INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 08 Issue 11 November 2025

DOI: 10.47191/ijmra/v8-i11-25, Impact Factor: 8.266

Page No. 6120-6129

Efficient Intrusion Detection using Feature Engineering Based on Deep Spectral Artificial Neural Network for IOT Network

Sri Sai Krishna Mukkamala

Senior Software developer, T-Mobile, Phoenix, Arizona, USA

ABSTRACT: Recently, the Internet of Things (IoT) and its wide range of applications have become one of the most popular and most researched areas. By implementing appropriate safety features and efficient security management techniques, as well as by efficiently monitoring Internet traffic with intrusion detection systems, IoT settings offer an additional defense against attacks on the Internet and connected devices. Detecting new threats, preserving massive data centers, and responding to real-time threat detection are all complex tasks for traditional Intrusion Detection Systems (IDS). However, IoT devices present the highest security challenges due to their lower cost and accuracy. To solve this problem, we propose a Deep Spectral Artificial Neural Network (DSANN) algorithm to detect attacks for IoT networks and provide an efficient IDS. Furthermore, the Z-Score Min-Max Normalization (ZSM^2N) model can pre-process data by removing redundant data and mitigating the impact of outliers. Additionally, the best feature subset can be selected from a high-dimensional NSL-KDD dataset using the Enhanced Particle Swarm Optimization (EPSO) algorithm. Finally, the accuracy can be improved by classifying the attacks on IoT networks into normal and abnormal traffic and building an efficient IDS using the proposed DSANN algorithm. Furthermore, using the proposed DSANN model to classify IoT network threats has increased to 97.32% by improving the performance evaluation, such as accuracy, precision, recall, and time complexity.

KEYWORDS: Internet of Things, IDS, NSL-KDD dataset network traffic, DSANN and EPSO.

I. INTRODUCTION

In recent decades, a revolution in computing has led to the development of advanced technology and communication between smart devices. The IoT facilitates in-house communication using sensor devices, a technology that is also gaining popularity in everyday life in the modern world [1]. The IoT devices rely on the Internet as their primary communication channel and transmit extensive data within the network with the minimum amount of human intervention. The effects of international interconnection and the exchange of information have far-reaching consequences in the field of education, commerce, health systems, military strength, international trade, farming, and internal use. Extraordinary security dilemmas characterize the IoT because of the enormous connectivity of mixed devices, insecure network infrastructure, and international data disclosure.

The concept of the IoT is used as a set of many interconnected devices and networks to connect people and things, creating favorable conditions for transportation systems, communities, health, energy, and other potential applications [2]. Therefore, the role of IDS is crucial, as it is the only means to detect anomalies and attacks within the system. Distributed computing is proposed as an effective and scalable security solution for detecting abnormalities in the IoT phase.

In the recent times, the use of IDS based on artificial intelligence (AI) in the IoT has also begun to emerge. Such systems are capable of auto learning and identifying common behavioral patterns of a network and can successfully identify abnormal behaviors [3]. An IDS has the capability of preventing attacks on IoT devices through the identification of intrusions and alerting the attackers to abnormal procedures before they can intrude on the IoT. Furthermore, it can detect attack signatures through automatic and intelligent means to detect possible security threats. Deep learning models are based on massive traffic data that is used to generate effective IDS models and distinguish normal and abnormal network activities.

Nevertheless, the IoT and distributed networks pose threats to IDS due to their intricate data processing and discrepancies [4]. Specifically, intrusion detection traditions face challenges with the spatiotemporal characteristics of features and the inequity of data. Therefore, they are not suitable for the problematic intrusion detection in complex network traffic. IoT's ease of use makes it vulnerable to cyberattacks, necessitating robust security measures [5]. As the technology evolves, vulnerability detection and

awareness become increasingly important. IoT's open nature and resource limitations create unique security challenges, predisposing it to breaches and targeted attacks.

A. Organization of the research

- The main contribution of this paper is that we can classify IoT network traffic attacks using the NSL-KDD IDS dataset collected from Kaggle.
- Furthermore, we can pre-process the data by removing redundant data using ZSM2N technique with input features in the dataset and reducing the impact of outliers.
- After that, the EPSO algorithm is used to select an optimal feature subset from the NSL-KDD dataset, reducing computational cost.
- In addition, we can improve accuracy by building an efficient IDS that classifies attacks on IoT networks into normal and abnormal traffic.

