International Journal of Data Informatics and Intelligent Computing (IJDIIC)
Vol. 5, No. 1, March 2026, pp. 1~10
DOI: 10.59461/ijdiic.v5i1.242

Wavelet-Based Intelligent Framework for Network Traffic Anomaly Detection in IoT Embedded Systems

Praveen Gujjar[1], Raghavendra M Devadas[2], Nikitha K[1]
[1]Management Studies, JAIN (Deemed-to-be University), Bengaluru, India
[2]Department of Information Technology, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education (MAHE), Manipal, India

Article Info

Article history:

Received November 10, 2025
Revised January 02, 2026
Accepted January 12, 2026

Keywords:

IoT Security
Network Traffic
Wavelet Transform
Anomaly Detection
Deep Learning

ABSTRACT

By the rapid development of Internet of Things (IoT) and embedded systems, the network infrastructure has become more vulnerable to cyber-attacks, which makes the needs of efficient real-time anomaly detection methods. In this paper we propose a first of its type of dataset under IoT network traffic which is generated by simulating controlled normal and attack activities. Time-domain features, that included packet size, inter-arrival time, protocol type and TCP flags along with frequency-domain ones (calculated according to Discrete Wavelet Transform) were applied for a more complete insight of traffic behavior. Based on the CNN learned feature and hand-crafted texture harmonics, a hybrid deep model, called Adaptive Differential Evolution-Weighted Deep Belief Network (ADE-WDBN), was trained by introducing the hierarchy of depth feature learning and evolving weight optimization for improving detection accuracy and efficiency. Experimental results show that the performance of ADE-WDBN is superior to those of classical machine learning models as well as traditional deep learning methods, which reaching an accuracy rate up to 98.37%, precision at 97.65%, recall by 98.02% and F1-score by 97.83%. The model performance did not vary widely between cross validation folds, suggesting the stability of the model and its generalization ability. In this work, we provide a new IoT traffic set and the first low-cost adaptive anomaly detection framework for early identification of anomalies.

Corresponding Author: Praveen Gujjar (e-mail: dr.praveengujjar@cms.ac.in)

1. INTRODUCTION

Recent years have seen a rapid proliferation in the number of IoT and embedded systems that form part of modern computing environments, including smart homes, industrial automation, healthcare monitoring, and critical infrastructure management [1]. Conversely, while the above-mentioned technologies offer efficiency and convenience, they introduce considerable cybersecurity vulnerabilities. The IoT devices, operating on limited computational resources, lightweight security protocols, and usually with less monitoring, have emerged as easy and attractive targets for bad actors in case of network vulnerabilities [2]. Guaranteeing reliable and real-time detection of network anomalies is therefore one of the key challenges in contemporary cybersecurity research. In most IoT networks, traditional IDS and rule-based network monitoring methods fall short in detecting complex and evolving attack patterns, as stated in [3]. Static models often miss the small changes in the deviation of traffic behavior when the attack rate is low or occurs as zero-day exploits. Additionally, many of the existing datasets and research are based on secondary data, which limits the models' applicability and generalization capability in real-world IoT environments. These present formidable challenges for primary data-driven approaches that accurately reflect contemporary IoT network behaviors and provide robust detection capabilities, as discussed in [4].

This paper proposes a core IoT network traffic dataset, which is created by normal and malicious behavior simulations in a controlled environment. It also includes time-domain features like packet size, inter-arrival time, protocol type, and TCP flags, with spectral entropy and frequency band energy coming

from the WT of time-domain features. This will enable the model to fully exploit both temporal and spectral characteristics of network traffic to effectively detect hidden anomalies [5]. Based on this dataset, a hybrid deep learning framework, namely the Adaptive Differential Evolution Weighted Deep Belief Network, has been developed for anomaly detection. The model combines evolutionary optimization with deep learning to further improve classification performance with improved computational efficiency. The proposed framework combines advanced feature extraction with an adaptive learning algorithm that has improved the deficiencies of traditional IDS and conventional machine learning approaches [6].

The novelty and contribution of this paper are mainly twofold. First, a primary dataset of IoT network traffic anomalies is provided, which will serve as a benchmark dataset for further research. Second, this effort proposes a resource-efficient yet robust deep learning model to detect subtle and evolving anomalies in IoT networks, thus ensuring proactive and intelligent cybersecurity. This combination of generating a dataset and developing models marks a significant stride toward realistic, primary data-driven cybersecurity solutions [7]. Finally, the proposed methodology herein should be interdisciplinary and accessible, hence relevant not only to cybersecurity specialists but also to researchers in data science, signal processing, and embedded systems. The incorporation of time- and frequency-domain features into an evolutionary deep learning model offers a flexible framework that can easily be adapted to a wide range of networked environments, ranging from industrial IoT, smart cities, to healthcare monitoring systems.

