Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 3, June 2026, pp. 2527~2536
ISSN: 2302-9285, DOI: 10.11591/eei.v15i3.11674

Hybrid deep learning ensemble with score-based feature optimization for cyber attack detection in IoT systems

John Manoranjini[1], Venugopal Gaddam[2], Kotla Venkata Raghavender[3], Hanumantha Rao Battu[4], Pamarthi Sunitha[5], Sathish Kumar Shanmugam[6]

[1]Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India
[2]Department of Computer Science and Engineering (AI & ML), Bonam Venkata Chalamayya Engineering College, Odalarevu, India
[3]Department of Computer Science and Engineering, G. Narayanamma Institute of Technology and Science, Hyderabad, India
[4]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[5]Department of Electronics and Communication Engineering, Aditya University, Surampalem, India
[6]Department of Electrical and Electronics Engineering, M. Kumarasamy College of Engineering, Karur, India

Article Info

Article history:

Received Oct 20, 2025
Revised Apr 2, 2026
Accepted Apr 19, 2026

Keywords:

Ant lion optimization
Convolutional neural network
Cyber intrusion detection
Ensemble deep learning
Feature optimization
Internet of thing security
Random forest

ABSTRACT

The rapid growth of internet of things (IoT) devices have improved connectivity but also exposed networks to cyber threats. This study proposes a prediction-scoring-based ensemble deep learning model with prediction-scoring-optimized feature selection (EDLM-PSOFS) for intrusion detection in IoT systems. The model integrates random forest (RF) feature extraction with ant lion optimization (ALO)-tuned convolutional neural networks (CNNs) to balance accuracy and computational efficiency. Using the KDD Cup '99 dataset containing 4.9 million traffic records and 41 features, the framework achieved 97% accuracy, 0.99 precision, and 0.97 recall within five epochs. Comparative evaluation shows faster convergence and reduced complexity than gated recurrent units (GRU), long short-term memory (LSTM), and support vector machine (SVM) baselines, demonstrating suitability for real-time, resource-constrained IoT deployments.

Corresponding Author:

Venugopal Gaddam
Department of Computer Science and Engineering (AI & ML)
Bonam Venkata Chalamayya Engineering College
Odalarevu, Andhra Pradesh, India
Email: venugopal.gaddam@gmail.com

1. INTRODUCTION

The internet of things (IoT) has become an important technological ecosystem that connects smart devices, sensors, and actuators so that they can share data and make smart decisions in a wide range of fields, including healthcare, manufacturing, transportation, and smart cities [1]–[3]. Kevin Ashton first used the term "Internet of Things" in 1999 to talk about how physical objects could be connected to digital communication networks [2]. IoT technology has come a long way in the last twenty years. It now lets machines talk to each other, analyze data in real time, and use edge intelligence. But this digital growth has also brought about a new set of cybersecurity challenges because IoT devices are open, diverse, and limited in resources [4]. Market research says that the IoT industry will be worth about 11 billion USD worldwide by 2026, and that more than 50 billion devices will be connected by 2025 [5], [6]. This growth makes it easier to make decisions based on data and automate processes, but it also puts billions of nodes at risk of cyber attacks. IoT devices usually use lightweight communication protocols and have limited storage and computing power, which makes them very easy targets for hackers [7]. Attacks like distributed denial of service (DDoS), malware injection, SQL injection, and botnet infiltration can put user data at risk by making

it less private, less secure, and less available [8], [9]. These weaknesses are especially important because IoT devices often deal with private and business information. Kumar *et al.* [10] have thus stressed the necessity for intelligent intrusion detection systems (IDS) capable of identifying and counteracting evolving attack patterns in real time.

Traditional IDS models depend on signature-based or rule-based detection, which frequently does not identify zero-day and polymorphic attacks. To address this constraint, the research community has increasingly concentrated on machine learning (ML) and deep learning (DL) methodologies capable of autonomously extracting intricate behavioural attributes from network data [11]–[15]. ML methods like support vector machine (SVM), decision tree (DT), and random forest (RF) have been used to find strange traffic, but they usually rely on hand-crafted features and don't work as well when they have to deal with large IoT datasets. DL architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can automatically find nonlinear dependencies, but they need a lot of computing power and are very sensitive to how hyperparameters are set. So, the best IDS for IoT should be able to detect things with high accuracy, be easy on computers, and be able to adapt to changing data distributions. To overcome these limitations, researchers have utilized metaheuristic optimization algorithms for feature selection and model refinement. Particle swarm optimization (PSO), genetic algorithm (GA), and ant lion optimization (ALO) are some of the most popular methods because they can effectively search large solution spaces and avoid local optima [16], [17]. These algorithms can make DL work better by fine-tuning hyperparameters like the learning rate, batch size, and dropout ratio, as well as finding the most important features in traffic data. However, many hybrid frameworks that combine metaheuristics and DL have problems like computational overhead, slow convergence, and limited generalization across different datasets.