B. Objective of the research

This paper objective to develop efficient IDS for IoT networks using NSL-KDD dataset. It uses ZSM2N preprocessing to remove redundant data and reduce the influence of outliers, and then uses the EPSO algorithm to select the most relevant features. This study aims to improve the accuracy of classifying IoT network traffic into normal and abnormal types by reducing the computational cost and focusing on the main features.

C. Motivation of the Research

- This paper enhances IDS for IoT networks by tackling challenges related to high-dimensional data, redundant features, and outliers within the NSL-KDD dataset.
- The intelligent IDS model employs ZSM2N preprocessing for data cleaning and normalization.
- Uses the EPSO algorithm to select key features, reducing computational overhead.
- The system classifies IoT network traffic to protect against cyberattacks and improve the reliability of IoT environments.

II. LITERATURE SURVEY

Introduces a comprehensive comparison of experimental designs, analysis, and IDS techniques based on Deep Learning (DL) models, such as datasets, feature extraction, and classifiers [6]. Additionally, the suggested technique can detect attacks more quickly than the standard algorithm, according to the results of comparing the new DL model to the device-based IDS (DIDS) standard algorithm [7]. The use of a standard dataset for IoT intrusion detection is evaluated using a DL model [8] based on Convolutional Neural Networks (CNNs). To improve anomaly detection in IoT, Feature Extraction using CNN implementation in IoT (FECNNIoT) is designed. Moreover, two key datasets, such as NSL-KDD and TON-IoT, are implemented for detecting IDS attacks [9]. Smart IDSs can detect IoT attacks by using DL algorithms to identify malicious network traffic [10].

To enhance each Deep Neural Network (DNN) model's distinct strengths and raise the overall capabilities of IDS, several strategies are presented. Interconnected systems, however, present serious security risks and decreased accuracy, even though they are convenient and efficient [11]. To increase accuracy in detecting IDS attacks and preventing security issues, a total of 21 neural network models were created and trained using the BoT-IoT dataset [12]. However, advanced analysis of data is required due to traditional security limits in attack and system variability. To improve intrusion detection, this study [13] proposed a real-time threat detection system for IoT based on DL, using 1D-CNN and Recurrent Neural Network (RNN) algorithms. The novel suggested an SDN-enabled IDS for IoT networks that uses a Long-Short-Term Memory (LSTM)-based method to identify network attacks [14]. Therefore, the existence of IoT devices complicates network management.

Table I. IOT NETWORK FOR IDS USING DEEP LEARNING ALGORITHM

SS	Year	Classification Method	Dataset	Performance Evaluation	Limitations
A.Fatani [15]	2025	CNN	KDDCup-99	Recall-78.2%, accuracy-71.22%	Cyber-attacks are growing at a rapid pace as security mechanisms fail to provide effective solutions.
Ali, M.A [16]	2025	Support Vector Machine (SVM)	MitM attack traffic dataset	highest accuracy (94%), false	These attacks threaten the integrity of

				positive rates-85.7%	intercepting communications
Elnakib [18]	2023	Generative Adversarial Network (GAN), CNN and LSTM	CICIDS2017 dataset	accuracy of 95%	IoT network attacks require adaptation of defenses due to resource constraints.
Islam [19]	2021	DNN, Deep Belief Network (DBN)	IoTDevNet, DS2OS, IoTID20, and IoT Botnet dataset.	Recall-92.3%, F1-score-87.28%	Node diversity in IoT raises security concerns.
Khan [20]	2021	k-Nearest Neighbour (kNN), Naive Bayes (NB)	MQTT-IoT-IDS2020	highest accuracy of 79.13%	Low bandwidths and memory
Musleh [21]	2023	VGG-16 and DenseNet.	Dataport dataset.	Highest accuracy of 88.3%.	Focuses on protecting vulnerable devices from malicious traffic.
Bhavsar, [22]	2023	Pearson-Correlation Coefficient - CNN (PCC-CNN)	NSL-KDD, CICIDS-2017	misclassification rate-0.02, 0.02, and 0.00	Securing IoT devices is critical due to increasing cybersecurity threats.
Idrissi [23]	2021	RNN, CNN	Bot-IoT dataset	validation loss-0.58% and prediction execution time-0.34 ms	The rise of botnet attacks presents many challenges to developing IDS.

As shown in Table 1, the classification method, performance valuation of the dataset, and threshold value are used to predict IoT network attacks for IDS based on the DL method.

