IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5727~5735
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5727-5735

Securing internet of things networks: hybrid deep learning for advanced threat detection

K. Venkata Subba Reddy[1], Shirisha Kasireddy[2], Venugopal Gaddam[3], Jagirdar Srinivas [4], Yadavalli Suresh Kumar[5], M. Madhusudhana Subramanyam[6]
[1]Department of Information Technology, Vidya Jyothi Institute of Technology, Hyderabad, India
[2]Department of Computer Science and Engineering (AI&ML), Vignana Bharathi Institute of Technology, Hyderabad, India
[3]Department of Computer Science and Engineering (AI&ML), Bonam Venkata Chalamayya Engineering College, Amalapuram, India
[4]Department of Information Technology, Matrusri Engineering College, Hyderabad, India
[5]Department of Computer Science and Engineering, Aditya University, Surampalem, India
[6]Department of Computer science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India

Article Info

Article history:

Received Jun 9, 2025
Revised Aug 14, 2026
Accepted Sep 20, 2026

Keywords:

Autoencoders
Deep belief networks
Internet of things security
Optimization techniques
Real-time IoT threat detection
Self-organizing maps

ABSTRACT

The rapid growth of internet of things (IoT) infrastructures has introduced serious security challenges due to the increasing sophistication and frequency of cyberattacks. Traditional intrusion detection techniques often struggle to cope with the dynamic and heterogeneous nature of IoT traffic, particularly when confronting previously unseen threats. To address this issue, this work presents a hybrid deep learning–based intrusion detection framework that integrates self-organizing maps (SOMs), deep belief networks (DBNs), and autoencoders to enhance both anomaly detection and attack classification. The proposed framework effectively captures complex spatial and hierarchical patterns within IoT network traffic while reducing feature redundancy. Model parameters are optimized using particle swarm optimization (PSO) to improve convergence speed and detection reliability. Extensive experiments conducted on benchmark datasets, including network security laboratory–knowledge discovery and data mining dataset (NSL-KDD), University of New South Wales–network based 2015 (UNSW-NB15) dataset, and Canadian Institute for Cybersecurity internet of things 2023 dataset (CICIoT2023), demonstrate strong detection capability across diverse attack scenarios. The proposed model achieves detection accuracies approaching 99.7%, with Matthew's correlation coefficient (MCC) values exceeding 99.2%, while maintaining low false alarm rates. These results confirm the framework's robustness, scalability, and suitability for real-time IoT security applications, particularly in rapidly evolving threat environments.

This is an open access article under the CC BY-SA license.

Corresponding Author:

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

1. INTRODUCTION

Internet of things (IoT) devices, essential in consumer and industrial contexts, have grown rapidly, complicating network traffic. Intelligent homes and industrial automation are subject to sophisticated hacks that evolve [1]–[4]. Fraudsters might exploit security holes in IoT ecosystems due to their rapid expansion, making standard detection methods unable to keep up. Advanced detection systems that recognize hazards

and react to new assault strategies are needed. Signature-based intrusion detection systems (IDS) limit network security by using threat detection patterns. They can patch vulnerabilities, but their reactive strategy cannot manage zero-day attacks in the continually evolving threat landscape [5]. Traditional systems struggle to accurately process and interpret network data in real time due to IoT traffic growth [6]. This gap emphasizes the need for innovative, resilient, and scalable IoT network protection against multiple threats. This paper provides a novel network intrusion detection framework to fix the concerns. Self-organizing maps (SOMs), deep belief networks (DBNs), autoencoders, and new optimization algorithms improve detection and operational efficiency. The framework comprehensively examines IoT traffic's complicated spatial and temporal aspects. This extensive analysis finds strange behaviors that typical approaches ignore, especially in fast-changing network situations. This improves detection precision and address scalability, making the framework suited for real-time use in massive IoT networks. A complete intrusion detection framework for dynamic and data-rich IoT environments using advanced machine learning and optimization methods.