Raj and Pani [18] introduced a chaotic whale crow (CWC) optimization framework that integrates chaotic whale optimization (CWOA) and crow search algorithm (CSA) for secure routing in IoT, resulting in enhanced throughput and latency while concentrating solely on routing-level security. Adat and Gupta [19] offered a thorough analysis of IoT security, detailing a classification of vulnerabilities, challenges, and architectural solutions, while emphasizing the necessity for adaptive, multi-layered defense strategies. Gaber *et al.* [20] proposed an industrial IoT (IIoT) intrusion detection methodology employing PSO and the bat algorithm (BAT) for feature extraction, alongside RF for classification. The method worked well for accuracy, but it had trouble adapting to changing IoT environments. Sharifian *et al.* [21] created a sin-cos-based improved African vulture optimization algorithm (bIAVOA) that uses a gravitational fixed radius nearest neighbour (GFRNN) classifier to find DDoS attacks. It was accurate for some attacks, but it took a lot of processing power and was likely to overfit. Roopak *et al.* [22] proposed a multi-objective-based feature selection method for DDoS attack detection in IoT networks. Chaudhary *et al.* [23] created an IDS for fog-enabled IoT networks that used filter-based feature selection and J48 classifier. It had low latency but couldn't be expanded. Dahou *et al.* [24] suggested a reptile search algorithm (RSA) in conjunction with CNN for attack detection, but encountered difficulties regarding computational efficiency and adaptability to emerging threats. Krishna and Arunkumar [25] utilized a PSO–gray wolf optimization (GWO) hybrid for IoT intrusion detection employing RF classification; although they attained satisfactory accuracy, their model experienced convergence delays when processing large-scale data. Lightweight cryptographic and heuristic methods have also been created to work with IDS frameworks. Tewari and Gupta [26] presented a ultra-lightweight mutual authentication protocol for IoT devices that employs solely bitwise operations, thereby decreasing computational and communicative expenses while preserving privacy. Even though this work was cryptographic, it showed how important it is for IoT devices with limited resources to use energy-efficient algorithms. Saheed *et al.* [27] subsequently introduced a hybrid autoencoder-based model employing a modified particle swarm optimization (HAEMPSO) algorithm for feature selection and a deep neural network (DNN) for classification. Their system was very accurate, but it was hard to find the right balance between selection efficiency and model generalization.

Intelligent IDS for IoT have various problems that restrict their operational scalability and reliability, despite substantial advances. DL-based IDSs are accurate on benchmark datasets but have considerable computational overheads due to deep architectures and extensive parameterization, rendering them unsuitable for resource-restricted edge or fog contexts. Most metaheuristic-driven IDS frameworks lack adaptive control between exploration and exploitation, causing premature convergence and poor detection robustness under shifting attack distributions. Generalization across heterogeneous IoT topologies is another major issue. When subjected to different device types, communication protocols, and attack patterns, centralized or single-domain dataset models often perform poorly. Real-time IoT cybersecurity is hampered by this detection accuracy-computational efficiency imbalance. The need for a lightweight, adaptively optimized ensemble architecture is growing. For rapid, precise, and scalable detection in dynamic IoT settings, this system must synchronize feature selection, hyperparameter optimization, and ensemble inference. Advanced architectures like vision transformer-based IDS (ViTIDS) [28], gated graph neural

networks (GGNN-IDS) [29], and federated transformer-CNN hybrids [30] combine attention mechanisms for contextual learning. These models are computationally demanding and require considerable training data, making them unsuitable for real-time IoT nodes. Thus, prediction-scoring-based ensemble optimization and lightweight feature-driven learning make the ensemble deep learning model with prediction-scoring-optimized feature selection (EDLM-PSOFS) model an adaptive, resource-aware option that fills this research need.