Experimental results using an ANN based on existing DL models showed better results compared to leading methods and achieved 94.12% accuracy [24]. Similarly, experimental results show that compared to known classification methods [25], the G-average of the offered method is 78%, that of KNN is 75%, and the G-average of other methods is less than 50%.

III. PROPOSED METHODOLOGY

The proposed method constructs a DSANN to develop an efficient IDS for IoT networks. First, we pre-process the data using the ZSM2N method to remove redundancy and minimise outliers. Then, we use the EPSO algorithm to select the most relevant features from the NSL-KDD dataset. Finally, the DSANN model can classify IoT traffic into normal or abnormal categories, improving detection accuracy and system reliability.

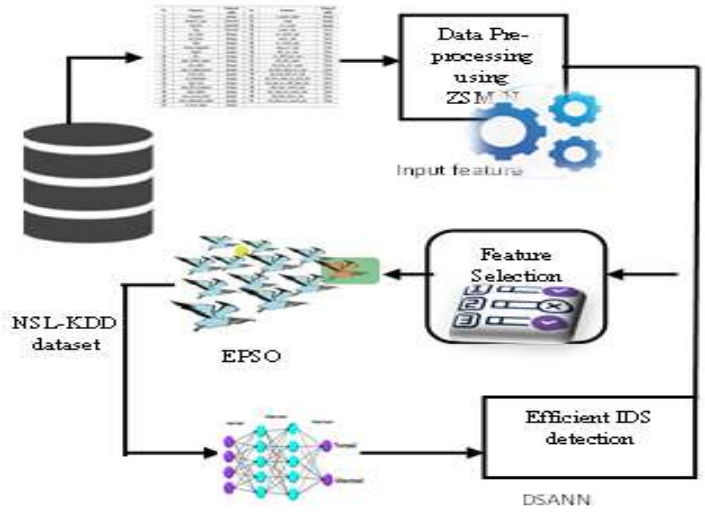

Fig. 1. Proposed DSANN Method based on Architecture Diagram

As shown in Figure 1, a new method is proposed in IoT networks that focuses on constructing a specially designed DSANN to develop an efficient IDS. Protecting the integrity and availability of IoT devices and data, the primary objective is to accurately and reliably distinguish normal and abnormal network traffic. The method begins with an essential data pre-processing step, where the ZSM2N method is used to carefully prepare the NSL-KDD dataset, which serves as the basis for training and evaluating the IDS. ZSM^{2}N techniques play a key role in refining datasets by removing redundant information and reducing the influence of outliers, thereby ensuring that subsequent analyses are based on high-quality and representative data. Following the pre-processing step, feature selection is performed to identify the most suitable features from the NSL-KDD dataset. This is achieved by using a sophisticated optimization technique called the EPSO algorithm. The EPSO algorithm intelligently selects a subset of the most relevant features to accurately classify network traffic, thereby reducing the computational complexity of the DSANN model and improving its generalization performance. The model is designed to categorize IoT network traffic into two distinct categories: normal and abnormal. DSANN models leverage the power of the DSANN algorithm within network traffic data, helping to detect malicious activity accurately.

A. Dataset Collection

This dataset shows the design and features of the NSL-KDD dataset, a benchmark for evaluating IDSs. It contains 4431 network traffic records, each of which is described by 41 attributes related to connections, protocol behaviour, and time- and content-based traffic patterns. Furthermore, the accuracy is improved by evaluating the training and testing set, which includes 3,503 records and 928 records from the total records collected through the NSL-KDD dataset. Moreover, the NSL-KDD dataset can be accessed through the website https://www.kaggle.com/datasets/programmer3/nsl-kdd-intrusion-detection-dataset.

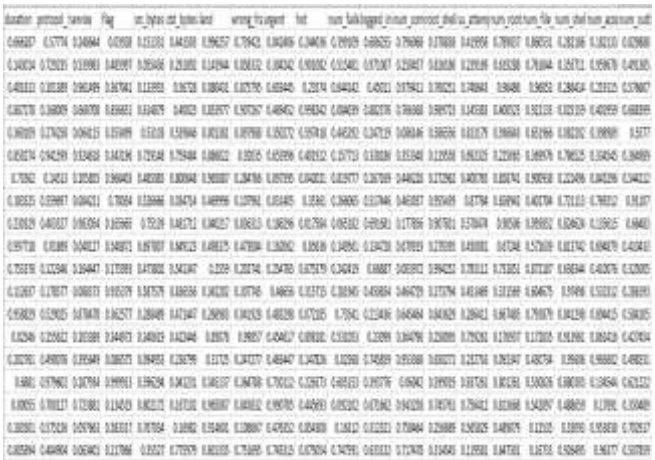

Fig. 2. Dataset Feature Collection

As shown in Figure 2, each record obtained through the dataset feature collection represents normal and stable network activity. Also, traffic collected from the dataset can be labeled as DoS, Probe, U2R, or R2L, which categorizes normal and abnormal traffic attacks.

