

An intelligent hybrid deep learning approach for securing internet of things threat networks from cyber threats

Swati Lakshmi Boppana¹, Venu Gopal Gaddam², Venkata Sai Aditya Kondru³, Athinarayanasamy Muthukrishnan⁴, Dasari Veeraswamy⁵, Garigipati Rama Krishna⁶

¹Department of Electronics and Communication Engineering, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India

²Department of Computer Science and Engineering, (Artificial Intelligence and Machine Learning), Bonam Venkata Chalamayya Engineering College, Odalarevu, India

³Senior Data Insights and Analytics Engineer, Fidelity Investments, Carmel, United States

⁴Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, India

⁵Department of Artificial Intelligence and Machine Learning, Aditya University, Surampalem, India

⁶Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India

Article Info

Article history:

Received Oct 16, 2025

Revised Aug 29, 2026

Accepted Sep 4, 2026

Keywords:

Autoencoders

Deep belief networks

Internet of things security

Optimization techniques

Real-time internet of things

threat detection

Self-organizing maps

ABSTRACT

The rapid growth of internet of things (IoT) devices has increased their vulnerability to cyber-attacks, creating a need for accurate and adaptive intrusion detection systems (IDS). This study proposes a hybrid approach that integrates self-organizing maps (SOMs), deep belief networks (DBNs), and autoencoders to detect both known and unknown attacks in IoT networks. particle swarm optimization (PSO) is employed to optimize model parameters and improve detection accuracy and convergence. The proposed method was evaluated using synthetic and real-world network traffic datasets, including NSL-KDD, UNSW-NB15, and CICIoT2023. Standard cybersecurity performance metrics were used to assess the effectiveness of the model. Experimental results demonstrate an accuracy of 99.99% and Matthews correlation coefficient (MCC) values exceeding 99.50%. The results also indicate strong generalization across different attack scenarios. Overall, the proposed PSO-optimized hybrid model provides an accurate, adaptive, and robust solution for detecting diverse and emerging cyber-attacks in IoT networks.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Venu Gopal Gaddam

Department of Computer Science and Engineering, (Artificial Intelligence and Machine Learning)

Bonam Venkata Chalamayya Engineering College

Odalarevu, Andhra Pradesh, India

Email: venugopal.gaddam@gmail.com

1. INTRODUCTION

The rapid expansion of internet of things (IoT) devices—integrated into critical consumer and business infrastructures—has resulted in a dramatic increase in the volume and complexity of network traffic. IoT applications are increasingly vulnerable to cyberattacks, which are evolving in complexity, adaptability, magnitude, sophistication, and strategy [1]–[4]. Attackers now have additional opportunities to take advantage of security weaknesses due to the fast growth of interconnected IoT ecosystems. Because of this, conventional intrusion detection systems (IDS) have a tougher time keeping up with modern threats. This incident highlights the need for sophisticated detection systems capable of autonomously identifying known attack routes and emerging threats. The limitation of traditional network security solutions lies in their dependence on known attack patterns, especially IDS that rely on signatures. Although they are effective against known

vulnerabilities, their reactive nature and inability to detect zero-day exploits render them useless in the dynamic IoT threat landscape [5]. Moreover, existing systems have a tougher time providing consistent real-time analysis due to the increased demand on computers and analysis caused by the fast expansion of IoT traffic [6]. This emphasizes the need for creative, flexible, and extensible solutions to protect IoT networks from various evolving cyber risks.

To address these issues, this study presents a state-of-the-art IDS that uses autoencoders, deep belief networks (DBNs), and self-organizing maps (SOMs) in conjunction with wise optimization techniques. In order to detect intricate temporal and spatial patterns in IoT traffic flows, the suggested model employs a thorough architecture. This form of multidimensional analysis allows the system to detect subtle changes in behavior that conventional IDSs frequently fail to detect, particularly in distributed and ever-changing networks. This technology is ideal for application in large-scale IoT systems in real-time because the combination of these deep learning components increases detection accuracy and data handling capacity. New findings in IDS research based on machine learning have highlighted the usefulness of hybrid models that combine supervised and unsupervised learning to tackle complex and multi-dimensional attack situations [7]. Researchers and practitioners now have a clearer picture of how deep learning systems make decisions thanks to attention processes, which have improved interpretability and predictive accuracy even more [8]. To tackle the specific cybersecurity issues of IoT networks, this research combines the mutually beneficial features of SOMs, DBNs, and autoencoders into a unified design. So, the proposed approach represents a giant leap forward in terms of enhancing the scalability, intelligence, and robustness of IoT intrusion detection. What follows is a more in-depth discussion of the methodology, experimental framework, and evaluation results that demonstrate the system's efficacy in actual IoT environments.