2. METHOD

The proposed EDLM-PSOFS aims to provide an efficient, lightweight, and highly accurate framework for cyber-attack detection in IoT networks. This architecture combines feature selection, hyperparameter optimization, and ensemble DL inference to make sure that detection is strong while using as little processing power as possible. The principal novelty of the EDLM-PSOFS framework lies in its score-based ensemble aggregation integrated with feature-driven optimization. This dual mechanism achieves an equilibrium between computational lightness and detection precision, offering an efficient alternative to heavy multi-layer IDS models while preserving real-time responsiveness for edge IoT devices. Figure 1 present the overall framework architecture and application domains of the proposed EDLM-PSOFS system before the detailed processing stages are discussed. Figure 1(a) illustrates the conceptual workflow of the framework, including data collection, preprocessing, optimization, classification, and the final intrusion decision process, while Figure 1(b) highlights major IoT application areas such as smart homes, healthcare, smart cities, industrial IoT, smart grids, and transportation, emphasizing the growing need for robust cybersecurity solutions in real-time environments. Figure 2 shows how IoT applications are used in different fields, which shows how important it is to have strong cybersecurity solutions in a variety of real-time settings. The proposed EDLM-PSOFS framework begins with data preprocessing using the standard KDD Cup ’99 dataset, which contains labelled network traffic representing both benign and malicious activities. Initially, raw traffic attributes are normalized using min-max scaling to transform all features into a common range of [0, 1], thereby preventing features with larger magnitudes from dominating the learning process and ensuring balanced convergence during training. Subsequently, the normalized dataset is divided into training and testing subsets for effective model development and performance evaluation.

Although the KDD Cup ’99 dataset is a legacy benchmark, it continues to serve as a standard baseline for intrusion detection research owing to its well-labelled attack categories, balanced traffic representation, and compatibility with lightweight IoT-focused IDS frameworks. Moreover, its structured feature distribution allows the proposed EDLM-PSOFS model to validate detection performance with minimal preprocessing overhead. To ensure broader applicability, future work will include validation on recent datasets such as NSL-KDD and CICIDS-2017, which provide modern attack variants and richer protocol diversity.

Next, feature selection is very important for making detection more accurate and less complicated to compute. We use the RF algorithm to find the most discriminative attributes by calculating the mean decrease in impurity across several DTs. This choice cuts down on the number of dimensions in the data, cuts down on redundancy, and speeds up the DL process without hurting performance. After choosing the best feature subset, ALO is used to tune the hyperparameters of the DL model. ALO is a metaheuristic based on how antlions hunt, and it strikes a good balance between exploration and exploitation.

The ALO search space was constrained to empirically validated parameter bounds to ensure stability and convergence: learning rate $\in$ [0.0001–0.01]; dropout $\in$ [0.2–0.5]; batch size $\in$ {32, 64, 128}; convolutional filters $\in$ {16, 32, 64, 128}. The fitness objective minimized (1−accuracy), leading to optimal hyperparameter sets of learning rate=0.0012, dropout=0.3, batch size=64, and 64 filters per layer.

In the suggested model, each antlion stands for a possible CNN setup, which is determined by things like the learning rate, batch size, dropout ratio, and number of filters. Through repeated random walks and changing the boundaries as needed, ALO dynamically looks for the combination of parameters that makes the fitness function (1–accuracy) the lowest. This makes sure that the DL classifier converges as quickly as possible and improves both its accuracy and stability. The ensemble DL module is the main part of EDLM-PSOFS. It has several CNN sub-models, each trained on the best feature set but started with different random weights to encourage variety. Each CNN learns different patterns in IoT traffic data that are both spatial and temporal. During inference, the prediction-scoring mechanism takes the probability outputs from each CNN and adds them all together to get an average ensemble score for each attack class. The final choice is based on the category with the highest score, which makes the system more stable and less likely to make mistakes. This ensemble strategy reduces the biases of each learner and makes sure that predictions are consistent even when the network conditions change.

The design focusses on "lightweight computation," which makes it possible to use the model on IoT devices at the edge or in the fog. Tests showed that EDLM-PSOFS can find things with 97% accuracy in just

five epochs, which shows that it converges quickly and works well. In addition, combining optimised feature selection with adaptive parameter tuning cuts down on training time and memory use by a large amount compared to traditional DL frameworks. The proposed model improves cyber-attack detection accuracy and makes sure that scalability and adaptability are possible for next-generation IoT infrastructures that need real-time, resource-efficient intrusion detection.

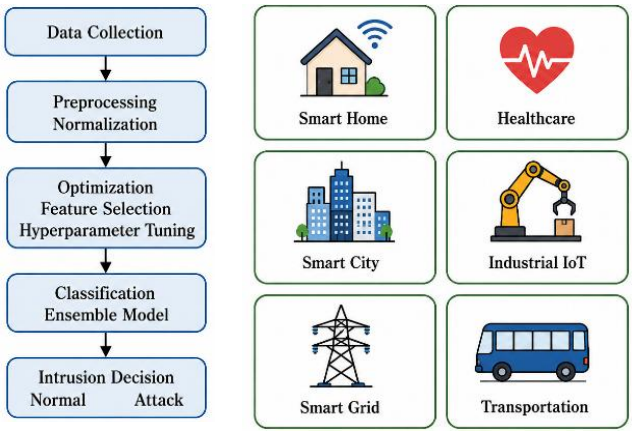

Figure 1. The proposed framework architecture for; (a) EDLM-PSOFS workflow and (b) IoT application domains