B. Z-score Min-Max Normalizztion (Z-SM²N)

In this section, the Z-SM2N model is used to preprocess the data, remove redundant data in the dataset, and reduce the impact of extreme values. In NSL-KDD, a feature measurement step is used when preprocessing network traffic data to analyze the input dataset. In addition, during min-max normalization, feature values in the dataset can be rescaled to a fixed range [0,1]. Additionally, the Z-SM2N model accelerates the convergence of input values within a fixed range and increases stability.

As shown in Equation 1, the eigenvalues are calculated by minimum-maximum normalization of the rescaling to a fixed range. Let's assume a −original feature value, a' −normalized data, $a_{max} - a_{min}$ −minimum and maximum value.

$$a' = \frac{a - a_{min}}{a_{max} - a_{min}} \quad (1)$$

The estimated standard deviation between the z-score standards is characterized by a mean of zero and a variance of one, as shown in Equation 2. Let's assume μ −mean value, σ −standard deviation.

$$a' = \frac{a - \mu}{\sigma} \quad (2)$$

The ZSM2N model detects outliers and removes unwanted features, reducing the influence of extreme values and ensuring that all features are centered at zero.

C. Enhanced Particle Swarm Optimization (EPSO)

This section uses the EPSO algorithm to select the optimal feature subset from the high-dimensional NSL-KDD dataset to improve the IDS detection performance and reduce the computational cost. Using the dataset of IoT-based IDS, each particle of the EPSO technique chooses an appropriate subset of 41 features, including period, protocol_type, service, src_bytes, dst_bytes, and statistical features like count and srv_count. The search space is guided by neighborhood information to analyze its own best position (pBest), swarm best position (gBest), and best feature combination. The fitness function optimizes feature selection for IDS classification accuracy, while the EPSO model minimizes computational cost. Similarly, the best subset of features can be selected by choosing the most appropriate features to detect normal and attack traffic in IoT networks.

Compute a candidate feature subset of 41 features for each particle in the particle representation, as shown in Equation 4. Let's assume a_m − position vector of particle.

$$a_m = a'[a_{m1}, a_{m2}, a_{m3} \dots, a_{m41}] \quad (4)$$

As illustrated in Equation 5, estimate the fitness function to maximize the improvement in IDS classification accuracy for a subset of the selected features. Let's assume S_F −selected feature, C −classifier, F −fitness function.

$$F(x_i) = Acc\left(C\left(S_F(a_m)\right)\right) \quad (5)$$

Update global, neighbour, and personal best velocities as shown in Equation 6. Let's assume d_m^{l+1} −current velocity of particle, m −iteration, a_m^l −current position, z − inertia weight, C −coefficients, r −random number, $Pbest_m$ −particle position, $gbest_m$ −global best position, $Nbest_m$ −neighbour position.

$$d_m^{l+1} = z.d_m^l + C_1.r_1\left(Pbest_m.a_m^l\right) + C_2.r_2\left(gbest_m.a_m^l\right) + C_3.r_3\left(Nbest_m.a_m^l\right) \quad (6)$$

As shown in Equations 7and 8, use a sigmoid function to convert the velocity into a binary feature selection to update the position. Let's assume a_{mn}^{l+1} −updated selection of feature particle, $rand\ ()$ −random number between 0 and 1

$$a_{mn}^{l+1} = \begin{cases} 1, & \text{if sigmoid } \left(d_{mn}^{l+1}\right) > \text{rand } () \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

$$\text{Sigmoid}(v) = \frac{1}{1+e^v} \quad (8)$$

As shown in Equation 9, the optimal feature subset is calculated by iterating through fitness evaluation, velocity update, and position update for a maximum number of iterations. Let's assume $a_{optimal}$ −**selected features** maximize IDS accuracy.

$$a_{optimal} = g_{best} \quad (9)$$

The EPSO is used to demonstrate particle representation, fitness assessment, velocity/position updating, and convergence on the NSL-KDD dataset.