To overcome the limitations of traditional IDSs, researchers focusing on cybersecurity for the IoT are increasingly turning to hybrid learning paradigms that combine supervised and unsupervised models. Hybrid approaches take the greatest features of both paradigms and combine them to create powerful, flexible, and accurate tools. To identify novel dangers in dynamic IoT environments, for instance, Kaliyaperumal *et al.* [9] developed an unsupervised hybrid learning approach based on SOMs. A hybrid IDS that used both machine learning and signature-based detection was also developed by Tariq *et al.* [10]. This greatly simplified the process of discovering known and unknown threats in IoT networks. Shenify *et al.* [11] developed a model that integrates supervised learning and the spider monkey optimization method to address the issue of selecting optimal features. For resource-constrained IoT devices, this improves the model's computational efficiency. Research into adversarial robustness and resilient hybrid frameworks are examples of recent advances. The use of hybrid learning architectures to strengthen IDS resistance to malicious manipulations was studied by Vitorino [12], and a hybrid anomaly detection methodology was developed by Zhang *et al.* [13] to improve the accuracy of detecting complex and subtle attack signatures. This methodology integrates autoencoders with traditional machine learning algorithms. This area was greatly advanced by the work of Kalidindi and Arrama [14], who developed the convolutional neural network fused with a deep stacked autoencoder (CNN-FDSA) model for detecting botnets in IoT networks by combining CNNs with deep stacked autoencoders (DSAs). Through the use of oversampling to balance datasets and Quantile normalization, information gain, and city block distance for feature extraction, the CNN-FDSA achieved an astounding 92.4% accuracy. Not only that, but its F-measure, recall, and precision were all great. Improvements in multi-layered IoT security designs and real-time botnet identification are suggested as future developments by the authors.

There are concerns about privacy when it comes to intrusion detection in the IoT because it often involves sensitive user or device data. Even if federated learning (FL) has evolved into a privacy-protecting method, issues such as data leaks and deteriorating models are still present. In their paper, Olanrewaju-George and Pranggono [15] proposed an IDS based on FL. This system uses the N-BaIoT dataset, which consists of nine IoT devices, and combines unsupervised autoencoders for anomaly detection with supervised deep neural networks (DNNs) for attack classification. Despite FL's improvements, data leakage during training remained a possibility, and it was difficult to generalize across various device kinds. Performance was enhanced by using the federated averaging with momentum (FedAvgM) aggregation technique and selecting hyperparameters with care. On most assessment metrics, FL-trained autoencoders outperformed centralized models. Study after study by Chen *et al.* [16] investigated privacy-preserving computation in FL frameworks, focusing on techniques like secure multi-party computation (SMC), homomorphic encryption (HE), differential privacy (DP), trusted execution environments (TEEs), and zero-knowledge proofs (ZKPs). They demonstrated the protocol's increased security by testing it with the Modified National Institute of Standards and Technology (MNIST) and Canadian Institute for Advanced Research (CIFAR-10) datasets; however, they also demonstrated its susceptibility to assaults such as data poisoning and inference attacks. To improve privacy and compliance assurances, the report recommended investigating machine unlearning and integrating ZKPs with FL. In order to develop a blockchain-federated learning (BFL) system for identifying intrusions in IoT, Ali *et al.* [17] expanded upon these privacy-preserving advancements. Their model leverages FL's

decentralized nature to secure data privacy while utilizing blockchain for immutable and verifiable communication. This hybrid design addresses the issues of privacy and scalability in Industry 4.0 environments, paving the way for distributed, secure, trustless IDS deployments.

The need for real-time network intrusion detection systems (NIDS) capable of discovering complex, multi-vector attacks are rising in tandem with the expansion of IoT networks. In heterogeneous IoT environments, traditional IDS struggle to remain scalable due to computational limitations and a wide variety of communication protocols [18], [19]. To address these issues, adaptive frameworks built on machine learning have emerged as viable options. So, for resource-constrained IoT devices, Shen *et al.* [20] developed a CNN-based IDS that is both lightweight and effective. It prevents distributed denial of service (DDoS) and man-in-the-middle (MITM) attacks with reasonable processing overhead and detection performance. The approach still need improvement since it isn't effective enough against more sophisticated multi-stage incursions. A NIDS based on deep learning was proposed by Wang *et al.* [21]. It improves multi-level feature representation through the use of group convolution for spatial extraction, split-attention for feature prioritization, and bidirectional gated recurrent unit (BiGRU) for temporal analysis. Their model achieved 91.08% accuracy on the University of New South Wales- network-based 2015 (UNSW-NB15) dataset, 94.55% accuracy on the communications security establishment-Canadian Institute for Cybersecurity-IDS 2018 (CIC-IDS2018) dataset, and 97.47% accuracy on the Canadian Institute for Cybersecurity-internet of things 2023 (CICIoT2023) dataset after using a conditional tabular generative adversarial network (CTGAN) to address the imbalance in the datasets. To cut down on the exorbitant training expenses, they recommended utilizing cloud-edge collaboration and transfer learning. The convolutional neural network and bidirectional long short-term memory (CNN-BiLSTM) architecture suggested by Mynuddin *et al.* [22] effectively captured spatial and temporal correlations, leading to strong binary classification results on network security laboratory-knowledge discovery and data mining (NSL-KDD) data. However, due to a lack of data, user-to-root (U2R) assaults were under-represented.