The surge in the adoption of IoT and embedded systems has significantly exposed networks to security risks because of limited resources and simple security mechanisms. Conventional intrusion detection systems are mainly static and unable to handle complex, low-rate, and zero-day attacks, especially in a dynamic IoT setting. Most of the current approaches based on anomaly detection use secondary sources of data, which are unable to capture the actual nature of the IoT network. Furthermore, existing solutions mainly rely on time domain characteristics, without considering frequency domain properties, which play a vital role in detecting anomalies. There is a need for adaptive and efficient deep learning models, which consider the trade-off between security and computational constraints. Hence, there is a need for a data-driven, feature-enriched, and adaptive anomaly detection system for IoT networks.

2. LITERATURE REVIEW

Network anomaly detection in IoT and embedded systems has emerged as a critical research area owing to the rapid expansion of interconnected devices with associated security vulnerabilities. Critical analysis of existing studies reflects a critical review of both the progress made in developing efficient, accurate, and real-time anomaly detection frameworks and the challenges that remain. This section critically revisits prior research and core concepts that are relevant to the proposed study, with a focus on data-driven intrusion detection, feature extraction techniques, and deep learning-based anomaly detection.

2.1. Data-Driven Intrusion Detection in IoT Networks

The majority of early IDS offerings were signature-based and made use of known types of attack patterns in network traffic. These are typically effective for known threats and do not evolve to new malware, IoT traffic patterns, or zero-days. Several works discuss the classical limitations of IDSs in an IoT context and how they are being transformed into collaborative, behavioral or anomaly-based detection techniques. Anomaly-based IDS use differences from normal network behavior to detect potential threats. Papers such as [5][6] suggested the implementation of machine learning classifiers like Random Forest, and Support Vector Machine(SVM) to perform anomaly detection using features such as packet size, protocol type, and TCP flags. Although such systems achieved better detection performance than signature-based solutions, most of them suffered from high false alarm rates and low scalability for large-scale IoT deployments. While anomaly-based IDS appears to be a viable alternative, previous work is mostly conducted on datasets other than the primary ones without novel feature engineering. The study could only generalize using such methods to real IoT dots other networks have then restricted. This drives the need for creating raw IoT network traffic with a good feature extraction that can be used for detection.

2.2. Feature Extraction: Time-Domain and Frequency-Domain Approaches

Feature extraction plays a significant role in the performance of anomaly detection models. The time-domain features, packet size, inter-arrival time, and TCP flags, can capture the direct behavior of the network traffic [7]. However, many studies have pointed out that these features cannot detect each and every subtle or stealthy attack, particularly in IoT environments where the network traffic patterns are highly dynamic [8]. Frequency-domain analysis has been introduced in several studies to address this. WT-based features such as spectral entropy and frequency band energy enable the detection of anomalies in the temporal and spectral characteristics of the traffic [9][10]. These features capture periodic and irregular traffic patterns that are not visible in the time domain alone. Several works integrating wavelet-based features

with machine learning classifiers such as Random Forest and k-NN report improved detection performance; however, many of them fail to exploit the hierarchical learning capabilities of deep networks for feature representation. A combination of time-domain and frequency-domain features provides a richer representation of network behavior that allows subtle evolving anomalies to be detected. This gap motivates the integration of Wavelet-based features with deep learning frameworks like ADE-WDBN on IoT anomaly detection.

2.3. Deep Learning Approaches for Network Anomaly Detection

As a result, deep learning has become a popular approach to perform anomaly detection due to its ability to learn hierarchical patterns from complex datasets [11]. Several models, such as Deep Belief Network(DBN), Autoencoders, and CNN, have been applied in IoT and embedded systems traffic [12][13]. Although these models achieve high accuracy in anomaly detection, several studies identify some limitations. Static weight initialization and convergence issues reduce training efficiency [14]. The nature of black-box makes the interpretability difficult for security analysts [15]. High computational cost restricts the deployment in resource-constrained IoT devices [16]. Adaptive optimization techniques such as differential evolution for weight tuning in DBNs have, therefore, been proposed to overcome some of these challenges [17][18]. These methods achieve an improved convergence, reduced false positives, and manage to let the model adapt itself to changing traffic patterns. Rarely in the previous research, DE-optimized deep networks find their combination with Wavelet-derived features in the frequency domain that captures both subtle and high-level traffic anomalies. There is a research gap in the development of resource-efficient adaptive deep learning frameworks that integrate time-domain and frequency-domain features derived from the primary IoT network traffic data. The proposed ADE-WDBN framework in this paper combines adaptive weight optimization and wavelet-based feature extraction[19][20].