Machine learning-based IDS have improved to use hybrid models that mix supervised and unsupervised learning to detect complex threats [7], [8]. Attention processes have increased deep learning model performance and interpretability, helping researchers understand model predictions [8]. This study uses SOMs, DBNs, and autoencoders to address IoT security issues, expanding on recent accomplishments. Finally, the detection mechanism improves network security. Modern machine learning methods are used to overcome present constraints and provide a flexible and scalable response to IoT cyberattacks. The approach, experimental setting, and results are explained in the following sections to demonstrate the framework's usefulness in real-world IoT applications. IoT threat detection developments favour mixed models with supervised and unsupervised learning. These models improve detection accuracy, flexibility, and robustness over conventional approaches by using both paradigms. SOMs helped Kaliyaperumal *et al.* [9] find unexpected risks in dynamic IoT ecosystems using hybrid unsupervised learning. Tariq *et al.* [10] created a hybrid IDS that detects new and existing threats, including zero-day attacks in IoT networks, using machine learning and signature-based methodologies. Liao *et al.* [11] created a supervised learning-spider monkey optimization model for feature selection. This method enhances feature selection in resource-limited IoT applications that prioritize computational efficiency. Other improvements include adversarial realism and robust learning. Vitorino [12] investigated hybrid learning to strengthen IoT IDS against adversaries. To better distinguish complicated assault patterns, Zhang *et al.* [13] investigated hybrid anomaly detection models that integrated autoencoders and machine learning. A convolutional neural network fused with a deep stacked autoencoder (CNN-FDSA) by Kalidindi and Arrama [14] is a deep learning IoT threat detection breakthrough. CNNs and DSAs identify IoT botnet attacks in this unique deep learning system. IoT network traffic and data imbalance are analyzed using quantile normalization, information gain, city block distance, and oversampling. CNN-FDSA handles complicated, imbalanced datasets with 92.4% accuracy, precision, recall, and F-measure and decreases false positives. This research could detect botnets in real time and construct multi-layered IoT security frameworks.

Intrusion detection in IoT networks may access sensitive data, raising privacy concerns. Federated learning (FL) does not eliminate data leakage or model accuracy issues. George and Pranggono [15] suggested a FL-based IoT IDS employing unsupervised and supervised deep learning models to address security and privacy. FL-trained and non-FL models are compared using the network-based detection of IoT botnet attacks (N-BaIoT) dataset from nine IoT devices. Unsupervised autoencoders for anomaly detection and supervised deep neural networks (DNNs) for attack categorization improve IDS robustness and accuracy, although data leakage and model consistency remain issues. FL is decentralized, therefore model generalization across devices may reduce accuracy, and sensitive data may leak into model training, compromising privacy and security. Federated averaging with momentum (FedAvgM) FL and hyperparameter tweaking improve model performance, with the FL-trained unsupervised autoencoder model outperforming others on many assessment measures. FL improves IoT IDS privacy and performance despite data breaches and model accuracy issues. Isma'ila *et al.* [16] focused on privacy-preserving computation in FL and artificial intelligence (AI) data protection. In this study, homomorphic encryption, differential privacy, trusted execution environments (TEEs), and zero-knowledge proofs are investigated. Inference attacks, rogue servers, and poisoning threaten Florida privacy, the paper says. It evaluates protocol security and efficiency using modified national institute of standards and technology database (MNIST) and Canadian Institute for advanced research-10 classes (CIFAR-10). The report recommends integrating zero-knowledge proof (ZKP) and FL and studying machine unlearning for privacy and regulation. Based on privacy-enhancing blockchain and FL, Ali *et al.* [17] developed an industrial internet of things (IIoT) IDS. The report says FL's decentralization over centralized IIoT machine learning methods address privacy and computational issues. FL provides collaborative model training without releasing sensitive data, while blockchain secures data transfers. The report discusses IDS methods, IIoT security problems, and blockchain-FL research. Modern, decentralized IDSs secure IIoT networks and drive Industry 4.0.