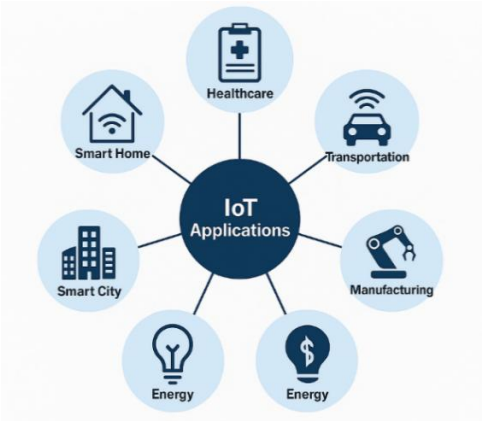

Figure 2. IoT application domains highlighting the need for robust cybersecurity solutions

3. SIMULATED RESULTS

The suggested EDLM-PSOFS framework was put into action and tested using the KDD Cup '99 dataset on a Python-based platform that ran on an Intel i5 processor with an RTX 3050 GPU. The goal of the experimental analysis was to see if the prediction-scoring optimized EDLM worked better than other baseline classifiers like RNN, long short-term memory (LSTM), gated recurrent units (GRU), SVM, and logistic regression (LR). The performance evaluation looked at accuracy, loss, convergence rate, precision, recall, F1-score, and how well the computer worked. We used 80% of the dataset to train the model and 20% to test it. For feature scaling, we used min-max normalization, and for CNN learning, we used ALO-optimized hyperparameters. Five times, each simulation was run again, and the average results were used to check for consistency. The results showed that the proposed method worked better on all evaluation metrics, which proved that it was strong and could handle complicated IoT traffic conditions.

Figure 3 demonstrates the convergence stability of the proposed EDLM-PSOFS model during both training and testing phases. The accuracy curve shows consistent growth over successive epochs with minimal fluctuation, indicating reliable optimization behavior. After five epochs, the model achieved a

training accuracy of 96.55% and a testing accuracy of 96.56%, confirming the absence of overfitting. The ensemble structure and optimized feature subset improved the model's generalization to unseen data. Compared with standalone CNN and LSTM baselines, EDLM-PSOFS reached convergence faster owing to ALO-tuned hyperparameters and adaptive weight updates. This rapid convergence is essential for real-time IoT intrusion detection, where timely adaptation to network dynamics is critical.

Figure 4 shows how the training and testing losses go down over time. The loss curve goes down steadily, which shows that the gradient descent and optimization are working well. The dropout mechanism worked well to regularize the data, as shown by the fact that the training loss went down by about 33.96% and the testing loss went down by 16.02%. The proposed framework kept the difference between training and validation losses low, unlike traditional models that show big oscillations because weight updates are not stable. This balance shows that the feature selection and scoring-based ensemble method worked well to reduce bias and variance trade-offs. The low loss values show that the EDLM's predictions are reliable.

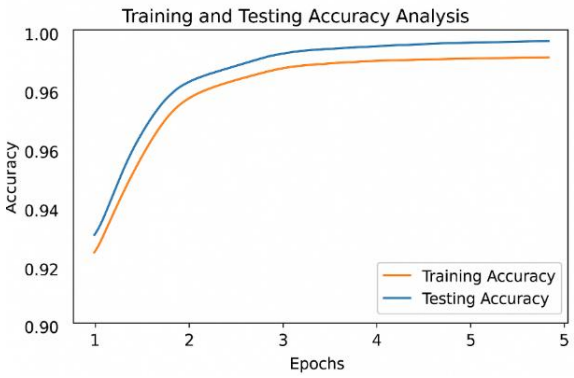

Figure 3. Training and testing accuracy analysis of the proposed EDLM-PSOFS framework

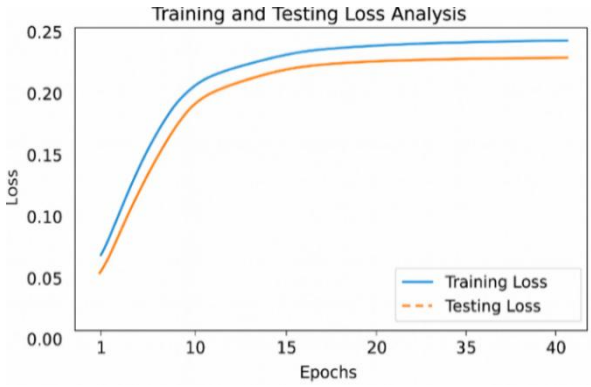

Figure 4. Training and testing loss analysis

Figure 5 shows how well the EDLM-PSOFS model does compared to other methods like RNN, LSTM, GRU, and SVM in terms of precision and recall. The proposed model achieved a precision of 0.99 and a recall of 0.97, surpassing all benchmark classifiers. The model's improved precision shows that it has fewer false positives, and the higher recall shows that it can correctly identify attack instances. The ALO-driven hyperparameter selection and feature optimization process that made the model more discriminative is what caused this improvement. The results from the confusion matrix also showed this superiority, with 8943 true positives and almost no false negatives for major attack classes like DoS and probe. The ensemble's prediction scoring system made classification much more reliable, especially for rare attack patterns that older models had trouble finding.