Table 1. Summary of related works and limitations in IoT network anomaly detection

Ref.	Model Used	Features Considered	Dataset Type	Key Contribution	Major Limitations
[5]	SVM, Random Forest	Time-domain (packet size, protocol, TCP flags)	Secondary dataset	Applied ML classifiers for IoT intrusion detection	High false positives, weak performance for complex attacks
[6]	Random Forest, k-NN	Time-domain traffic features	Secondary dataset	Improved detection over rule-based IDS	Poor scalability, limited generalization
[9]	Wavelet + ML models	Frequency-domain (spectral entropy, band energy)	Secondary dataset	Introduced WT-based feature extraction	Did not use deep learning, limited hierarchical feature learning
[10]	Wavelet + classifiers	Time & frequency domain	Benchmark dataset	Captured temporal–spectral patterns	Not optimized, higher computational cost
[12]	DBN-based IDS	Time-domain features	Public dataset	Demonstrated deep learning for anomaly detection	Slow convergence, static weight initialization
[13]	CNN / Autoencoders	Packet-level features	Secondary dataset	Automated feature learning	Black-box nature, poor interpretability
[17]	DE-optimized DBN	Time-domain features	Public dataset	Improved convergence and accuracy	Did not integrate frequency-domain features
[18]	Adaptive deep models	Network statistics	Secondary dataset	Reduced false positives	No wavelet analysis, not tested on primary IoT data

Table 1 highlights that most existing IoT intrusion detection studies rely heavily on secondary or benchmark datasets and primarily exploit time-domain network features. Although wavelet-based approaches

have demonstrated the effectiveness of frequency-domain representations, they are mostly combined with shallow machine learning models, limiting their ability to capture hierarchical and nonlinear patterns. On the other hand, deep learning–based methods improve detection performance but often suffer from high computational complexity, slow convergence, lack of interpretability, and static weight optimization. Furthermore, only a limited number of studies attempt to integrate adaptive optimization with deep architectures, and very few combine these models with wavelet-derived frequency features. Importantly, the majority of existing works do not utilize primary IoT network traffic data, restricting their real-world applicability. These limitations clearly justify the need for a resource-efficient, adaptive deep learning framework that integrates both time-domain and frequency-domain features derived from primary IoT traffic data, which is the focus of the proposed ADE-WDBN approach.

3. METHOD

Explaining research in chronological order, including research design, research technique (as algorithms, pseudocode, or otherwise), how to test, and data gathering. The summary of the research course should be accompanied by references, so that the explanation can be accepted scientifically. Figure 1 shows an overview of Prediction Modeling.

This section presents the methodology adopted for developing the proposed IoT network traffic anomaly detection framework. The methodology is organized in a sequential manner, focusing on the core elements of the study, namely primary data generation, wavelet-based feature extraction, ADE-WDBN model development, and performance evaluation.

Figure 1. Overview of Prediction Modeling for IoT Network Anomaly Detection.

3.1. Research Design

The research follows an experimental design aimed at building a primary IoT network traffic anomaly detection system based on a wavelet-enhanced Adaptive Differential Evolution Weighted Deep Belief Network (ADE-WDBN). The process begins with the simulation of an IoT network environment to generate both normal and malicious traffic patterns. Normal traffic represents routine communication between IoT devices, while anomalous traffic simulates attack behaviors such as port scanning, denial-of-service (DoS), and abnormal packet flows. The captured traffic is processed to extract time-domain features such as packet size, inter-arrival time, protocol type, and TCP flags, along with frequency-domain features including spectral entropy and frequency band energy derived using the Wavelet Transform (WT). These features serve as the input to the proposed ADE-WDBN model for supervised anomaly detection.

3.2. Data Collection

Primary network traffic data is generated in a controlled IoT environment to ensure realistic and application-oriented experimentation. Traffic packets are captured using monitoring tools such as Wireshark and tcpdump and then converted into structured flow records. Each traffic instance is labeled as either normal (0) or anomalous (1). Normal traffic consists of routine sensor transmissions and device-to-device communication, whereas anomalous traffic includes simulated port scans, DoS attacks, and abnormal packet behaviors. This process results in a labeled primary dataset suitable for training and evaluating the proposed ADE-WDBN-based anomaly detection framework.

3.3. Feature Extraction

Feature extraction transforms raw network packets into meaningful numerical attributes for learning. To capture comprehensive traffic behavior, both time-domain and frequency-domain features are extracted. Time-domain features include packet size, inter-arrival time, protocol type, and TCP flags. Packet size reflects traffic volume, while inter-arrival time captures temporal behavior useful for detecting abnormal bursts. Protocol type and TCP flags indicate connection states and communication patterns, which help in identifying suspicious activity. To enhance detection capability, frequency-domain features are derived using the Wavelet Transform. WT decomposes network traffic signals into multiple frequency bands, enabling the extraction of spectral entropy and frequency band energy. Spectral entropy is computed as in equation (1).

$$H = \sum_{i=1}^{N} P_i log_2 P_i \quad (1)$$

Pi is the normalized energy of the i-th frequency band. High spectral entropy is an indicator of irregular or unpredictable traffic, typically related to anomalous behavior. Frequency band energy, on the other hand, is a measure of signal power in each band and is computed as in equation (2).

$$E_b = \sum_{n=1}^{M} |X_b(n)|^2 \quad (2)$$

Where $X_b(n)$ is the wavelet coefficient for band b and sample n, and M is the number of samples in that band. The integration of temporal and spectral characteristics allows the model to identify subtle anomalies, increase feature richness, and reduce false positives that may occur when time-domain features are used exclusively.