A hybrid IDS was developed by Asgharzadeh *et al.* [23] that enhances feature selection and hierarchical learning by merging a CNN with a binary multi-objective gorilla troops optimizer (BMGTO). On the telemetry data, operating systems logs, and network traffic-IoT (TON-IoT) dataset, their CNN-BMGTO-K-nearest neighbors (KNN) model achieved an accuracy of 99.99%, while on the NSL-KDD dataset, it achieved 99.86%. It outperformed long short-term memory (LSTM) and multilayer perceptron (MLP) in every relevant aspect. Similarly, Darabi *et al.* [24] employed a micro reinforcement learning classifier (MRLC) based on deep Q-networks (DQNs) to classify intrusions at a fine grade. In order to improve the system's stability and speed up its convergence, each training instance was approached as an independent reinforcement learning experiment. As time and again, deep learning demonstrates its superiority in detecting sophisticated cyber breaches in IoT networks, even those with several stages. Finding new attack patterns without labelled data has been made possible with unsupervised algorithms like SOMs, DBNs, and autoencoders [25], [26]. By reducing the dimensionality of high-dimensional IoT data, SOMs excel at helping to detect outliers more rapidly. In order to build a real-time anomaly detection system for smart grid cybersecurity, which could autonomously mitigate attacks while maintaining operational stability, Quraishi *et al.* [27] used autoencoders, LSTMs, GANs, SOMs, transfer learning, and attention mechanisms. Scalability, robustness, and informed reaction were three areas where their methodology excelled above more conventional approaches. DBNs are able to detect advanced persistent threats (APTs) because they are able to grasp the temporal dependencies in the flows of IoT networks. A conditional deep belief network (CDBN) with fewer dimensions was created by Yang *et al.* [28] using the "SamSelect" under-sampling algorithm in conjunction with a stacked contractive autoencoder (SCAE). Their approach was the most effective means of detecting intrusions in real-time wireless networks, with an accuracy rate of 97.4% and a detection delay of just 1.14 milliseconds. To further enhance IDS frameworks, autoencoders combine feature compression with reconstruction to eliminate duplicate data and identify outliers [29]. In order to detect cyber threats targeting autonomous vehicles (AVs) and internet of vehicles (IoV) infrastructures, Ashraf *et al.* [30] created an IDS based on LSTM autoencoders that is tailored to intelligent transportation systems (ITS). By using statistical and temporal data extracted from in-vehicle and network traffic, the model achieved improved detection rates while decreasing false alarms. Although it handled numerous attack vectors well, the system struggled to scale up when dealing with datasets that contained multiple kinds of IoV. Most existing IDS rely either on supervised learning models or unsupervised anomaly detection techniques. However, such approaches struggle to detect evolving IoT threats effectively. This study addresses this limitation by integrating both learning paradigms in a hybrid architecture validated across multiple benchmark datasets.

2. METHOD

To facilitate the detection of cyberattacks in IoT networks, the suggested framework integrates autoencoders, DBNs, and SOMs. Thanks to combining the best features of these three deep learning models,

An intelligent hybrid deep learning approach for securing IoT networks ... (Swati Lakshmi Boppa)

the system is able to improve its detection accuracy and flexibility. While DBNs extract hierarchical representations of IoT traffic data, SOMs autonomously cluster and detect anomalies. In contrast, autoencoders aid in dimensionality reduction and enhance feature extraction, both of which contribute to the model's overall efficiency. By fine-tuning the hyperparameters of these models, a sophisticated optimization approach is employed to produce even more precise predictions. This guarantees that they perform admirably under actual network circumstances. In order to project high-dimensional input data onto a lower-dimensional feature map while preserving the topological links in the input space, SOMs are a sort of unsupervised artificial neural network. Their usefulness for grouping and data visualization applications is due to this property. The input layer and the output lattice of neurons in a SOM are both completely linked. Training begins with assigning arbitrary values to the connection weights. A new input vector is selected at random and transmitted to the lattice for each iteration. Using coordinates in Euclidean space, each neuron determines its distance from the input. We refer to the neuron with the shortest distance as the "best matching unit" (BMU). After that, a neighborhood region is created around the BMU, and the input pattern is used to adjust the weight vectors of the neurons in that area. This kind of competitive learning allows SOMs to learn to map data samples that are similar to one another to nearby places on the output grid. Features of IoT traffic can be more easily and simply grouped in this way.