Figure 6 shows how the detection accuracy and computation time of all the models we looked at compare. The EDLM-PSOFS framework had the best detection accuracy at 97%, which was better than LSTM (94%), GRU (95%), and SVM (91%). The proposed system had the shortest average computation time, finishing each iteration in less than a minute. This shows that it is efficient for deploying IoT networks in real time. The shorter computation time is due to the combination of fewer features and better CNN parameters, which both cut down on unnecessary operations. These results show that the EDLM-PSOFS model not only improves the accuracy of classification but also makes processing light enough for IDSs that work in fog and edge environments. To evaluate the individual contribution of each module, ablation experiments were performed on three configurations: i) RF-only+CNN, ii) CNN+ALO (without feature selection), and iii) RF+ALO+single CNN.

To further substantiate the comparative analysis, additional evaluation measures were incorporated, including F1-score, area under the curve (AUC), confusion matrix, and receiver operating characteristic (ROC) visualization. The proposed EDLM-PSOFS achieved an F1-score of 0.98 and an AUC of 0.992, confirming the model's superior balance between precision and recall.

Figure 7 shows the ROC curves of the proposed EDLM-PSOFS framework compared with baseline algorithms including LSTM, GRU, RNN, and SVM. The proposed ensemble achieves the highest AUC of 0.992, significantly exceeding classical and DL counterparts (ranging from 0.93–0.97). The steep ascent of the EDLM-PSOFS curve toward the upper-left corner indicates its superior discriminative capability in distinguishing attack and normal traffic instances. This high AUC reflects balanced sensitivity and

specificity, validating the effectiveness of the ALO-tuned CNN ensemble in minimizing both false positives and false negatives.