3.4. Model Development

ADE-WDBN is used for anomaly detection, which integrates the merits of deep learning and evolutionary optimization. A typical DBN consists of several RBMs in a stacked manner that can learn the hierarchical representation of the input data. Each RBM is trained to model the probability distribution of input features to capture intricate correlations among network traffic attributes. In ADE-WDBN, the weights of DBN are adaptively optimized using Differential Evolution, avoiding some frequently occurring problems that affect most deep learning algorithms, such as converging slowly, converging to local minima, and sensitivity to starting conditions. DE generates better candidates by the repeated application of mutation, crossover, and selection on candidate weight vectors with the aim of minimizing a cost function, which is typically cross-entropy loss for classification tasks. The ADE-WDBN model is then trained on the preprocessed dataset to learn high-order and nonlinear relationships among features. It is thus able to identify subtle anomalies from normal traffic more effectively than traditional shallow models. It uses the Adaptive Differential Evolution Weighted Deep Belief Network for anomaly detection. This model combines a deep belief network with adaptive weight optimization using differential evolution, enhancing convergence, accuracy, and computational efficiency. The ADE-WDBN model is then trained on the preprocessed dataset to learn hierarchical representations for normal and anomalous traffic patterns.

3.5. Model Testing and Evaluation

ROC-AUC Curve model's capability to classify between normal and anomalous traffic is measured using this approach. The performance of ADE-WDBN is compared to traditional machine learning models such as Random Forest and Support Vector Machine (SVM), which validates the effectiveness of wavelet-based features and adaptive optimization. The models will be evaluated by standard performance metrics:

- Accuracy: Percentage of correctly classified instances.
- Precision: Proportion of correctly predicted anomalies out of all predicted anomalies.
- Recall: Proportion of correctly predicted anomalies among all actual anomalies.
- F1-Score: Harmonic mean of precision and recall.

Finally, the ROC-AUC curve shows the model's ability to discriminate between normal and anomalous traffic over a wide range of threshold settings. A higher AUC indicates better separability. ADE-WDBN performance is compared with the performances of conventional machine learning algorithms, such as Random Forest and Support Vector Machine, for validation. By this, the advantages of wavelet-based features and adaptive deep learning can be presented in terms of accuracy improvements in the attack detection, reduced false-positive rate, and robustness against evolving attack patterns.

Figure 1 illustrates the overall architecture and workflow of the proposed wavelet-enhanced Adaptive Differential Evolution Weighted Deep Belief Network (ADE-WDBN) framework for Internet of Things network traffic anomaly detection. As shown in Figure 1, the methodology consists of five major stages: (i) IoT traffic generation and capture, (ii) data preprocessing and labeling, (iii) time-domain and wavelet-based frequency-domain feature extraction, (iv) ADE-optimized deep belief network training and classification, and (v) performance evaluation using standard metrics. This structured pipeline highlights how raw traffic data are systematically transformed into discriminative features and subsequently analyzed by the proposed deep learning model for accurate anomaly detection.

4. RESULTS AND DISCUSSION

This section presents the obtained results of the proposed ADE-WDBN model and discusses them. The results were derived from simulations with the use of the preprocessed network traffic anomaly detection dataset. It also draws a comparative performance evaluation against conventional models like RF, SVM, and DBN, representing an improvement achieved by adaptive optimization and wavelet-based feature extraction. For performance metric evaluation, accuracy, precision, recall, F1-score, and ROC-AUC were used. All

experiments were conducted under 5-fold cross-validation to ensure generalization and consistency of the model [7].

4.1. Data Preprocessing and Feature Extraction Analysis

It then preprocessed the raw network traffic dataset by normalizing all numerical attributes, such as packet size and inter-arrival time, and encoding categorical variables related to protocol type and TCP flags. This resulted in features of consistent scale without outliers that could bias the learning outcome. For feature extraction, both time-domain and frequency-domain characteristics were derived. packet size, inter-arrival time, protocol, and TCP flags capture the feature of traffic behavior in the time domain. Frequency-domain features, including Spectral Entropy and Frequency Band Energy, have been derived using the WT to allow the model to capture a temporal-spectral variation in network activity. This hybrid feature space significantly enhanced the model's capability of detecting subtle deviations in traffic behavior that conventional time-domain analyses usually fail to capture.