Due to the increased use of IoT devices, real-time network intrusion detection systems (NIDS) are needed to detect complex cyberattacks. Traditional IDS methods struggle with IoT's massive, distributed systems, constrained resources, and various communication protocols [18], [19]. Recent studies have used machine learning to improve detection in adaptive and intelligent frameworks to address these difficulties. The lightweight IDS proposed by Zeng and Azumi [20] is for resource-constrained IoT devices. CNN architecture allows real-time deployment by balancing detection accuracy and computing overhead. This method lowers distributed denial of service (DDoS) and man-in-the-middle attacks but not sophisticated intrusion patterns, requiring further investigation. After these improvements, Bhukya *et al.* [21] created a deep learning-based NIDS that increases feature extraction by combining group convolution for spatial features, split-attention for feature selection, and bidirectional gated recurrent unit (BiGRU) for temporal features. A conditional tabular generative adversarial network (CTGAN) increased dataset detection accuracy for data imbalance issues. They had 91.08%, 94.55%, and 97.47% accuracy on University of New South Wales–network based 2015 (UNSW-NB15), Canadian Institute for Cybersecurity Intrusion Detection Evaluation dataset 2018 (CIC-IDS2018), and Canadian Institute for Cybersecurity-internet of things 2023 (CIC-IoT2023). Cloud–edge collaboration and transfer learning should scale the system's high computing resource needs and long training times, say the experts. IoT NIDS was improved by He *et al.* [22] with a CNN–bidirectional long short-term memory (Bi-LSTM) spatial feature extraction and temporal pattern learning system. This model had strong binary classification and detection rates on network security laboratory–knowledge discovery and data mining dataset (NSL-KDD). User-to-root (U2R) class issues owing to insufficient data suggest that data imbalance must be addressed to improve robustness. A hybrid IoT IDS by Charyyev and Gunes [23] employs deep learning and optimization to detect anomalies. The feature extraction convolutional neural network for internet of things (FECNNIoT) extracted high-level and low-level features, while binary multi-objective enhanced gorilla troops optimizer (BMEGTO) optimized feature selection. CNN-BMEGTO-k-nearest neighbors (KNN) was 99.99% accurate on telemetry and observability network for IoT (TON-IoT) and 99.86% on NSL-KDD. In accuracy, precision, recall, and F1-score, it exceeds long short-term memory (LSTM) and multilayer perceptron (MLP). Novel CNN design and gorilla troops optimizer (GTO) for multi-objective binary feature selection. Bhukya *et al.* [24] developed a deep Q-network (DQN) agent-based micro reinforcement learning classifier (MRLC) for IDS to classify binary and multiclass data finely. To enable robust learning, the MRLC evaluates each training sample as an independent experiment depending on the agent's learning rate.