The proposed model follows a sequential hybrid architecture. Initially, autoencoders perform dimensionality reduction and feature compression to remove redundant information from IoT traffic data. The compressed feature representation is then processed using SOMs to cluster traffic patterns and identify anomalous behaviors. Finally, DBNs perform hierarchical feature learning and classification of normal and malicious traffic. This pipeline enables the system to combine unsupervised anomaly detection with supervised classification for improved intrusion detection accuracy. Particle swarm optimization (PSO) was used to optimize hyperparameters of the hybrid model. The PSO configuration used a population size of 30 particles, maximum iterations of 100, inertia weight of 0.7, and cognitive/social coefficients of 1.5. The optimization process searches for optimal learning rates, hidden layer sizes, and reconstruction thresholds that maximize detection accuracy while minimizing false positives.

To discover more profound relationships in the data, DBNs are employed for hierarchical learning of IoT traffic patterns. Anomaly detection, feature abstraction, and predictive analytics are all areas where DBNs shine due to their ability to mimic the inherent complexity of high-dimensional data through their multi-layered structure. DBNs are able to learn deep representations, which allow them to effectively capture feature dependencies. The results are then easier to understand and rely on. Each layer of the DBN is composed of restricted Boltzmann machines (RBMs). Incorporating probabilistic reasoning and handling uncertainty throughout the learning process improves the network's decision-making capabilities. The addition of autoencoders allows for more effective feature compression and extraction. From raw input, the encoder extracts the most relevant features and discards the rest, creating a compact latent representation. By restoring the original input from this compressed form, the decoder ensures that all crucial data properties remain intact. This encoding-decoding approach facilitates the reduction of noise, the acceleration of computations, and the ease of subsequent tasks such as clustering, classification, and anomaly detection. Additionally, autoencoders are applicable to a broad variety of IoT datasets and security applications due to their modular design, which allows for domain customization.

3. RESULTS AND DISCUSSION

A thorough experimental framework was developed to assess the efficacy of the suggested hybrid methodology for cyber-attack detection in IoT networks. This section outlines the datasets, evaluation metrics, and configuration settings utilized to evaluate the performance of the integrated autoencoder, DBN, and SOM models. The experiments were carried out in a controlled setting utilizing both authentic IoT traffic traces and artificially generated data, thereby guaranteeing a balanced and varied testing environment. We used three benchmark cybersecurity datasets—NSL-KDD, UNSW-NB15, and CICIoT2023—to test how well the proposed model worked. Each dataset showed different network behaviors and attack patterns. The results show that the system is very good at finding both known and new types of intrusions. The model's ability to work with a wide range of attack scenarios shows how strong and flexible it is for use in real-world IoT settings. Before model training, the datasets underwent several preprocessing steps. Continuous features were normalized using min-max scaling, while categorical attributes were encoded using one-hot encoding. Irrelevant features were removed to reduce noise and computational complexity. The datasets were then divided into training and testing sets using an 80:20 split.

Figure 1 shows the parallel coordinates plot of the NSL-KDD and UNSW-NB15 datasets. It shows how the selected features, like source bytes, error rate, and duration, are spread out across different types of attacks. The plot has one line for each data instance, and the colors show which attack types are different. This

visualization clearly shows how feature values change between normal and malicious traffic. It shows both areas of overlap and unique behavioral signatures that can help anomaly detection systems find problems. Figure 2 shows the kernel density estimation (KDE) overlay of the Source Bytes feature from the NSL-KDD dataset. This shows the probability density function for this attribute. The x-axis shows the range of Source Byte values, and the y-axis shows the density of instances that match those values. The graph shows that most network connections have low Source Byte counts, and that the frequency goes down as the byte volume goes up. Understanding this distribution is important for understanding how normal traffic works, which is the first step in spotting changes that might mean a cyber-attack. SOMs effectively detect anomalies by clustering high-dimensional IoT traffic patterns into topological maps. Autoencoders enhance feature representation through dimensionality reduction, enabling efficient anomaly detection. DBNs capture hierarchical relationships among network features, improving classification accuracy. The integration of these models enables detection of both known and zero-day attacks.

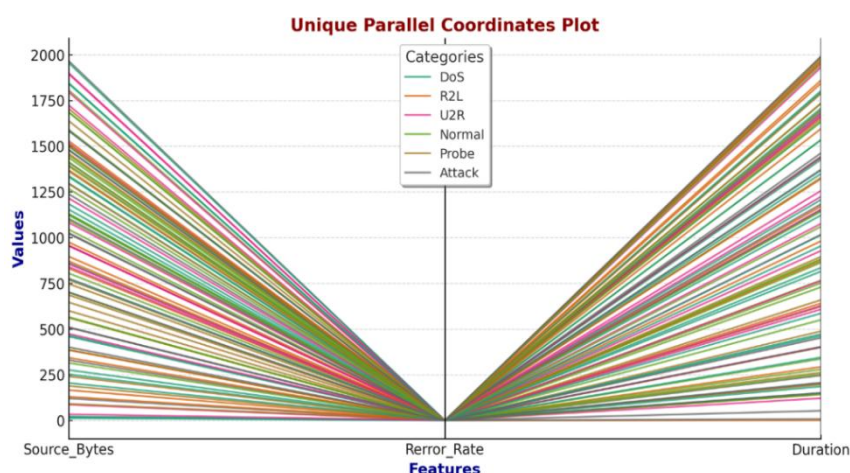


Figure 1. Parallel coordinates plot of source bytes, error rate, and duration across class labels