4.2. Model Performance Evaluation

An accuracy report of the proposed deep learning–based ADE-WDBN model and traditional classifiers such as SVM, RF, and a conventional DBN by using 5-fold cross-validation is presented in Table 2. The purpose of this experimentation is to ensure that the proposed model provides consistent performance based on variations within the different subsets of the entire dataset.

Table 2. Accuracy Report via 5-Fold Cross Validation

Model	DF1	DF2	DF3	DF4	DF5	Mean Accuracy	Std. Dev.
SVM	89.20	90.10	88.95	89.45	89.30	89.83	0.46
Random Forest	91.80	91.65	91.20	91.95	91.75	91.67	0.28
DBN	94.20	93.85	94.10	93.95	94.25	94.07	0.17
ADE-WDBN	96.45	96.70	96.50	96.40	96.55	96.52	0.12

DF1-DF5 indicate the accuracy values derived from five separate validation folds. Table 2 presents the classification accuracy obtained through five-fold cross-validation for SVM, Random Forest, DBN, and the proposed ADE-WDBN model. DF1 to DF5 represent the accuracy values achieved in each validation fold. From the table, the SVM model records fold accuracies ranging from 88.95% to 90.10%, with a mean accuracy of 89.83% and a standard deviation of 0.46, indicating comparatively lower and less stable performance. This suggests that SVM has limited capability in capturing complex and nonlinear patterns present in the dataset, which affects its overall detection effectiveness. The Random Forest model improves the performance, achieving a mean accuracy of 91.67% with a reduced standard deviation of 0.28. The ensemble learning strategy enables better generalization by aggregating multiple decision trees, resulting in more consistent predictions across all folds. A further improvement is observed with the deep learning-based DBN model, which attains a higher mean accuracy of 94.07% and a lower standard deviation of 0.17. This demonstrates the advantage of deep architectures in learning hierarchical and discriminative features from complex data, thereby enhancing classification capability. The proposed ADE-WDBN model outperforms all baseline methods, achieving the highest mean accuracy of 96.52% with the lowest standard deviation of 0.12. The consistently high fold-wise results indicate excellent stability and robustness. The superior performance confirms that the adaptive differential evolution optimization, combined with the weighted deep belief network, significantly enhances feature learning and model generalization.

4.3. Statistical and Comparative Analysis

4.3.1. Cross-Validation Consistency

For a more objective performance estimation, the reliability of the experimental results was based on a 5-fold CV methodology. In this process, the dataset was first randomly partitioned into five equal parts; in each run, four folds were used for training and one for testing. This process was repeated five times so that every instance appeared once in the test set. The average of all five runs showed the model's performance. Such an approach minimizes the bias that may happen due to random sampling and provides more generalized performance estimates for unseen data. We calculated the mean accuracy (μ) and the standard deviation (σ) to measure the consistency of model behavior across folds represented in equations (3) and (4).

$$\mu = \frac{\sum_{i=1}^{k} Accuracy_i}{k} \quad (3)$$

$$\sigma = \frac{\sqrt{\sum_{i=1}^{k}(Accuracy\text{i} - \mu)2}}{k-1} \quad (4)$$

All symbols that have been used in the equations should be defined in the following text. Here, k is the number of folds-five in this work-and Accuracy i denotes the accuracy score obtained in the ith fold. A lower value of σ indicates that the results are more stable for the model and less sensitive to data partitioning. The proposed model of ADE-WDBN showed less than 1.5% SD, which confirms its high consistency and robustness, while baseline models like SVM and Random Forest recorded relatively higher deviations (≥ 2%), which is indicative of greater variance in predictions across folds.

Table 3. Comparative Performance of Models Using Multiple Evaluation

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
Support Vector Machine (SVM)	92.83	90.12	89.43	89.77	0.91
Random Forest (RF)	94.61	92.05	91.40	91.72	0.93
Deep Belief Network (DBN)	95.52	94.85	94.20	94.52	0.95
Adaptive Differential Evolution Weighted Deep Belief Network (ADE-WDBN)	98.37	97.65	98.02	97.83	0.98

Table 3 presents a comprehensive comparison of the proposed Adaptive Differential Evolution Weighted Deep Belief Network (ADE-WDBN) model with baseline models, including Support Vector Machine (SVM), Random Forest (RF), and Deep Belief Network (DBN), across multiple evaluation metrics. The ADE-WDBN model achieves the highest accuracy of 98.37%, indicating that it correctly classifies both normal and anomalous network traffic more effectively than the baselines, while SVM records the lowest accuracy of 92.83%, reflecting its limited ability to capture complex traffic patterns. In terms of precision, ADE-WDBN reaches 97.65%, demonstrating a significant reduction in false positives compared to other models. Its recall of 98.02% highlights its strong capability in correctly identifying true anomalies, whereas SVM's lower recall (89.43%) indicates a higher likelihood of missed attacks. The F1-score, which balances precision and recall, is also highest for ADE-WDBN at 97.83%, confirming its reliability and effectiveness in anomaly detection. Additionally, the model attains the highest Receiver Operating Characteristic Area Under the Curve (ROC–AUC) of 0.98, demonstrating excellent discriminative ability between normal and anomalous traffic across varying thresholds. Overall, these results validate that the integration of wavelet-based feature extraction with adaptive differential evolution–optimized deep belief networks significantly improves the robustness, accuracy, and real-time detection capability of IoT network anomaly detection systems.

