jaya optimization algorithm with SMOTE-ENN resampling to handle class imbalance in cyberattack datasets. Their

approach significantly improved detection precision and recall by refining feature selection and sample distribution. While effective for structured intrusion datasets, such optimization- based techniques depend heavily on labeled data and static attack profiles, reducing resilience to zero-day threats and adaptive adversaries.

Similarly, Alhayan et al. (2025) introduced an enhanced anomaly detection framework utilizing an improved snow ablation optimizer for dimensionality reduction coupled with a hybrid deep learning model. Their system demonstrated superior performance in high-dimensional intrusion detection tasks by optimizing feature relevance prior to classification. Despite its robustness, the model remained tailored to packet- level network intrusion data and did not explicitly capture temporal interference dynamics or spectral distortions inherent in wireless jamming attacks.

Temporal deep learning models have also been extensively explored for anomaly detection. Dash et al. (2025) proposed an optimized LSTM-based architecture capable of learning long-term dependencies in network traffic flows, achieving improved detection accuracy for stealthy intrusions. The study highlighted the strength of recurrent models in capturing evolving behavioral patterns. Nonetheless, standalone temporal models often struggle with spatial or frequency-domain feature extraction, which is crucial for identifying complex wireless interference behaviors.

From a spatial-feature learning perspective, Andresini et al. (2021) developed a CNN-based intrusion detection approach using nearest cluster representations to enhance local feature discrimination. Their convolutional framework effectively captured localized anomaly structures within network data distributions, outperforming conventional classifiers. However, the model did not incorporate temporal sequence modeling, limiting its ability to detect evolving attack strategies over time.

Optimization-driven intrusion detection systems have further enhanced anomaly classification performance. Albasheer et al. (2024) developed an IDS incorporating the Jaya optimization algorithm with SMOTE-ENN resampling to handle class imbalance in cyberattack datasets. Their approach significantly improved detection precision and recall by refining feature selection and sample distribution. While effective for structured intrusion datasets, such optimization- based techniques depend heavily on labeled data and static attack profiles, reducing resilience to zero-day threats and adaptive adversaries.

Similarly, Alhayan et al. (2025) introduced an enhanced anomaly detection framework utilizing an improved snow ablation optimizer for dimensionality reduction coupled with a hybrid deep learning model. Their system demonstrated superior performance in high-dimensional intrusion detection tasks by optimizing feature relevance prior to classification. Despite its robustness, the model remained tailored to packet- level network intrusion data and did not explicitly capture temporal interference dynamics or spectral distortions inherent in wireless jamming attacks.

Temporal deep learning models have also been extensively explored for anomaly detection. Dash et al. (2025) proposed an optimized LSTM-based architecture capable of learning long-term dependencies in network traffic flows, achieving improved detection accuracy for stealthy intrusions. The study highlighted the strength of recurrent models in capturing evolving behavioral patterns. Nonetheless, standalone temporal models often struggle with spatial or frequency-domain feature extraction, which is crucial for identifying complex wireless interference behaviors.

From a spatial-feature learning perspective, Andresini et al. (2021) developed a CNN-based intrusion detection approach using nearest cluster representations to enhance local feature discrimination. Their convolutional framework effectively captured localized anomaly structures within network data distributions, outperforming conventional classifiers. However, the model did not incorporate temporal sequence modeling, limiting its ability to detect evolving attack strategies over time.

System Model and Architecture

Network and Threat Model

Consider a wireless communication environment consisting of multiple legitimate transmitter–receiver pairs operating over shared radio spectrum, such as IoT networks, cyber-physical systems, or next-generation cellular infrastructures. Let $S(t, f)$ denote the received signal power distribution over time t and frequency f. Under normal operation, signal behavior follows statistically stable transmission patterns governed by channel conditions, traffic load, and noise characteristics.

A jammer is assumed to be an intelligent adversary capable of launching diverse interference strategies, including:

- **Constant jamming:** continuous high-power interference across selected frequency bands
- **Reactive jamming:** transmission triggered by legitimate activity detection
- **Adaptive jamming:** dynamically varying power, timing, and spectral occupancy

The jammer's objective is to degrade communication reliability while avoiding detection through pattern randomization.

Signal Preprocessing and Feature Representation

The raw received wireless signals are first converted into time–frequency representations using Short-Time Fourier Transform (STFT):

$$X(t, f) = \sum_{n=-\infty}^{\infty} x(n)w(n - t)e^{-j2\pi fn}$$

where x(n) is the sampled signal and w(·) denotes the windowing function.

The magnitude spectrogram:

$$P(t, f) = | X(t, f) |2$$

serves as the primary input to the deep learning model, capturing both spectral energy distribution and temporal evolution.