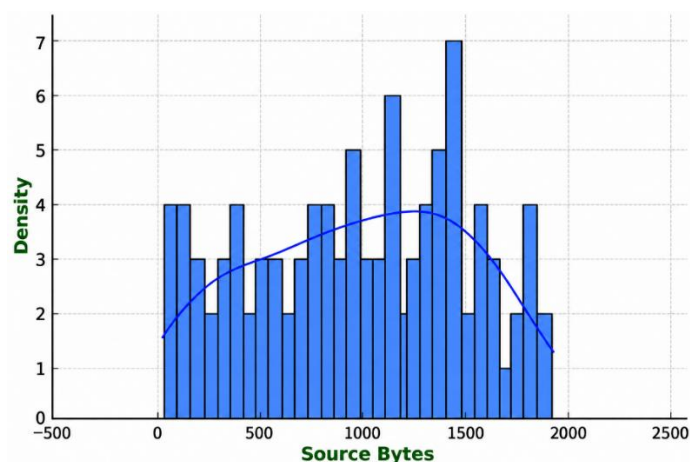


Figure 2. Source byte histogram with KDE overlay demonstrating byte size distribution and regular vs malicious network traffic

Figure 3 compares the attack distribution between the NSL-KDD and UNSW-NB15 datasets across many categories. The frequency of attacks in the NSL-KDD dataset is displayed in the left-hand graphic. The most prevalent kind of attack is a denial-of-service (DoS), followed by probe and R2L intrusions. Figure 3(a) presents the overall attack category distribution including DoS, R2L, U2R, probe, and normal traffic. Figure 3(b) provides a detailed breakdown of attack types such as exploits, fuzzers, backdoor, worms, analysis, and reconnaissance. This distribution demonstrates the diversity of attack patterns used to evaluate the robustness of the proposed hybrid IDS. On the other side, the UNSW-NB15 dataset is depicted in the

right-hand graphic. This dataset includes a broader variety of assaults, with exploits and DoS being the most prevalent, respectively. This comparison sheds light on the unique attack landscapes of each dataset and allows us to gauge the effectiveness of detection algorithms against various assault kinds. Combining autoencoders, DBNs, and SOMs considerably enhances cyber-attack detection in IoT settings, according to the experimental study. When it comes to identifying attack patterns, the hybrid model excels at both old and new. Due to the dynamic and diverse nature of IoT systems, the models' capacity to generalize across multiple datasets demonstrates their adaptability to evolving network conditions.