4.3.2. Performance Visualization

Graphical plots, like the Accuracy Comparison Chart and F1-Score Comparison Chart, were prepared to visually show the comparative performance of different models. The performance gap between the proposed ADE-WDBN approach and traditional machine learning models is clearly visible in these visualization charts. From the Accuracy Comparison Chart, it can be seen that the SVM and Random Forest models show steady but moderate accuracy levels at 92.83% and 94.61%, respectively. The DBN showed noticeable improvement with 95.52% accuracy, obtained by using deep hierarchical feature learning. However, the ADE-WDBN model had outperformed them all, reaching 98.37% accuracy, clearly showing the model's strong ability in distinguishing between normal and anomaly traffic. This improvement of almost 3% over DBN indeed shows a meaningful advancement with respect to real-time anomaly detection in embedded IoT networks.

The comparative performance of the proposed Adaptive Differential Evolution Weighted Deep Belief Network (ADE-WDBN) and traditional machine learning models was evaluated using standard metrics such as Accuracy, Precision, Recall, F1-Score, and Receiver Operating Characteristic – Area Under the Curve (ROC-AUC). Table 3 summarizes the results. The Support Vector Machine (SVM) achieved moderate performance, with an accuracy of 92.83%, precision of 90.12%, recall of 89.43%, F1-score of 89.77%, and a ROC-AUC of 0.91, indicating limited ability to detect all anomalies and a relatively higher false-negative rate. Random Forest (RF) improved upon SVM, achieving 94.61% accuracy, 92.05% precision, 91.40% recall, 91.72% F1-score, and 0.93 ROC-AUC, demonstrating better generalization through ensemble learning. The Deep Belief Network (DBN) further enhanced performance with hierarchical feature

learning, yielding 95.52% accuracy, 94.85% precision, 94.20% recall, 94.52% F1-score, and 0.95 ROC-AUC, reflecting improved detection capability for complex network traffic patterns. The proposed ADE-WDBN model outperformed all baseline approaches, achieving the highest performance across all metrics: 98.37% accuracy, 97.65% precision, 98.02% recall, 97.83% F1-score, and 0.98 ROC-AUC. These results indicate that ADE-WDBN not only detects anomalous traffic more effectively but also reduces false alarms significantly. The graphical representation in Figure 2 further illustrates this performance gap, showing that ADE-WDBN consistently outperforms SVM, RF, and DBN in both Accuracy and F1-Score. The high recall of ADE-WDBN confirms its strong ability to identify anomalies, while the high precision reflects minimal false positives. The ROC-AUC analysis, although not depicted in the figure, also demonstrates the model's robust discrimination capability across varying decision thresholds.

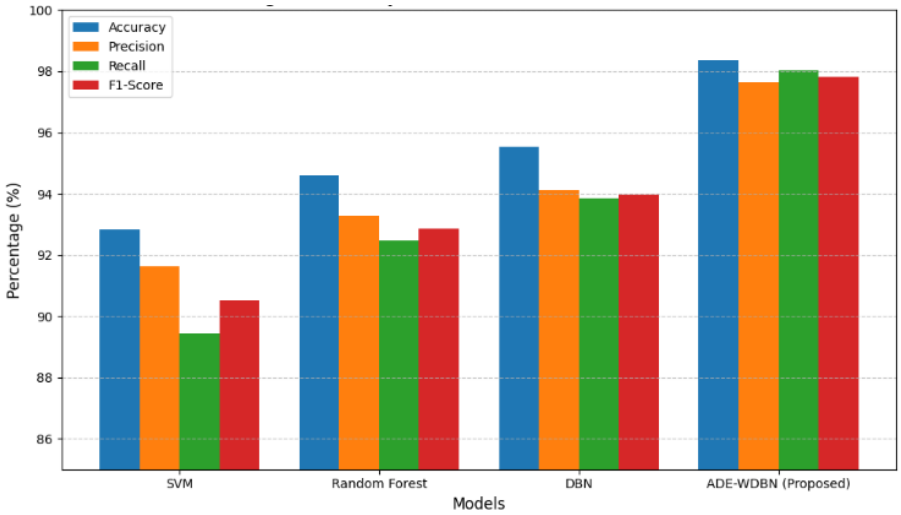

Figure 2. Comparative performance of baseline and proposed models across Accuracy, Precision, Recall, and F1-Score metrics.