To enhance learning stability, the spectrograms undergo:

- Logarithmic scaling
- Min–max normalization
- Sliding window segmentation for sequence modeling

Hybrid Deep Neural Network Architecture

The proposed Anomaly-Driven Jamming Attack Identification Framework (AD-JAIF) employs a hybrid CNN–BiLSTM architecture designed to exploit complementary feature learning capabilities.

Convolutional Feature Extraction

The CNN module processes spectrogram inputs to extract localized spatial-frequency features:

$$Fk = \sigma(Wk * P + bk)$$

where Wk and bk denote convolution kernels and biases, $*$ represents convolution, and σ(·) is the ReLU activation.

Multiple convolutional layers with max-pooling progressively capture:

- Narrowband interference signatures
- Burst-like jamming patterns
- Energy concentration anomalies

Anomaly Scoring and Decision Module

Rather than relying solely on supervised classification, the framework employs anomaly-driven learning by modeling normal communication patterns.

A reconstruction-based anomaly detector is integrated using a dense autoencoding layer

Each spectrogram segment is processed by a convolutional neural network to automatically extract spatial-

$$\hbar t = g(f(ht))$$

frequency features. Through hierarchical convolution and pooling operations, the CNN identifies localized energy

The anomaly score is computed as:

$$At = \| ht - \hbar t \| 2$$

If:

$$At > \theta$$

where θ is a dynamically learned threshold, the instance is flagged as a potential jamming attack.

This mechanism enables:

- Detection of zero-day jammers
- Reduced dependence on labeled attack data Improved adaptability to evolving threat

End-to-End Detection Workflow

The proposed Anomaly-Driven Jamming Attack Identification Framework (AD-JAIF) follows a structured end-to-end processing pipeline that transforms raw wireless signals into reliable jamming attack decisions. Each stage of the workflow is designed to progressively refine signal representations while enhancing anomaly detection accuracy in dynamic wireless environments.

Wireless Signal Acquisition

The detection process begins with continuous acquisition of radio frequency signals at the receiver node using communication interfaces or software-defined radio platforms. These signals inherently include legitimate transmissions, environmental noise, channel fading effects, and potential interference components. High-resolution sampling is employed to preserve spectral characteristics critical for identifying abnormal transmission behaviors. This stage ensures that real-world wireless dynamics are accurately captured for further analysis.

Time–Frequency Transformation Using STFT

To reveal both temporal and spectral characteristics of the received signals, the Short-Time Fourier Transform is applied. This converts the one-dimensional temporal signal into a two-dimensional spectrogram representing energy distribution across frequency bands over time. Distinctive jamming signatures such as continuous spectral flooding, burst interference, and dynamic frequency hopping become clearly observable in this representation, enabling efficient feature learning by deep neural networks.

Spectrogram Normalization and Segmentation

The generated spectrograms are subjected to logarithmic scaling and min–max normalization to mitigate large power fluctuations and ensure numerical stability during training. Subsequently, the normalized spectrograms are segmented into overlapping temporal windows. This segmentation allows the model to capture short-term variations while maintaining long-term signal continuity, which is essential for learning evolving jamming behaviors.

CNN-Based Spatial-Frequency Feature Extraction

Each spectrogram segment is processed by a convolutional neural network to automatically extract spatial-frequency features. Through hierarchical convolution and pooling operations, the CNN identifies localized energy distortions, frequency occupancy irregularities, and interference patterns characteristic of jamming attacks. This automated feature learning eliminates dependency on handcrafted signal descriptors and improves generalization across diverse wireless environments.

BiLSTM-Based Temporal Pattern Modeling

The spatial-frequency features produced by the CNN are reshaped into sequential inputs and fed into a bidirectional long short-term memory network. The BiLSTM captures both past and future dependencies in signal behavior, enabling accurate modeling of temporal dynamics associated with persistent or adaptive jamming strategies. This dual- directional learning enhances the system's ability to distinguish malicious interference from transient channel noise.

Anomaly Scoring and Threshold-Based Decision Making

To enable detection of previously unseen jamming strategies, an anomaly-driven learning mechanism is employed. The framework learns baseline normal communication behavior and computes reconstruction-based anomaly scores during inference. When deviations exceed a dynamically determined threshold, the signal instance is classified as anomalous. This approach minimizes reliance on labeled attack data while improving resilience against zero- day jamming attacks.

Jamming Alert Generation and Mitigation Triggering

Upon detection of a jamming anomaly, the system generates real-time security alerts and activates mitigation protocols. These may include adaptive frequency hopping, power control, channel reassignment, or jammer localization mechanisms. This rapid response ensures minimal service disruption and maintains network reliability under adversarial conditions.

Experimental Setup and Performance Evaluation

The proposed AD-JAIF framework was evaluated using a MATLAB–Python co-simulation environment integrated with wireless signal generation modules. The simulation modeled a realistic wireless communication system consisting of multiple legitimate transmitters and a dynamic jammer operating across shared frequency bands.