Deep learning detects multi-stage IoT hacks. SOMs, DBNs, and autoencoders can reveal undiscovered attack patterns without labelled datasets [25], [26]. Research has examined the use of SOMs to map high-dimensional data into compact representations for IoT anomaly detection. Abdulkareem *et al.* [27] used autoencoders, LSTMs, GANs, SOMs, transfer learning, and attention to detect and mitigate real-time irregularities in IoT-based smart grid cybersecurity systems. Real-time adaptive mitigations autonomously mitigated cyber threats, maintaining the smart grid [27]. Comprehensive real-world testing of the system's scalability and cyberattack resilience confirmed its applicability and robustness. It outperformed previous systems in anomaly detection, intelligent mitigation, and scalability. This comprehensive and flexible solution protected IoT-based smart grids against escalating cybersecurity risks, boosting the sector. IoT network traffic temporal connections help DBNs detect complicated persistent attacks. Yang *et al.* [28] used a conditional DBN (CDBN) to identify wireless network breaches live. The researchers developed "SamSelect" under-sampling and the stacked contractive autoencoder (SCAE) for feature reduction to handle data imbalance and dimensionality. They detected real-time attacks with 97.4% accuracy and 1.14 ms detection time utilizing CDBN and these methods. To balance the Aegean Wi-Fi intrusion dataset (AWID), they pioneered wireless network intrusion detection with CDBN and SamSelect. They outperformed deep and shallow learning, were noise-resistant, and conducted cybersecurity research. Autoencoders reduce data dimensionality and separate outliers, improving detection frameworks [29]. To identify cyberattacks on autonomous vehicles (AVs) and the internet of vehicles (IoV), Ashraf *et al.* [30] developed an LSTM autoencoder-based IDS for intelligent transportation systems (ITS). The IDS used statistical feature extraction and LSTM learning to find anomalies in in-vehicle communications and external network data. By eliminating duplication and identifying highly representative traits, the approach improved heterogeneous data detection and reduced false alarms. The comprehensive solution addressed in-vehicle and external communication system threat vectors. Though promising, the system struggled to classify multiclass attacks and scale for complicated IoV environments.

2. METHOD

The suggested method uses SOMs, DBNs, and autoencoders to identify cyberattacks in IoT networks. Attack detection systems are improved by combining the strengths of each technique. SOMs are used for unsupervised clustering and anomaly detection, followed by DBNs for hierarchical data

representations. Dimensionality reduction and feature extraction using autoencoders improve model performance. These models' hyperparameters are fine-tuned using an innovative optimization method for optimal performance in real-world circumstances. Unsupervised learning is used by SOMs and artificial neural networks to reduce high-dimensional data to a lower-dimensional representation while preserving the input space's topological links [31]. These capabilities make SOMs great data visualization and clustering tools.

The SOM topology has two fully connected layers: a data input layer and a node-lattice output layer. Weights are randomly initialized to start SOM learning. Randomly choose and deliver an input vector to the lattice. Euclidean distance is used by each node to calculate its distance from the input vector. The node with the least distance is the best matching unit (BMU). A neighborhood radius is constructed around the BMU, and nearby node weights are modified to match the input vector. This competitive learning method teaches the SOM to map similar inputs to adjacent output lattice regions. IoT traffic data hierarchies are learned using DBNs. This design lets DBNs model high-dimensional IoT traffic, making them suitable for anomaly detection, feature extraction, and predictive modeling. DBNs can better grasp data linkages and features by learning a deep hierarchical structure, resulting in more robust and accurate analyses. DBNs' probabilistic restricted Boltzmann machines (RBMs) allow uncertainty and probabilistic reasoning in decision-making. Dimensionality reduction and feature extraction use autoencoders. The encoder translates input data into a lower-dimensional latent space, capturing the most important elements and rejecting unnecessary information [32]. The decoder reconstructs the original data from the compressed form, preserving important properties. It reduces noise and speeds up downstream tasks like classification, clustering, and anomaly detection. Autoencoders can also be customized for specific domains or datasets, making them adaptable for data preparation and feature engineering.