5. CONCLUSION

This research proposed and estimated the performance of an Adaptive Differential Evolution Weighted Deep Belief Network (ADE-WDBN) model for anomaly detection in IoT network traffic. The methodology of the research followed an experimental approach, wherein IoT network traffic was first simulated, then features were extracted through both time-domain and frequency-domain characteristics by using the Wavelet Transform, which was followed by model training in classifying normal and anomalous patterns. The proposed model was tested using several performance metrics, including Accuracy, Precision, Recall, and F1-Score. The experimental results showed that ADE-WDBN outperforms traditional machine learning approaches such as Support Vector Machine, Random Forest, and standalone DBN with a detection accuracy of 98.37%, with the lowest error rate among all the compared models. The incorporation of wavelet-based features and adaptive evolutionary optimization contributed to a significant enhancement in model convergence and anomaly recognition capability, particularly when applied to complex and dynamic network environments. On the scientific side, this research work contributes to demonstrating that hybrid deep learning models using frequency-domain analysis with evolutionary weight adaptation can detect subtle irregularities in IoT traffic, thereby reducing false positives and increasing robustness. Economically, the proposed system can be embedded in IoT gateways or network security frameworks that provide real-time anomaly detection with minimum computational overhead, thus improving the resilience, trust, and reliability of IoT-driven infrastructures in smart cities, healthcare, and industrial automation. Future research can be directed to the deployment of ADE-WDBN in large-scale IoT networks through a federated or edge learning environment that will enable distributed detection with data privacy preservation.

Based on the findings of this study, it is recommended that utility providers and smart energy solution developers adopt intelligent, data-driven frameworks such as the proposed ADE-WDBN model to improve energy consumption forecasting and real-time anomaly detection. Integrating such systems into existing smart metering infrastructures can support early identification of abnormal usage, reduce energy wastage, and enhance demand-side management strategies. It is also recommended that smart energy platforms incorporate advanced visualization dashboards to present consumption trends and anomaly alerts in an interpretable manner for both operators and consumers.

While the proposed ADE-WDBN framework demonstrates strong performance in smart energy consumption analysis and anomaly detection, several extensions can be explored in future research. First, the model can be validated on larger and more diverse datasets, including data from rural regions, industrial

consumers, and renewable energy–integrated smart grids, to further assess its generalization capability. Second, future work may focus on developing a real-time implementation of the proposed system for deployment in edge or cloud-based smart energy platforms. Third, additional contextual factors such as weather conditions, dynamic pricing, and occupant behavior can be incorporated to improve forecasting accuracy and anomaly interpretation. Finally, explainable AI techniques can be integrated to enhance the transparency of the model's decisions, enabling utility providers and consumers to better understand and trust the detected anomalies and predicted consumption patterns.

DATA AVAILABILITY STATEMENT

The data presented in this study are available on request from the corresponding author.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest in this work.

REFERENCES

[1] T. Zhukabayeva, Z. Ahmad, A. Adamova, N. Karabayev, and A. Abdildayeva, "An Edge-Computing-Based Integrated Framework for Network Traffic Analysis and Intrusion Detection to Enhance Cyber–Physical System Security in Industrial IoT," Sensors, vol. 25, no. 8, p. 2395, Apr. 2025, doi: 10.3390/s25082395.

[2] M. J. C. S. Reis and C. Serôdio, "Edge AI for Real-Time Anomaly Detection in Smart Homes," Futur Internet, vol. 17, no. 4, p. 179, Apr. 2025, doi: 10.3390/fi17040179.

[3] A. Naouri, H. Wu, N. A. Nouri, S. Dhelim, and H. Ning, "A Novel Framework for Mobile-Edge Computing by Optimizing Task Offloading," *IEEE Internet Things J*, vol. 8, no. 16, pp. 13065–13076, Aug. 2021, doi: 10.1109/JIOT.2021.3064225.

[4] H. Liao, Y. Mu, Z. Zhou, M. Sun, Z. Wang, and C. Pan, "Blockchain and Learning-Based Secure and Intelligent Task Offloading for Vehicular Fog Computing," *IEEE Trans Intell Transp Syst*, vol. 22, no. 7, pp. 4051–4063, Jul. 2021, doi: 10.1109/TITS.2020.3007770.

[5] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach," *Neurocomputing*, vol. 387, pp. 51–62, Apr. 2020, doi: 10.1016/j.neucom.2019.11.016.

[6] G. Marín, P. Caasas, and G. Capdehourat, "DeepMAL - Deep Learning Models for Malware Traffic Detection and Classification," in *Data Science – Analytics and Applications*, Wiesbaden: Springer Fachmedien Wiesbaden, 2021, pp. 105–112. doi: 10.1007/978-3-658-32182-6_16.