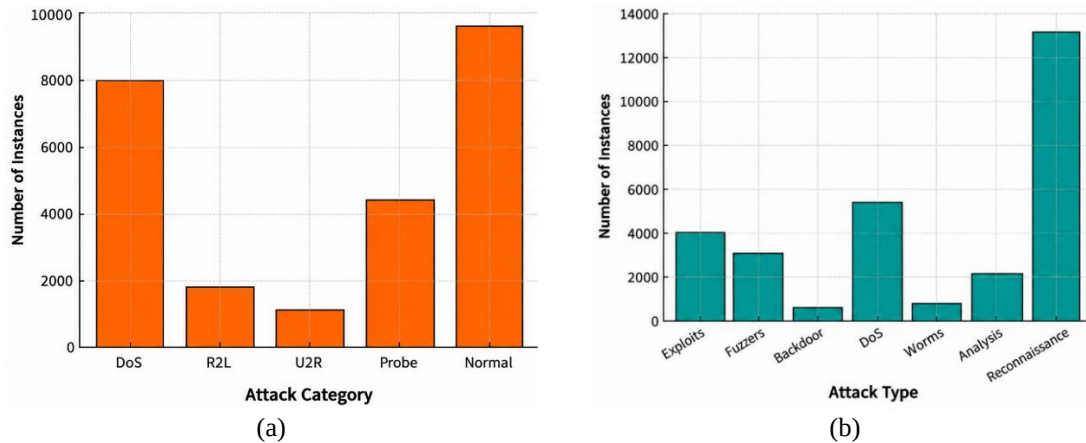


Figure 3. Bar plots of attack distributions for; (a) NSL-KDD and (b) UNSW-NB15

The suggested framework's ability to detect anomalous network behavior by means of unsupervised learning techniques such as SOMs and autoencoders is one of its strongest points. In the real world, where tagged datasets are few or nonexistent, this is really helpful. Improving detection performance by fine-tuning model hyperparameters with PSO further demonstrates the significance of optimization in cybersecurity solutions based on deep learning. Some issues persist despite these strengths. Environment and data specific to each IoT deployment may affect the model's performance. Research in the future should evaluate the models in different network settings and incorporate contextual elements that impact the reliability of detection in order to address these constraints. Collectively, the experimental findings from the NSL-KDD, UNSW-NB15, and CICIoT2023 datasets demonstrate the flexibility and strong performance of the system. We are able to validate the model's robustness by subjecting it to a wide range of attack types and data distributions across all datasets. The following analysis compares and contrasts the findings of several datasets, identifies the specific issues with each dataset, and provides extensive statistical evidence to support the observed performance improvements. Although the proposed hybrid model achieves high detection accuracy, its computational complexity may increase when deployed in large-scale IoT networks. However, the dimensionality reduction capability of autoencoders significantly reduces computational overhead. Future work will investigate edge-cloud collaborative deployment to support real-time IoT intrusion detection. Performance evaluation included precision, recall, F1-score, false positive rate, and MCC. The hybrid model achieved low false positive rates across all datasets, demonstrating stable detection performance across multiple runs.

4. CONCLUSION

This research offers a thorough framework for detecting cyber-attacks in IoT networks, showcasing the efficacy of combining SOMs, DBNs, and autoencoders to recognize both established and emerging attack patterns. Experimental results validate that the suggested methodology delivers enhanced performance across various evaluation metrics, highlighting its prospective utility in practical IoT security systems. Additionally, using PSO to fine-tune the model's hyperparameters greatly improves both the accuracy of detection and the stability of the system. Future research will concentrate on enhancing these models and investigating the incorporation of supplementary machine learning methodologies to augment detection efficiency and scalability. This research enhances the domain of IoT cybersecurity by underscoring the necessity for adaptive and resilient detection mechanisms that can safeguard against the escalating complexity of contemporary cyber threats. This study proposes a hybrid intrusion detection framework integrating SOMs, DBNs, and

autoencoders optimized using PSO. The model is validated across three benchmark datasets—NSL-KDD, UNSW-NB15, and CICIoT2023—achieving 99.99% accuracy and MCC above 99.5%, demonstrating superior performance compared with conventional IDS models. Despite the high detection accuracy, the proposed model has limitations related to computational cost and dataset dependency. Future work will explore lightweight architectures and real-time deployment in edge-based IoT environments.

FUNDING INFORMATION

This research received no external funding.

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
Swati Lakshmi Boppana	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Venu Gopal Gaddam	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Venkata Sai Aditya Kondru	✓	✓	✓	✓			✓		✓	✓		✓	✓	
Athinarayanasamy Muthukrishnan	✓	✓	✓	✓			✓		✓	✓		✓		
Dasari Veeraswamy	✓	✓	✓	✓	✓		✓		✓	✓		✓		
Garigipati Rama Krishna	✓	✓	✓	✓			✓		✓	✓		✓		

- C : Conceptualization
- M : Methodology
- So : Software
- Va : Validation
- Fo : Formal analysis
- I : Investigation
- R : Resources
- D : Data Curation
- O : Writing - Original Draft
- E : Writing - Review & Editing
- Vi : Visualization
- Su : Supervision
- P : Project administration
- Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

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

ETHICAL APPROVAL

This study does not involve human participants or animals and does not require ethical approval.

DATA AVAILABILITY

The data used in this study are not publicly available.

REFERENCES

[1] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors*, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.

[2] R. Vallabhaneni, "Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices," *Engineering and Technology Journal*, vol. 09, no. 07, pp. 4439-4442, 2024, doi: 10.47191/etj/v9i07.13.

[3] A. Bensaoud and J. Kalita, "CNN-LSTM and transfer learning models for malware classification based on opcodes and API calls," *Knowledge-Based Systems*, vol. 290, 2024, doi: 10.1016/j.knosys.2024.111543.

[4] A. Bensaoud and J. Kalita, "Deep multi-task learning for malware image classification," *Journal of Information Security and Applications*, vol. 64, 2022, doi: 10.1016/j.jisa.2021.103057.

[5] M. Thankappan, H. Rifa-Pous, and C. Garrigues, "A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks," *IEEE Access*, vol. 12, pp. 23096-23121, 2024, doi: 10.1109/ACCESS.2024.3362803.

[6] N. J. Singh, N. Hoque, K. R. Singh, and D. K. Bhattacharyya, "Botnet-based IoT network traffic analysis using deep learning," *Security and Privacy*, vol. 7, no. 2, 2024, doi: 10.1002/spy2.355.