D. Deep Spectral Artificial Neural Network (DSANN)

This section developed an efficient IDS using the proposed DSANN algorithm to detect and classify attacks for IoT networks. The DSANN method combines spectral feature extraction with deep neural learning to capture frequency-based and non-linear relationships in the data. By applying DSANN to the NSL-KDD dataset, the model can automatically learn meaningful

patterns from the selected features and improve its ability to distinguish normal traffic from various types of network attacks. This DSANN approach minimizes manual feature engineering and improves the accuracy and reliability of IDS in IoT environment.

The spectral function is evaluated to optimize the frequency-based or correlation-based methods as described in Equation 10. Let's assume q −spectral feature, Φ − spectral transformation function.

$$q = a_{optimal}\,\Phi(a) \quad (10)$$

Calculate the weighted shift for each hidden layer as described in Equation 11. Let's assume $f^{(t)}$ −output of hidden layer, $z^{(t)}, y^{(t)}$ −weights and bias of layer, h −activation function.

$$f^{(t)} = h\left(z^{(t)} f^{t-1} + y^{(t)}\right) \quad (11)$$

The output layer is evaluated, and the final softmax layer traffic is classified as either normal (0) or attacked, as presented in Equation 12. Let's assume $\widehat{b_t}$ −predicted probability of class, o − number of output classes.

$$\widehat{b_t} = \frac{g^{w_m}}{\sum_{n=1}^{o} g^{w_m}}, \quad w = Z^{(t)} f^{(t-1)} + y^{(t)} (12)$$

As shown in Equation 13, the loss function is estimated using cross-entropy loss, and the model parameters are optimized. Let's assume t −loss function, b_m −true class label.

$$T = -\sum_{m=1}^{o} b_m \log\left(\widehat{b_t}\right) \quad (13)$$

Update the optimization parameters using gradient descent as shown in Equation 14. Let's assume θ − network parameters, η − learning rate.

$$\theta \leftarrow \theta - \eta . \nabla_\theta T \quad (14)$$

By combining spectral feature extraction with deep neural learning, DSANN can effectively develop an IDS for IoT networks. This approach automatically learns traffic patterns from the NSL-KDD dataset, which enables accurate classification of network traffic as normal or attack.

IV. RESULT AND DISCUSSION

Using performance parameters including accuracy, precision, recall, and time complexity, this part improves the IDS for IoT network traffic detection using the suggested DSANN model. Furthermore, when compared to earlier techniques like DenseNet, LSTM, and PCC-CNN, the suggested DSANN method greatly increases accuracy.

Table II. SIMULATION PARAMETER

Simulation	Variable
Dataset Name	NSL-KDD Intrusion Detection Dataset
Number of dataset	4431
Language	Python
Tool	Jupyter
Training	3503
Testing	928

The parameters described in Table 2 were used to simulate the suggested system. Using Python and the NSL-KDD Intrusion Detection Dataset, which had 101 records from various sources, experiments were carried out in a Jupyter environment.

Table III. PERFORMANCE OF PRECISION

Number of Records	DenseNet	LSTM	PCC-CNN	DSANN
1,107	71.12	73.14	74.21	76.10
2,214	74.3	76.12	79.11	81.09
3,321	76.1	79.05	82.48	86.02
4,431	79.16	83.28	86.11	90.23

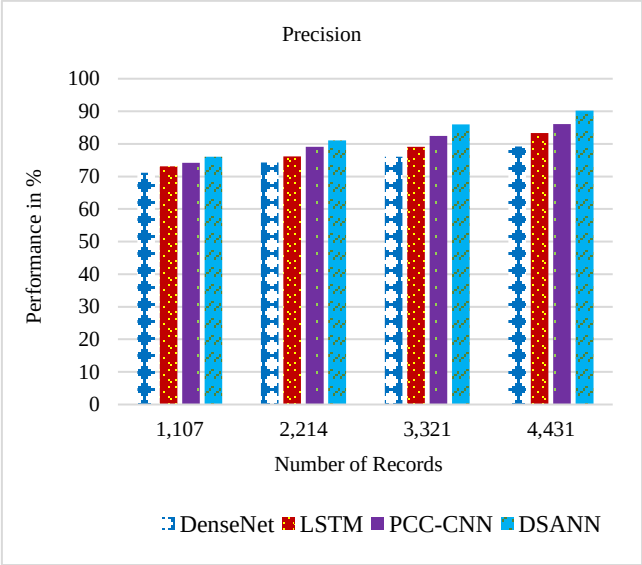

Fig. 3. Analysis of Precision

Figure 3 and Table 3 demonstrate that the proposed DSANN method accurately measures precision compared to traditional approaches, thereby enhancing IDS performance through the detection of IoT network traffic. When compared to the conventional DenseNet, LSTM, and PCC-CNN techniques, the PSO-KNN approach achieved precision rates of 79.16%, 83.28%, and 86.11%, respectively, during classification. Furthermore, the DSANN method improves analysis efficiency and increases precision by 90.23% for IDS in IoT network traffic detection.