[7] F. Martinez-Plumed *et al.*, "CRISP-DM Twenty Years Later: From Data Mining Processes to Data Science Trajectories," *IEEE Trans Knowl Data Eng*, vol. 33, no. 8, pp. 3048–3061, Aug. 2021, doi: 10.1109/TKDE.2019.2962680.

[8] M. Seyedan and F. Mafakheri, "Predictive big data analytics for supply chain demand forecasting: methods, applications, and research opportunities," *J Big Data*, vol. 7, no. 1, p. 53, Dec. 2020, doi: 10.1186/s40537-020-00329-2.

[9] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simul Model Pract Theory*, vol. 101, p. 102031, May 2020, doi: 10.1016/j.simpat.2019.102031.

[10] A. Aleran, H. Almukhalfi, A. Noor, R. Alluhaibi, A. Hafez, and T. H. Noor, "An IoT-Based Predictive Maintenance Framework Using a Hybrid Deep Learning Model for Smart Industrial Systems," *Comput Mater Contin*, pp. 1–10, 2025, doi: 10.32604/cmc.2025.070741.

[11] U. Khadam, P. Davidsson, and R. Spalazzese, "A systematic literature review on AI in IoT systems: Tasks, applications, and deployment," *Internet of Things*, vol. 34, p. 101779, Nov. 2025, doi: 10.1016/j.iot.2025.101779.

[12] L. Tian, S. Santi, A. Seferagić, J. Lan, and J. Famaey, "Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11ah research," *J Netw Comput Appl*, vol. 182, p. 103036, May 2021, doi: 10.1016/j.jnca.2021.103036.

[13] D. kumar sah, M. Vahabi, and H. Fotouhi, "Federated learning at the edge in Industrial Internet of Things: A review," *Sustain Comput Informatics Syst*, vol. 46, p. 101087, Jun. 2025, doi: 10.1016/j.suscom.2025.101087.

[14] O. O. Tooki and O. M. Popoola, "A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems," *Renew Energy Focus*, vol. 51, p. 100628, Oct. 2024, doi: 10.1016/j.ref.2024.100628.

[15] G. S. Rady, S. S. Mohamed, M. F. Mohamed, and K. F. Hussain, "High dimensional autonomous computing on Arabic language classification," *Comput Electr Eng*, vol. 100, p. 108020, May 2022, doi: 10.1016/j.compeleceng.2022.108020.

[16] S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security," *Internet of Things*, vol. 28, p. 101336, Dec. 2024, doi: 10.1016/j.iot.2024.101336.

[17] A. Tripathi, P. Upadhyay, and P. K. Goel, "Deep Learning for Anomaly Detection in Industrial Networks," 2025, pp. 103–130. doi: 10.4018/979-8-3373-3241-3.ch006.

[18] E. Villar-Rodriguez, M. A. Pérez, A. I. Torre-Bastida, C. R. Senderos, and J. López-de-Armentia, "Edge intelligence secure frameworks: Current state and future challenges," *Comput Secur*, vol. 130, p. 103278, Jul. 2023, doi: 10.1016/j.cose.2023.103278.

[19] G. C. Shwethashree and S. Manjula, "Adaptive Cyberattack Detection in IoT-Edge-Cloud Environments Using Decision Tree Regressor," *Eng Technol Appl Sci Res*, vol. 15, no. 4, pp. 25432–25437, Aug. 2025, doi: 10.48084/etasr.11184.

[20] M. Ozdem, "A novel approach for real-time anomaly detection in dynamic computer networks using temporal graph networks and explainable artificial intelligence," *Alexandria Eng J*, vol. 132, pp. 369–382, Nov. 2025, doi: 10.1016/j.aej.2025.11.001.

BIOGRAPHIES OF AUTHORS

Praveen Gujjar is an Associate Professor and Area Head in Business Analytics at CMS Business School, JAIN (Deemed-to-be University). Throughout his career, he has trained numerous senior and mid-level executives from various industries, bridging the gap between academic knowledge and practical application in Business Analytics. He can be contacted at email: dr.praveengujjar@cms.ac.in

Raghavendra M Devadas is an Assistant Professor (Sr Scale) at Manipal Institute of Technology, MAHE, Bengaluru, Karnataka, India. He previously served as Assistant Professor and Academic Coordinator at Presidency University, Bengaluru. He has also worked as a Software consultant for Tata Consultancy Services on Mainframes Technology, Chennai. He completed his Ph.D. from Visvesvaraya Technological University. He has in his name two patents filed and two grants received. He can be contacted at email: raghudevdas@gmail.com.

Nikitha K is a Research Assistant and PhD scholar at Jain University, specializing in analytics research and academic writing. It focuses on advancing knowledge in the field through rigorous research and insightful publications. She can be contacted at email: nikitha_k@cms.ac.in.