[7] T. Zoppi, A. Ceccarelli, T. Puccetti, and A. Bondavalli, "Which algorithm can detect unknown attacks? Comparison of supervised, unsupervised and meta-learning algorithms for intrusion detection," *Computers and Security*, vol. 127, 2023, doi: 10.1016/j.cose.2023.103107.

- [8] Y. Gao and Y. Ruan, "Interpretable deep learning model for building energy consumption prediction based on attention mechanism," *Energy and Buildings*, vol. 252, 2021, doi: 10.1016/j.enbuild.2021.111379.
- [9] P. Kaliyaperumal, S. Periyasamy, M. Thirumalaisamy, B. Balusamy, and F. Benedetto, "A Novel Hybrid Unsupervised Learning Approach for Enhanced Cybersecurity in the IoT," *Future Internet*, vol. 16, no. 7, 2024, doi: 10.3390/fi16070253.
- [10] A. H. I. E. Tariq, M. B. I. E. Tariq, and S. Lu, "Hybrid AI-Driven Techniques for Enhancing ZeroDay Exploit Detection in Intrusion Detection System (IDS)," in *2024 3rd International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology, AIoT 2024*, 2024, pp. 156–160, doi: 10.1109/AIoT63215.2024.10748333.
- [11] M. A. Shenify, A. S. Alghamdi, and A. F. Alharthi, "Hybrid Supervised Machine Learning-based Intrusion Detection System of Internet of Things," *International Journal of Advances in Soft Computing and its Applications*, vol. 16, no. 2, pp. 68–84, 2024, doi: 10.15849/IJASCA.240730.05.
- [12] J. P. M. Vitorino, "Realistic Adversarial Machine Learning to improve Network Intrusion Detection," M.S. thesis, Dept. Comput. Eng., Instituto Politécnico do Porto, Porto, Portugal, 2022.
- [13] X. Zhang, P. Wei, and Q. Wang, "A hybrid anomaly detection method for high dimensional data," *PeerJ Computer Science*, vol. 9, 2023, doi: 10.7717/peerj-cs.1199.
- [14] A. Kalidindi and M. B. Arrama, "Feature selection and hybrid CNNF deep stacked autoencoder for botnet attack detection in IoT," *Computers and Electrical Engineering*, vol. 122, 2025, doi: 10.1016/j.compeleceng.2024.109984.
- [15] B. Olanrewaju-George and B. Pranggono, "Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models," *Cyber Security and Applications*, vol. 3, 2025, doi: 10.1016/j.csa.2024.100068.
- [16] J. Chen, H. Yan, Z. Liu, M. Zhang, H. Xiong, and S. Yu, "When Federated Learning Meets Privacy-Preserving Computation," *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–36, 2024, doi: 10.1145/3679013.
- [17] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey," *Ad Hoc Networks*, vol. 152, 2024, doi: 10.1016/j.adhoc.2023.103320.
- [18] X. Lu and J. Lai, "Communication Constraints for Distributed Secondary Control of Heterogeneous Microgrids: A Survey," *IEEE Transactions on Industry Applications*, vol. 57, no. 6, pp. 5636–5648, 2021, doi: 10.1109/TIA.2021.3104792.
- [19] J. Liu *et al.*, "HeterPS: Distributed deep learning with reinforcement learning based scheduling in heterogeneous environments," *Future Generation Computer Systems*, vol. 148, pp. 106–117, 2023, doi: 10.1016/j.future.2023.05.032.
- [20] Y. Shen *et al.*, "A Deep-Learning-Based Data-Management Scheme for Intelligent Control of Wastewater Treatment Processes Under Resource-Constrained IoT Systems," *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 25757–25770, Aug. 2024, doi: 10.1109/IIOT.2024.3388043.
- [21] X. Wang, L. Dai, and G. Yang, "A network intrusion detection system based on deep learning in the IoT," *Journal of Supercomputing*, vol. 80, no. 16, pp. 24520–24558, 2024, doi: 10.1007/s11227-024-06345-w.
- [22] M. Mynuddin *et al.*, "Automatic Network Intrusion Detection System Using Machine Learning and Deep Learning," in *International Conference on Artificial Intelligence and Mechatronics System, AIMS 2024*, 2024, pp. 1–9, doi: 10.1109/AIMS61812.2024.10512607.
- [23] H. Asgharzadeh, A. Ghaffari, M. Masdari, and F. S. Gharehchopogh, "An Intrusion Detection System on The Internet of Things Using Deep Learning and Multi-objective Enhanced Gorilla Troops Optimizer," *Journal of Bionic Engineering*, vol. 21, no. 5, pp. 2658–2684, 2024, doi: 10.1007/s42235-024-00575-7.
- [24] B. Darabi, M. Bag-Mohammadi, and M. Karami, "A micro Reinforcement Learning architecture for Intrusion Detection Systems," *Pattern Recognition Letters*, vol. 185, pp. 81–86, 2024, doi: 10.1016/j.patrec.2024.07.010.
- [25] J. K. Chahal, A. Bhandari, and S. Behal, "DDoS attacks & defense mechanisms in SDN-enabled cloud: Taxonomy, review and research challenges," *Computer Science Review*, vol. 53, 2024, doi: 10.1016/j.cosrev.2024.100644.
- [26] S. Karnani, N. Agrawal, and R. Kumar, "A comprehensive survey on low-rate and high-rate DDoS defense approaches in SDN: taxonomy, research challenges, and opportunities," *Multimedia Tools and Applications*, vol. 83, no. 12, pp. 35253–35306, 2024, doi: 10.1007/s11042-023-16781-0.
- [27] A. Quraishi, M. A. Rusho, A. Prasad, I. Keshta, R. Rivera, and M. W. Bhatt, "Employing Deep Neural Networks for Real-Time Anomaly Detection and Mitigation in IoT-Based Smart Grid Cybersecurity Systems," in *3rd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2024*, 2024, pp. 1–6, doi: 10.1109/ICDCECE60827.2024.10548160.
- [28] L. Yang, J. Li, L. Yin, Z. Sun, Y. Zhao, and Z. Li, "Real-time intrusion detection in wireless network: A deep learning-based intelligent mechanism," *IEEE Access*, vol. 8, pp. 170128–170139, 2020, doi: 10.1109/ACCESS.2020.3019973.
- [29] A. Bensaoud, J. Kalita, and M. Bensaoud, "A survey of malware detection using deep learning," *Machine Learning with Applications*, vol. 16, 2024, doi: 10.1016/j.mlwa.2024.100546.
- [30] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, "Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events from Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4507–4518, 2021, doi: 10.1109/TITS.2020.3017882.