3. RESULTS AND DISCUSSION

The proposed hybrid intrusion detection framework was evaluated using the NSL-KDD, UNSW-NB15, and CICIoT2023 datasets to validate its effectiveness across heterogeneous IoT traffic environments. The obtained results demonstrate consistently high detection accuracy, strong Matthew's correlation coefficient (MCC) values, and low false alarm rates, indicating the robustness and reliability of the proposed approach when handling both known and previously unseen attack patterns. The strong detection capability can be primarily attributed to the integration of unsupervised and deep learning techniques. Unsupervised clustering mechanisms have been widely reported to be effective in identifying unknown and zero-day attacks in IoT environments, particularly when labeled data are limited. In this study, SOMs enable effective separation of anomalous and normal traffic by preserving the topological structure of high-dimensional data, which explains the improved anomaly discrimination observed across all datasets. Hierarchical feature learning using DBNs enhances the model's ability to capture complex temporal and spatial dependencies present in IoT network traffic. Similar deep learning–based intrusion detection frameworks have demonstrated improved performance when hierarchical representations are employed, especially in detecting sophisticated and persistent attack behaviors. The results obtained in this work further validate these observations, as reflected by stable performance across datasets with diverse attack distributions. Autoencoders contribute significantly by reducing feature redundancy and suppressing noise, thereby improving class separability and reducing false positives. Prior studies have shown that latent-space representations generated by autoencoders enhance detection reliability in high-dimensional network traffic. The experimental findings in this study align with these conclusions, particularly in datasets characterized by class imbalance and overlapping attack features. Furthermore, the application of particle swarm optimization (PSO) for hyperparameter tuning improves convergence stability and overall detection performance. Optimization-driven IDS reported in the literature consistently achieve higher accuracy and robustness compared to non-optimized counterparts. The superior results observed across all evaluation metrics confirm the effectiveness of this optimization strategy. The experimental analysis demonstrates that the proposed hybrid framework effectively addresses dataset-specific challenges such as imbalance, traffic diversity, and evolving attack strategies. When compared with recently reported IDS, the proposed approach exhibits competitive or superior performance, highlighting its suitability for real-time IoT security applications.

The experimental performance obtained in this study is consistent with recent advances in deep learning-based intrusion detection for IoT environments. Hossain [33] reported detection accuracies approaching 99.9% by combining CNN with an optimization algorithm for feature selection, demonstrating that optimization significantly improves classification capability. Similarly, showed that integrating deep neural architectures with enhanced feature extraction techniques substantially improves intrusion detection performance on UNSW-NB15 and CIC-IoT datasets. The proposed hybrid framework follows a comparable direction but further combines unsupervised learning through SOMs and autoencoders with hierarchical

feature extraction using DBNs, enabling effective identification of both known and previously unseen attacks. Compared with conventional machine learning approaches such as support vector machines, decision trees, random forests, and standalone CNNs reported in previous studies, the proposed hybrid framework consistently exhibits superior robustness by reducing false alarms while maintaining high detection accuracy across multiple benchmark datasets. The integration of PSO further enhances parameter selection, allowing faster convergence and improved generalization capability. These findings demonstrate that combining optimization techniques with hybrid deep learning architectures provides a reliable solution for real-time IoT intrusion detection in dynamic and heterogeneous network environments.

Parallel coordinates plots of NSL-KDD and UNSW-NB15 feature distributions for different attack classes are shown in Figure 1. Each sample line shows source bytes, error rate, and duration along the axes. Different colors represent attack classes, allowing visual pattern separation across datasets. This image shows how feature values differ between normal and attack instances, revealing overlaps and distinctive traits that can inform anomaly detection systems. To better understand the characteristics of the benchmark datasets used for intrusion detection, several visual analyses are presented. These figures illustrate the statistical distribution of important traffic features and attack categories in the NSL-KDD and UNSW-NB15 datasets. Such visualization helps identify feature variability, class imbalance, and attack diversity, which directly influence the learning capability of the proposed hybrid intrusion detection framework. The graphical analysis also provides insight into why feature extraction using SOMs, DBNs, and autoencoders is effective for distinguishing normal and malicious traffic patterns.