Wireless signals were generated using quadrature phase shift keying (QPSK) modulation over Rayleigh fading channels with additive white Gaussian noise (AWGN). Three jamming strategies were simulated: constant jamming, reactive jamming, and adaptive intelligent jamming. Each scenario included both normal and attack transmission intervals.

Table I. Key Simulation Parameters

Parameter	Value
Carrier frequency	2.4 GHz
Bandwidth	20 MHz
Modulation	QPSK
Sampling rate	10 MHz
Channel model	Rayleigh fading + AWGN
SNR range	−5 dB to 20 dB
Window size (STFT)	256 samples
CNN layers	3 convolution + pooling
BiLSTM units	128
Training epochs	100
Batch size	64

Table I summarizes the simulation environment used to ensure realistic wireless signal behavior. The wide SNR range allows evaluation under both harsh and favorable channel conditions, while hybrid CNN–BiLSTM parameters were selected to balance accuracy and computational efficiency.

The proposed AD-JAIF was compared against:
- Support Vector Machine (SVM)
- Random Forest (RF)
- Standalone CNN
- Standalone LSTM
- Hybrid CNN–LSTM (supervised)

Table II. Overall Detection Performance (%)

Model	Accuracy	Precision	Recall	F1-score
SVM	88.21	86.95	85.40	86.17
RF	90.63	89.78	88.92	89.35
CNN	93.14	92.20	91.48	91.84
LSTM	94.02	93.41	92.87	93.14
CNN–LSTM	95.61	95.02	94.37	94.69
AD-JAIF (Proposed)	98.12	97.86	97.43	97.64

As shown in Table II, the proposed AD-JAIF significantly outperforms traditional ML and standalone DL models. The hybrid temporal–spatial learning combined with anomaly scoring enables superior generalization across diverse jamming behaviors, achieving over 98% detection accuracy.

Table III highlights that adaptive intelligent jammers are the most challenging to detect for conventional methods. However, AD-JAIF maintains high accuracy even under evolving attack behaviors, demonstrating strong robustness enabled by anomaly-driven learning.

Table III. Detection Accurcy Across Jamming Types (%)

Model	Constant	Reactive	Adaptive
SVM	90.3	85.6	78.9
RF	92.1	88.4	83.7
CNN	95.2	91.0	87.4
LSTM	96.1	92.6	89.1
CNN–LSTM	97.3	94.8	92.5
AD-JAIF	99.1	98.0	96.7

As observed in Table IV, AD-JAIF achieves the lowest false alarm rate while simultaneously reducing detection latency. This confirms its suitability for real-time wireless security applications where rapid response is critical.

Table IV. False Alarm Rate and Detection Delay

Model	FAR (%)	Avg. Detection Delay (ms)
SVM	7.84	42
RF	6.13	38
CNN	4.95	29
LSTM	4.21	31
CNN–LSTM	3.18	27
AD-JAIF	1.06	18

Table V demonstrates that the proposed framework maintains high detection reliability even in low-SNR environments, outperforming comparative models particularly under noisy channel conditions.

Table V. Detection Accuracy under Varying SNR Conditions (%)

SNR (dB)	CNN	CNN–LSTM	AD-JAIF
−5	82.3	86.7	91.5
0	88.4	91.2	95.6
5	92.1	94.0	97.3
10	95.3	96.8	98.5
20	97.0	98.1	99.2

The experimental results collectively demonstrate the effectiveness of the proposed AD-JAIF framework in addressing the complex challenges of jamming attack detection in dynamic wireless environments. The integration of hybrid CNN–BiLSTM learning enables comprehensive representation of jamming patterns by jointly capturing spatial-frequency distortions and long-term temporal dependencies, leading to substantially improved detection performance compared to standalone models. Moreover, the anomaly-driven detection mechanism enhances resilience against zero-day and adaptive jamming strategies by identifying deviations from normal communication behavior without heavy reliance on labeled attack data. As a result, AD-JAIF consistently achieves superior accuracy, strong robustness, and significantly reduced false alarm rates across all evaluated scenarios. Furthermore, the framework maintains reliable performance under varying signal-to-noise conditions and across diverse jamming strategies, confirming its adaptability and suitability for real-time deployment in next-generation wireless security systems.