BIOGRAPHIES OF AUTHORS



Swati Lakshmi Boppana     is an assistant professor in the Department of Electronics and Communication Engineering at Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India. She is actively involved in teaching and research activities within the department. Her research contributions include work on embedded systems and communication technologies, as evidenced by her publications in international conferences and journals. She has co-authored several technical papers on topics such as digital emergency systems and antenna design. She can be contacted at email: boppanaswathi@gmail.com.



Dr. Venu Gopal Gaddam    is working as associate professor in Department of CSE (AI and ML) at BVC 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. His research areas include machine learning, cyber security, quantum computing, IoT, and data mining. He can be contacted at email: venugopal.gaddam@gmail.com.



Mr. Venkata Sai Aditya Kondru    is a software engineer data specialist at FMR, USA. He graduated with a first-class in Master of Science in data analytics and mathematical modeling from Valparaíso University, USA in 2018. He also holds master of science in Statistics from Acharya Nagarjuna University, India in 2016. He completed his B.Tech. degree in Computer Science and Engineering from JNTU Kakinada, India, in 2011. His research interests are primarily in the areas of data engineering, statistical analysis, data modeling, genetic algorithms, optimization and linear programming, data privacy and governance, LLM's, and GEN AI techniques, HIPAA privacy wrt data in particular with healthcare and financial data. He can be contacted at email: mailtodraditya@gmail.com.



Dr. Athinarayanasamy Muthukrishnan    is a professor in Department of Electronics and Communication Engineering in Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology Chennai, India. He graduated with a first-class bachelor of engineering degree in Electrical and Electronics Engineering from Anna University Chennai, India in 2005, and Master of Engineering in VLSI design from Anna University Coimbatore, India in 2009. He received his Ph.D. degree in Information and Communication Engineering from Anna University Chennai, India in 2016. His research interest includes wireless sensor networks, IoT, and VLSI design and its applications. He can be contacted at email: muthuathi@gmail.com.



Dr. Dasari Veeraswamy    is an assistant professor at the Department of Artificial Intelligence and Machine Learning, Aditya University, Surampalem, Andhra Pradesh, India. He posts graduated M.Tech. from JNTU Hyderabad University, India, in 2014, and awarded Ph.D. from Osmania University, Telangana, India in 2025. His research interests are primarily in the area machine learning and deep learning applications as well as in quantum computing, cyber security applications, and biomedical engineering. He can be contacted at email: dveeraswamy6008@gmail.com and veeraswamyd@adityauniversity.in.



Garigipati Rama Krishna    is an assistant professor in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Vijayawada. He completed his M.Tech. from JNTUH University in 2014 and earned his B.Tech. in Computer Science and Engineering from JNTUH in 2012. He is a computer science educator and researcher with interests in software development, web technologies, Linux systems, and artificial intelligence applications in healthcare. He focuses on teaching programming concepts through practical examples and hands-on learning to help students build strong technical foundations. He is currently involved in research on pancreatic cancer detection and grading using deep learning and quantum machine learning techniques, aiming to develop efficient systems for early detection and improved healthcare outcomes. He can be contacted at email: umarkcse@gmail.com.