Table IV. PERFORMANCE OF RECALL

Number of Records	DenseNet	LSTM	PCC-CNN	DSANN
1,107	73.16	76.2	79.25	83.12
2,214	76.22	79.18	82.9	86.3
3,321	79.15	81.9	84.10	89.47
4,431	81.28	84.11	87.15	93.13

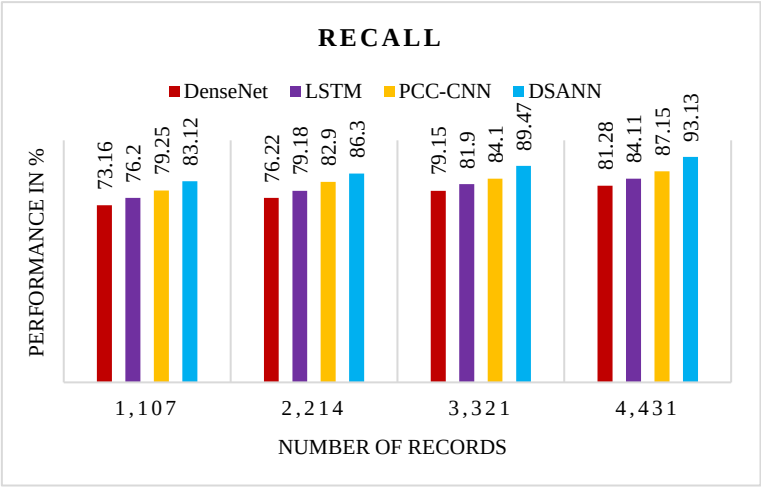

Fig. 4. Analysis of Recall

Figure 4 and Table 4 show that the proposed DSANN method can accurately measure recall compared to traditional approaches and boost IDS performance by detecting IoT network traffic. When compared to the conventional DenseNet, LSTM, and PCC-CNN techniques, the PSO-KNN approach achieved recall rates of 81.28%, 84.11%, and 87.15%, respectively, during classification.

Furthermore, the DSANN method improves analysis efficiency and increases recall by 93.13% for IDS in IoT network traffic detection.

Table V. PERFORMANCE OF TIME COMPLEXITY

Number of Records	DenseNet	LSTM	PCC-CNN	DSANN
1,107	39.21	34.03	31.12	25.11
2,214	36.17	32.05	25.14	19.09
3,321	33.2	29.06	21.09	14.05
4,431	30.14	27.15	20.10	10.05

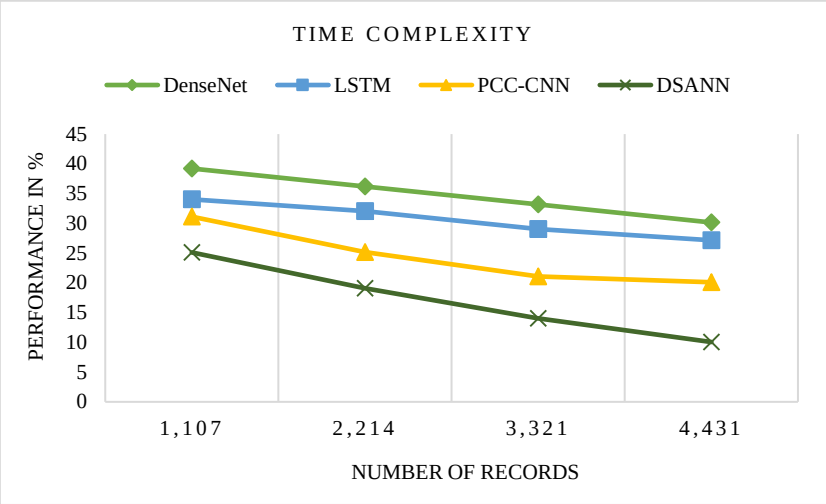

Fig. 5. Analysis of Time Complexity

Figure 5 and Table 5 show that the proposed DSANN method accurately measures the time complexity compared to traditional approaches and improves the IDS performance through IoT network traffic detection. Compared to the traditional DENSNET, LSTM, and PCC-CNN techniques, the BSO-KNN approach achieved 79.16%, 83.28%, and 86.11% of the time in problem classification, respectively. Moreover, the DSANN method improves the analysis efficiency and increases the time complexity of IDS by 90.23% in IoT network traffic detection.