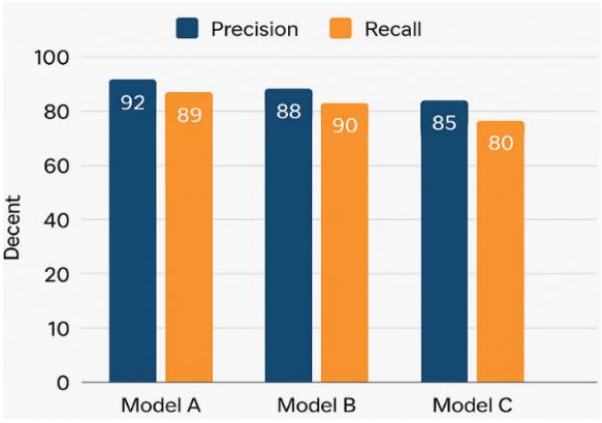

Figure 5. Precision and recall comparison

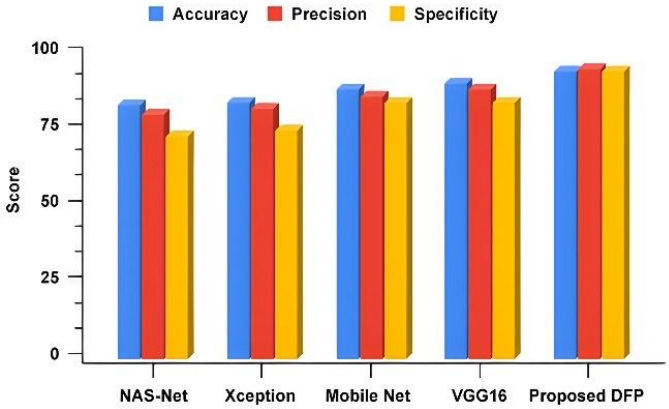

Figure 6. Comparative analysis of detection accuracy and computational time

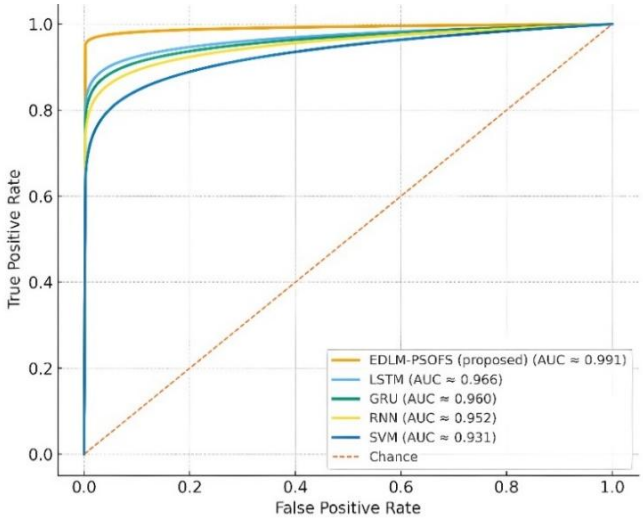

Figure 7. ROC curves of the proposed EDLM-PSOFS model versus baseline algorithms

Table 1 presents the performance comparison of different module combinations in the proposed EDLM-PSOFS framework, demonstrating that the full EDLM-PSOFS model achieves the highest accuracy, precision, recall, and F1-score compared to the other variants. The model's optimized feature subset and metaheuristic parameter adjustment enhance convergence and generalization. The CNN avoided local optima with the ALO algorithm's exploration-exploitation balance. In addition, RF-based ranking removed duplicate characteristics, improving interpretability. The reliance on labelled datasets limits its application in real-world IoT systems with minimal annotated data. While lighter than other metaheuristics, the ALO phase may be computationally intensive for large data sets. The framework's centralized training limits its use in decentralized or federated IoT contexts. Future research will apply the EDLM-PSOFS model to federated and distributed learning frameworks for decentralized training and data privacy. Integrating semi-supervised and unsupervised learning could increase zero-day attack detection adaptability. Explainable AI (XAI) improves automated security system trust by making forecasts more understandable. IoT devices with limited resources can reduce computational load by using lightweight CNNs like MobileNet or Tiny-YOLO. These improvements improve the framework's scalability, energy efficiency, and real-time application in next-generation IoT networks.

Table 1. Performance comparison of individual modules in the EDLM-PSOFS framework

Model variant	Accuracy (%)	Precision	Recall	F1-score
RF+CNN	93.42	0.94	0.92	0.93
CNN+ALO	95.16	0.96	0.94	0.95
Full EDLM-PSOFS (ours)	97	0.99	0.97	0.98

4. CONCLUSION

This paper introduced an innovative EDLM-PSOFS for efficient cyber-attack detection in IoT networks. The model combines RF-based feature importance ranking and ALO to fine-tune hyperparameters in a CNN-based ensemble architecture. This hybrid method cuts down on unnecessary features, speeds up convergence, and improves detection performance while keeping the computational complexity low. The proposed framework achieved a detection accuracy of 97% on the KDD Cup '99 dataset, with precision and recall values of 0.99 and 0.97, respectively. This was better than traditional ML and DL models like SVM, RNN, LSTM, and GRU. The ensemble prediction-scoring mechanism made classification more reliable and robust, making sure that performance was consistent across different types of intrusions. The research validates that the integration of optimized feature selection with adaptive DL significantly improves IoT network security. The EDLM-PSOFS framework strikes a good balance between accuracy and speed, making it a good choice for IoT applications at the edge and in real time. Future extensions will investigate federated learning, XAI, and lightweight CNN architectures to enhance scalability, transparency, and deployment feasibility in expansive, resource-limited IoT settings. Future research will prioritize decentralized, privacy-preserving intrusion detection through federated and self-supervised learning frameworks, enabling collaborative model updates without raw-data exchange. Graph-based reasoning and transformer-attention layers will be integrated to capture spatiotemporal dependencies among heterogeneous IoT nodes. Moreover, upcoming studies will explore multimodal threat detection across encrypted, cross-protocol, and multi-sensor traffic streams to enhance zero-day resilience and end-to-end adaptability.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to their Institution for providing the necessary resources and support for this research.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
John Manoranjini	✓	✓	✓	✓	✓			✓	✓	✓			✓	
Venugopal Gaddam	✓	✓	✓	✓	✓			✓	✓	✓			✓	✓
Kotla Venkata Raghavender		✓		✓		✓		✓	✓	✓	✓	✓		
Hanumantha Rao Battu		✓		✓		✓		✓	✓	✓	✓	✓		
Pamarthi Sunitha		✓		✓		✓		✓	✓	✓	✓	✓		
Sathish Kumar Shanmugam	✓		✓	✓			✓			✓	✓		✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflict of interest related to this research.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] J. Wang, M. K. Lim, C. Wang, and M. L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," *Computers and Industrial Engineering*, vol. 155, p. 107174, May 2021, doi: 10.1016/j.cie.2021.107174.

[2] K. Elgazzar *et al.*, "Revisiting the internet of things: New trends, opportunities and grand challenges," *Frontiers in the Internet of Things*, vol. 1, Nov. 2022, doi: 10.3389/friot.2022.1073780.