Conclusion

This paper presented an Anomaly-Driven Jamming Attack Identification Framework (AD-JAIF) that integrates hybrid deep neural networks with anomaly-based learning to provide a resilient and adaptive security solution for wireless communication systems. By jointly leveraging convolutional neural networks for spatial–frequency feature extraction and bidirectional long short-term memory networks for temporal pattern modeling, the proposed framework effectively captures the complex and evolving characteristics of jamming interference. Unlike conventional detection approaches that depend heavily on labeled attack data or static signal thresholds, the anomaly-driven mechanism enables reliable identification of both known and previously unseen jamming strategies. Extensive experimental evaluations under diverse channel conditions and jamming scenarios demonstrated that AD-JAIF significantly outperforms traditional machine learning models and standalone deep learning architectures in terms of detection accuracy, robustness, false alarm reduction, and real-time responsiveness.

The framework maintained high performance even in low signal-to-noise environments and against adaptive intelligent jammers, confirming its suitability for deployment in practical wireless infrastructures such as IoT networks, cyber-physical systems, and next-generation communication platforms. The results highlight the critical importance of hybrid feature learning and anomaly-based intelligence in addressing modern wireless security threats. By eliminating reliance on handcrafted signal descriptors and improving adaptability to evolving adversarial behaviors, the proposed approach offers a scalable and future-proof defense mechanism against jamming attacks. Future work will focus on extending the framework to distributed and federated learning environments to enable collaborative jamming detection across large-scale networks while preserving data privacy.

Additionally, integration with proactive mitigation strategies, jammer localization techniques, and real-world hardware deployments will further enhance system effectiveness and operational resilience. Exploring lightweight model optimization for resource-constrained edge devices also represents a promising direction for practical adoption.

References

1. S. B. Mitikiri, V. L. Srinivas, and M. Pal, “Anomaly detection of adversarial cyber attacks on electric vehicle charging stations,” e-Prime – Advances in Electrical Engineering, Electronics and Energy, vol. 11, Art. no. 100911, 2025.
2. A. Jain, W. M. Ead, M. Alshahrani, et al., “Designing a hybrid neural network framework for real-time anomaly detection in cybersecurity applications,” Int. J. Inf. Technol., vol. 17, pp. 3173–3179, 2025, doi: 10.1007/s41870-025-02493-1.
3. M. Grekov, “Architecture of a multistage anomaly detection system in computer networks,” in Proc. Int. Siberian Conf. Control Commun. (SIBCON), Tomsk, Russia, 2022, pp. 1–5.
4. F. O. Albasheer, R. R. Haibatti, M. Agarwal, and S. Y. Nam, “A novel IDS based on Jaya optimizer and SMOTE-ENN for cyberattacks detection,” IEEE Access, vol. 12, pp. 101506–101518, 2024.
5. F. Alhayan, A. Alshuhail, A. O. A. Ismail, et al., “Enhanced anomaly network intrusion detection using an improved snow ablation optimizer with dimensionality reduction and hybrid deep learning model,” Sci. Rep., vol. 15, Art. no. 13270, 2025, doi: 10.1038/s41598-025-97398-1.
6. N. Dash et al., “An optimized LSTM-based deep learning model for anomaly network intrusion detection,” Sci. Rep., vol. 15, no. 1, Art. no. 1554, 2025.
7. G. Andresini, A. Appice, and D. Malerba, “Nearest cluster-based intrusion detection through convolutional neural networks,” Knowl.- Based Syst., vol. 216, Art. no. 106798, 2021.

8. D. P. Kavadi et al., "Design of an improved model for anomaly detection in CCTV systems using multimodal fusion and attention-based networks," IEEE Access, vol. 13, Art. no. 27287, 2025.
9. I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection," IEEE Access, vol. 6, pp. 33789–33795, 2018.
10. C. S. Rao and K. B. Raju, "MapReduce accelerated signature-based intrusion detection mechanism with pattern matching," in Soft Computing in Data Analytics, Springer, 2019, pp. 157–164.
11. W. Khan and M. Haroon, "An efficient framework for anomaly detection in attributed social networks," Int. J. Inf. Technol., vol. 14, pp. 3069–3076, 2022, doi: 10.1007/s41870-022-01044-2.
12. A. S. Iliyasu and H. Deng, "N-GAN: A novel anomaly-based network intrusion detection with generative adversarial networks," Int. J. Inf. Technol., vol. 14, pp. 3365–3375, 2022.
13. M. Munir, S. A. Siddiqui, A. Dengel, and S. Ahmed, "DeepAnT: A deep learning approach for unsupervised anomaly detection in time series," IEEE Access, vol. 7, pp. 1991–2005, 2019, doi: 10.1109/ACCESS.2018.2886457.
14. X. Xu, J. Li, Y. Yang, and F. Shen, "Toward effective intrusion detection using log-cosh conditional variational autoencoder," IEEE Internet Things J., vol. 8, no. 8, pp. 6187–6196, 2021.
15. S. Suma, "A deep learning based integrated memory-aware twin autoencoder network for anomaly detection in video surveillance on edge devices," Int. J. Intell. Eng. Syst., vol. 18, no. 1, Art. no. 1162, 2025.