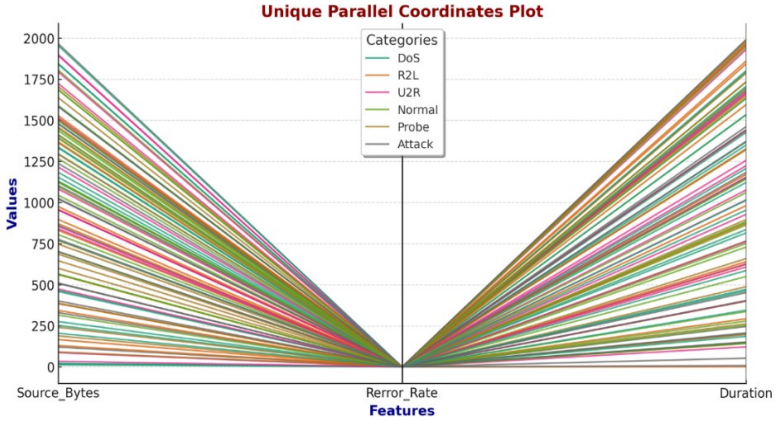


Figure 1. Parallel coordinates plot of source bytes, error rate, and duration across class labels

Figure 2 shows the NSL-KDD dataset's source byte distribution with a kernel density estimate (KDE) overlay to show the probability density function. The x-axis shows the number of source bytes, whereas the y-axis displays the instance density for each value range. This graphic shows that most connections have low source bytes and decrease in frequency as they rise. Analyzing network traffic and detecting anomalies requires understanding this distribution. The distribution of network traffic attributes is further examined using a histogram with KDE. This visualization highlights the probability distribution of source-byte values and reveals the presence of skewed traffic behavior that is commonly observed in real IoT communication. Such statistical characteristics justify the need for robust feature learning methods capable of handling heterogeneous network traffic.

Figure 3 illustrates the comparison of instances across different attack types within the NSL-KDD and UNSW-NB15 datasets. The left plot illustrates the distribution of attack instances in NSL-KDD, highlighting that DoS attacks are the most common, followed by Probe and remote-to-local (R2L) types. The right plot for UNSW-NB15, on the other hand, reveals a broader array of attack types, with exploits and DoS emerging as the most prevalent. This comparison offers valuable insights into the attack landscape present in each dataset and aids in comprehending the effectiveness of various detection methods for different types of attacks. To evaluate the diversity of cyberattacks contained in the benchmark datasets, the distribution of attack categories is illustrated. The comparison between NSL-KDD and UNSW-NB15 demonstrates significant differences in attack frequency and class imbalance. These observations emphasize the necessity of designing an intrusion detection model that maintains high detection accuracy across multiple attack types and varying data distributions.

This research shows that SOMs, DBNs, and autoencoders can improve IoT cyberattack detection. The experiments show that these models can recognize a variety of attack types, including new threats. Since

IoT systems are dynamic, the models' capacity to generalize across datasets suggests they can adapt to varied network conditions. Its ability to discover network traffic anomalies using unsupervised learning methods like SOMs and autoencoders is a major benefit. Emerging cyber dangers can make labeled data scarce; thus, the proposed technique decreases reliance on it. Optimizing model hyperparameters via PSO improves performance, showing the relevance of fine-tuning in machine learning. There are certain restrictions. Based on IoT environment factors, model performance may vary. These constraints should be addressed by testing the models in different settings and adding contextual aspects that may affect detection efficacy. The proposed model performs well on NSL-KDD, UNSW-NB15, and CICIoT2023, according to experiments. Each dataset challenges the model's robustness and flexibility with different attack methods and data distributions. This study discusses how the proposed model performs across multiple datasets, solves dataset-specific problems, and presents statistical analysis to confirm performance gains.

The comparative analysis demonstrates that the proposed framework not only achieves high classification accuracy but also maintains stable performance across datasets containing diverse attack categories and varying traffic characteristics. Unlike several existing approaches that rely on a single deep learning architecture, the integration of SOMs, DBNs, autoencoders, and PSO enables complementary feature learning, anomaly detection, and parameter optimization. Consequently, the proposed model provides improved generalization capability, making it more suitable for deployment in practical IoT environments where attack patterns continuously evolve.