Table VI. PERFORMANCE OF ACCURACY

Number of Records	DenseNet	LSTM	PCC-CNN	DSANN
1,107	73.2	77.56	80.5	83.25
2,214	76.4	80.28	83.26	86.17
3,321	80.36	84.9	86.14	90.12
4,431	84.24	89.13	90.26	94.28

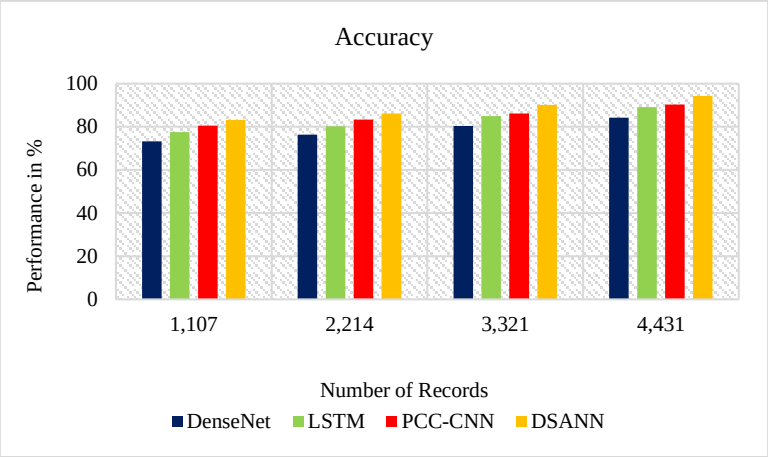

Fig. 6. Analysis of Accuracy

Figure 6 and Table 6 validate the effectiveness of the proposed DSANN method in assessing accuracy and improving IDS for IoT network traffic detection. In classification, DSANN achieved accuracy rates of 84.24%, 89.13%, and 90.26% compared to DenseNet, LSTM, and PCC-CNN, respectively. DSANN also enhances analysis efficiency and improves accuracy by 94.28% for IDS in IoT network traffic detection.

V. CONCLUSION

In conclusion, this paper demonstrates the value of classifying attacks targeting IoT network traffic by using the valuable resource NSL-KDD Intrusion Detection dataset obtained from Kaggle. This study highlights the importance of data preprocessing, particularly using ZSM2N techniques to remove redundant data in the input features of the dataset. This preprocessing step plays a vital role in reducing the negative impact of outliers, thereby improving the quality of data used for subsequent analysis. Furthermore, we use the EPSO algorithm as a means to select the most relevant and influential subset of features from the NSL-KDD dataset. This feature selection process helps in reducing the overall computational cost associated with the classification task. The proposed DSANN method has been proven to be very effective in accurate estimation and significantly improves the IDS functionality for IoT network traffic detection. In attack classification, DSANN shows its superiority by achieving better accuracy rates of 84.24%, 89.13%, and 90.26%, respectively, compared to alternative deep learning architectures such as DenseNet, LSTM, and PCC-CCNN. DSANN contributes to improving not only the accuracy but also the analysis capability, significantly improving the overall accuracy of IDS in IoT network traffic detection, helping to achieve an accuracy of 94.28%.

A. Limitation of the research

- The complexity and variability of actual IoT traffic may not be well captured by using benchmark datasets.
- This system relies heavily on predefined capabilities, which can lead to performance variations when applied to dynamic and evolving attack patterns.
- This approach can be computationally intensive when scaling to very large or heterogeneous IoT environments.
- These limitations highlight the need for further efforts to improve adaptability, scalability and real-time performance in practical deployment scenarios.

B. Future Work

- The application of intelligent IDS to IoT networks with dynamic topologies will be the primary focus of future research.
- This IDS model can serve as a benchmark for the network and security research community in developing DL-based IDS solutions.
- Furthermore, a real-time assistance tool could be developed to enhance IoT network performance.