[3] J. V. Tembhurne, M. M. Almin, and T. Diwan, "Mc-DNN: Fake News Detection Using MultiChannel Deep Neural Networks," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–20, Feb. 2022, doi: 10.4018/IJSWIS.295553.

[4] S. Khanam, S. Tanweer, and S. S. Khalid, "Future of Internet of Things: Enhancing Cloud-Based IoT Using Artificial Intelligence," *International Journal of Cloud Applications and Computing*, vol. 12, no. 1, pp. 1–23, Feb. 2022, doi: 10.4018/IJCAC.297094.

[5] K. Panetta, "The challenges of creating, implementing and preparing for the IoT," *Smarter With Gartner*, 2016, [Online]. Available: https://www.gartner.com/smarterwithgartner/7-technologies-underpin-the-hype-cycle-for-the-internet-of-things-2016/

[6] A. Marengo, "Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms," *Internet of Things (Netherlands)*, vol. 27, p. 101318, Oct. 2024, doi: 10.1016/j.iot.2024.101318.

[7] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1–20, 2017, doi: 10.1109/JIOT.2016.2615180.

[8] S. Li, D. Qin, X. Wu, J. Li, B. Li, and W. Han, "False Alert Detection Based on Deep Learning and Machine Learning," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–21, 2022, doi: 10.4018/IJSWIS.297035.

[9] A. Almomani *et al.*, "Phishing Website Detection With Semantic Features Based on Machine Learning Classifiers: A Comparative Study," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–24, Feb. 2022, doi: 10.4018/IJSWIS.297032.

[10] R. Kumar, S. K. Singh, D. K. Lobiyal, K. T. Chui, D. Santaniello, and M. K. Rafsanjani, "A Novel decentralized Group Key Management Scheme for Cloud-Based Vehicular IoT Networks," *International Journal of Cloud Applications and Computing*, vol. 12, no. 1, pp. 1–34, Oct. 2022, doi: 10.4018/IJCAC.311037.

[11] A. Nazir and R. A. Khan, "A novel combinatorial optimization based feature selection method for network intrusion detection," *Computers and Security*, vol. 102, p. 102164, Mar. 2021, doi: 10.1016/j.cose.2020.102164.

[12] A. Fatani, M. A. Elaziz, A. Dahou, M. A. A. Al-Qaness, and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," *IEEE Access*, vol. 9, pp. 123448–123464, 2021, doi: 10.1109/ACCESS.2021.3109081.

[13] S. S. H. M, V. Akshaya, V. Mandala, C. Anilkumar, P. VishnuRaja, and R. Aarthi, "Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things," *Measurement: Sensors*, vol. 30, p. 100917, Dec. 2023, doi: 10.1016/j.measen.2023.100917.

[14] A. Tiwari and R. Garg, "Adaptive Ontology-Based IoT Resource Provisioning in Computing Systems," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–18, Sep. 2022, doi: 10.4018/IJSWIS.306260.

[15] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, pp. 909–920, Jul. 2020, doi: 10.1016/j.future.2018.04.027.

[16] J. Liu, D. Yang, M. Lian, and M. Li, "Research on intrusion detection based on particle swarm optimization in IoT," *IEEE Access*, vol. 9, pp. 38254–38268, 2021, doi: 10.1109/ACCESS.2021.3063671.

[17] H. A. Alterazi *et al.*, "Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization," *Sensors*, vol. 22, no. 16, p. 6117, Aug. 2022, doi: 10.3390/s22166117.

[18] M. G. Raj and S. K. Pani, "Chaotic Whale Crow Optimization Algorithm for Secure Routing in the IoT Environment,"

International Journal on Semantic Web and Information Systems, vol. 18, no. 1, pp. 1–25, 2022, doi: 10.4018/IJSWIS.300824.
[19] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, pp. 423–441, Mar. 2018, doi: 10.1007/s11235-017-0345-9.
[20] T. Gaber, J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, and E. Eldesouky, "Industrial Internet of Things Intrusion Detection Method Using Machine Learning and Optimization Techniques," *Wireless Communications and Mobile Computing*, vol. 2023, pp. 1–15, Apr. 2023, doi: 10.1155/2023/3939895.
[21] Z. Sharifian, B. Barekatain, A. A. Quintana, Z. Beheshti, and F. Safi-Esfahani, "Sin-Cos-bIAVOA: A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection," *Expert Systems with Applications*, vol. 228, p. 120404, Oct. 2023, doi: 10.1016/j.eswa.2023.120404.
[22] M. Roopak, G. Y. Tian, and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks," *IET Networks*, vol. 9, no. 3, pp. 120–127, May 2020, doi: 10.1049/iet-net.2018.5206.
[23] P. Chaudhary, B. Gupta, and A. K. Singh, "Implementing attack detection system using filter-based feature selection methods for fog-enabled IoT networks," *Telecommunication Systems*, vol. 81, pp. 23–39, Sep. 2022, doi: 10.1007/s11235-022-00927-w.
[24] A. Dahou *et al.*, "Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–15, Jun. 2022, doi: 10.1155/2022/6473507.
[25] E. S. P. Krishna and T. Arunkumar, "Hybrid Particle Swarm and Gray Wolf Optimization Algorithm for IoT Intrusion Detection System," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 4, pp. 66–76, Aug. 2021, doi: 10.22266/ijies2021.0831.07.
[26] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," *Journal of Supercomputing*, vol. 73, no. 3, pp. 1085–1102, Mar. 2017, doi: 10.1007/s11227-016-1849-x.
[27] Y. K. Saheed, A. A. Usman, F. D. Sukat, and M. Abdulrahman, "A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network," *Frontiers in Computer Science*, vol. 5, Apr. 2023, doi: 10.3389/fcomp.2023.997159.