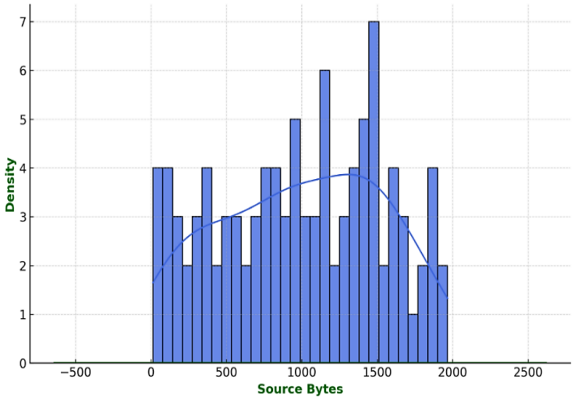
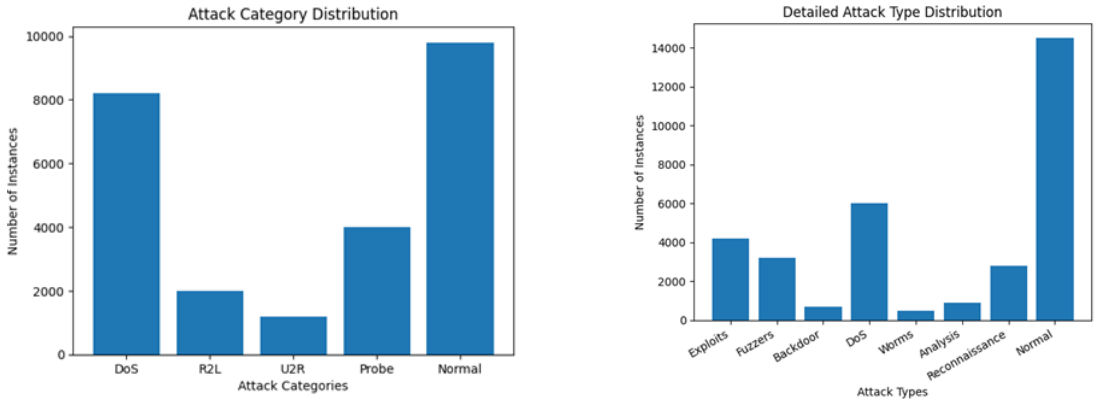


Figure 2. Source byte histogram with KDE overlay demonstrating byte size distribution and regular vs. malicious network traffic



(a) (b)

Figure 3. The distribution of attack types for (a) NSL-KDD and (b) UNSW-NB15

4. CONCLUSION

This paper outlines a thorough methodology for detecting cyber-attacks within IoT networks, showcasing the efficacy of SOMs, DBNs, and autoencoders in recognizing both familiar and unfamiliar types of attacks. The experimental results demonstrate that the proposed methodology attains high performance across multiple evaluation metrics, highlighting its potential for practical applications. Moreover, optimizing

model hyperparameters using PSO significantly improves both detection accuracy and reliability. Future work will concentrate on enhancing these models and investigating the incorporation of supplementary machine learning techniques to elevate detection capabilities. This study enhances the understanding of cybersecurity within IoT environments, emphasizing the necessity for adaptive and resilient detection mechanisms to protect against the growing complexity of cyber threats.

ACKNOWLEDGMENTS

The authors express our sincere gratitude to our Institutions for providing the necessary resources and facilities to conduct this research. The authors extend our appreciation to our advisors for their invaluable guidance, insightful feedback, and continuous encouragement throughout this study.

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
K. Venkata Subba Reddy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Shirisha Kasireddy	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Venugopal Gaddam	✓	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓
Jagirdar Srinivas	✓	✓	✓	✓			✓		✓	✓		✓		✓
Yadavalli Suresh Kumar	✓	✓	✓	✓	✓		✓		✓	✓		✓		✓
M. Madhusudhana Subramanyam	✓	✓	✓	✓			✓		✓	✓		✓		✓

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 conflicts of interest related to this research.