REFERENCES

1) Jayalaxmi, P. L. S., et al. "Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey." IEEe Access 10 (2022): 121173-121192.
2) Karne, RadhaKrishna and Mounika, S. and V, KarthikKumar and Dr. Nookala, Venu, Applications of IoT on Intrusion Detection System with Deep Learning Analysis (July 2022). International Journal from Innovative Engineering and Management Research (IJIEMR) 2022, Available at SSRN: https://ssrn.com/abstract=4232107

3) H. Liao et al., "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," in IEEE Access, vol. 12, pp. 4745-4761, 2024, doi: 10.1109/ACCESS.2023.3349287.
4) Zhang, Y., Muniyandi, R. C., & Qamar, F. (2024). A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance. Applied Sciences, 15(3), 1552. https://doi.org/10.3390/app15031552.
5) Haripriya A P, Meenu V, Malavika M Hari, Risvana K A, Sruthi P R, "A Survey on Machine and Deep Learning Based Intrusion Detection Systems for IoT", ISSN: 2321-9653, Publish Date: 2023-06-22, DOI Link: https://doi.org/10.22214/ijraset.2023.5435.
6) H. Liao et al, "Survey of Deep Learning Technologies for Intrusion Detection in IoT", VOLUME 12, 2024, Digital Object Identifier 10.1109/ACCESS.2023.3349287.
7) Madhu, B., Venu Gopala Chari, M., Vankdothu, R., Silivery, A. K., & Aerranagula, V. (2023). Intrusion detection models for IOT networks via deep learning approaches. Measurement: Sensors, 25, 100641. https://doi.org/10.1016/j.measen.2022.100641
8) Banaamah, A. M., & Ahmad, I. (2021). Intrusion Detection in IoT Using Deep Learning. Sensors, 22(21), 8417. https://doi.org/10.3390/s22218417
9) Asgharzadeh, H., Ghaffari, A., Masdari, M. et al. An Intrusion Detection System on The Internet of Things Using Deep Learning and Multi-objective Enhanced Gorilla Troops Optimizer. J Bionic Eng 21, 2658–2684 (2024). https://doi.org/10.1007/s42235-024-00575-7.
10) Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2021). Intrusion Detection System on IoT with 5G Network Using Deep Learning. Wireless Communications and Mobile Computing, 2022(1), 9304689. https://doi.org/10.1155/2022/9304689
11) Mehdi Selem, Farah Jemili, "Deep Learning for Intrusion Detection in IoT Networks", April 2024, DOI:10.21203/rs.3.rs-4306367/v1.
12) Zhang, H. Development of an intelligent intrusion detection system for IoT networks using deep learning. Discov Internet Things 5, 74 (2025). https://doi.org/10.1007/s43926-025-00177-7
13) Md. Alamgir Hossain, "Deep Learning-Based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach", March 2025, DOI:10.21203/rs.3.rs-6042512/v1.
14) Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2022). Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks. Information, 14(1), 41. https://doi.org/10.3390/info14010041
15) A. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," in IEEE Access, vol. 9, pp. 123448-123464, 2021, doi: 10.1109/ACCESS.2021.3109081.
16) Ali, M.A., Al-Sharafi, S.A.H. Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation. Discov Internet Things 5, 48 (2025). https://doi.org/10.1007/s43926-025-00104-w.
17) Saba, Tanzila, et al. "Anomaly-based intrusion detection system for IoT networks through deep learning model." Computers and Electrical Engineering 99 (2022): 107810.
18) Elnakib, Omar, et al. "EIDM: deep learning model for IoT intrusion detection systems." Journal of Supercomputing 79.12 (2023).
19) Islam, Nahida, et al. "Towards machine learning based intrusion detection in IoT networks." Comput. Mater. Contin 69.2 (2021): 1801-1821.
20) Khan, Muhammad Almas, et al. "A deep learning-based intrusion detection system for MQTT enabled IoT." Sensors 21.21 (2021): 7016.
21) Musleh, Dhiaa, et al. "Intrusion detection system using feature extraction with machine learning algorithms in IoT." Journal of Sensor and Actuator Networks 12.2 (2023): 29.
22) Bhavsar, Mansi, et al. "Anomaly-based intrusion detection system for IoT application." Discover Internet of things 3.1 (2023): 5.
23) Idrissi, Idriss, et al. "Toward a deep learning-based intrusion detection system for IoT against botnet attacks." IAES International Journal of Artificial Intelligence 10.1 (2021): 110.
24) Pampapathi, B. M., Nageswara Guptha, and M. S. Hema. "Towards an effective deep learning-based intrusion detection system in the internet of things." Telematics and Informatics Reports 7 (2022): 100009.
25) Qaddoura, Raneem, et al. "A multi-layer classification approach for intrusion detection in iot networks based on deep learning." Sensors 21.9 (2021): 2987.