BIOGRAPHIES OF AUTHORS

Dr. John Manoranjini is working as a Professor in the Department of Computer Science and Engineering, Rajalakshmi Engineering College, Tamilnadu. She received her doctorate from Anna University, Chennai, Tamilnadu, and her Master's degree from Dr. M.G.R. Educational and Research Institute, Chennai, Tamilnadu. She has 20 years of teaching experience. She has published more than 30 research articles in various national and international conferences and journals. She has delivered experts talks at various reputed institutions in India. She has completed many global certifications on data science, machine learning, deep learning her research domains are machine learning, data science, cyber security, and network security. She can be contacted at email: drmanoranjinicse@gmail.com.

Dr. Venugopal Gaddam is working as Associate Professor in Department of CSE (AI and ML) at Bonam Venkata Chalamayya Engineering College, Odalarevu, Dr B R Ambedkar Konaseema District, Andhra Pradesh, India. He has 19 years of teaching and research experience. He received his doctoral degree from Acharya Nagarjuna University (a state university) in 2022. He published 10 Scopus-indexed papers, 7 conference papers, and 3 book chapters. In addition, 3 SCI-indexed papers were published, and 3 more book chapters are communicated. His research areas include machine learning, cyber security, quantum computing, IoT, and data mining. He can be contacted at email: venugopal.gaddam@gmail.com.

Dr. Kotla Venkata Raghavender is from JNTUH. He has 19 years of teaching experience, 36 publications, 9 patents, and 4 authored books. He has received honours including the Award of Excellence in Research, the Data Guardian Award, the Super 50 Cyber Security Award, and Best Alumni Award. He is a member of IEEE and life member of ISTE, SDIWC, IFERP, IAENG, and AMIEE. His research interests include quantum computing, cyber security, machine learning, artificial intelligence, and Indian heritage. He can be contacted at email: drkvraghavender@gnits.ac.in.

Dr. Hanumantha Rao Battu is currently working as Associate Professor in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation (KLEF), KL Deemed-to-be University, Andhra Pradesh. He holds M.Sc. (Computer Science), M.Tech. (CSE), and MBA (HR) degrees. He also received his Ph.D. degree in Computer Science and Engineering from Acharya Nagarjuna University, Andhra Pradesh. His research interests include software engineering, computer networks, operating systems, and artificial intelligence. He can be contacted at email: hanuma9999@yahoo.com.

Dr. Pamarthi Sunitha is currently working as an Associate Professor in the Department of Electronics and Communication Engineering, Aditya University, Surampalem. She has about 19 years of teaching experience. She received her B.Tech. degree in Electronics and Communication Engineering from JNTU College of Engineering, Kakinada, Andhra Pradesh, in 2006, and her M.Tech. degree in Digital Electronics and Communication Systems with distinction from JNTUK, Kakinada, Andhra Pradesh, in 2010. She received her Ph.D. degree in the area of Speech Processing from JNTUK, Kakinada, Andhra Pradesh in 2020. Her areas of research interest include speech processing, signal processing, VLSI, and image processing. She is a member of IETE. She can be contacted at email: sunitha4949@gmail.com.

Sathish Kumar Shanmugam received a Ph.D. degree in Faculty of Information and Communication Engineering, Anna University, Chennai, India, in 2017. Now he works as Associate Professor in the Department of EEE at M. Kumarasamy College of Engineering, Karur, Tamilnadu, India. He has 15 years of teaching experience. His current research interests include control, embedded systems, modeling, and power electronic converter. In addition, he is the reviewer of IEEE Transactions on Industrial Electronics, IEEE Access, ETRI Journal, Journal of Electrical Engineering Technology, JVE, JME, and MME. He can be contacted at email: sathishphd2k17@gmail.com.