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, 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. 9, no. 7, 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, Apr. 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. R.-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, Mar. 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 & Security*, vol. 127, Apr. 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, Dec. 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, Jul. 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 (AIoTC)*, Sep. 2024, pp. 156–160, doi: 10.1109/AIoTC63215.2024.10748333.
[11] H. Liao *et al.*, "A survey of deep learning technologies for intrusion detection in internet of things," *IEEE Access*, vol. 12, pp. 4745–4761, 2024, doi: 10.1109/ACCESS.2023.3349287.
[12] J. P. M. Vitorino, "Realistic adversarial machine learning to improve network intrusion detection," M.S. thesis, Instituto Politécnico do Porto, Porto, Portugal, 2023.
[13] X. Zhang, P. Wei, and Q. Wang, "A hybrid anomaly detection method for high-dimensional data," *PeerJ Computer Science*, vol. 9, Jan. 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. O.-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] U. A. Isma'ila, K. U. Danyaro, A. A. Muazu, and U. D. Maiwada, "Review on approaches of federated modeling in anomaly-based intrusion detection for IoT devices," *IEEE Access*, vol. 12, pp. 30941–30961, 2024, doi: 10.1109/ACCESS.2024.3369915.
[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, Jan. 2024, doi: 10.1016/j.adhoc.2023.103320.
[18] R. Modak, S. Phadikar, K. Majumder, and A. Dasgupta, "Next-generation intrusion detection for IoT networks: a detailed survey and analysis," in *Proceedings of Sixth International Conference on Advances in Computer Engineering and Communication Systems. ICACECS 2025. Smart Innovation, Systems and Technologies*, 2026, vol. 488 SIST, pp. 402–412, doi: 10.1007/978-3-032-22114-8_37.
[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] Q. Zeng and Y. H.-Azumi, "Hardware/software codesign of real-time intrusion detection system for internet of things devices," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 22351–22363, 2024, doi: 10.1109/JIOT.2024.3380822.
[21] B. N. Bhukya, V. Venkataiah, S. M. Kuchibhatla, S. Koteswari, R. V. S. L. Kumari, and Y. R. Raju, "Integrating the internet of things to protect electric vehicle control systems from cyber attacks," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 3, pp. 433–440, 2024.
[22] M. He, Y. Huang, X. Wang, P. Wei, and X. Wang, "A Lightweight and efficient IoT intrusion detection method based on feature grouping," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2935–2949, 2024, doi: 10.1109/JIOT.2023.3294259.
[23] B. Charyyev and M. H. Gunes, "Identifying anomaly in IoT traffic flow with locality sensitive hashes," *IEEE Access*, vol. 12, pp. 89467–89478, 2024, doi: 10.1109/ACCESS.2024.3420238.
[24] B. N. Bhukya, S. M. Kuchibhatla, N. K. Bhagavatham, T. L. Narayana, M. R. Chunduru, and B. K. Madhavi, "Implementation of meta-heuristic and deep learning algorithms for power system cybersecurity," *Bulletin of Electrical Engineering and Informatics*, vol. 15, no. 1, pp. 648–656, 2026, doi: 10.11591/eei.v15i1.8569.
[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] D. Alsalman, "A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats," *IEEE Access*, vol. 12, pp. 14719–14730, 2024, doi: 10.1109/ACCESS.2024.3359033.
[27] S. A. Abdulkareem, C. H. Foh, M. Shojafar, F. Carrez, and K. Moessner, "Network intrusion detection: an IoT and non IoT-related survey," *IEEE Access*, vol. 12, pp. 147167–147191, 2024, doi: 10.1109/ACCESS.2024.3473289.
[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.
[31] A. Bensaoud and J. Kalita, "Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models," *Ad Hoc Networks*, vol. 170, Apr. 2025, doi: 10.1016/j.adhoc.2025.103770.
[32] T. Arnaut *et al*., "From restricted Boltzmann machines to deep belief networks: a multi-dataset performance study," in *Advanced Technologies, Systems, and Applications X (IAT 2025)*, vol. 1625. Cham, Switzerland: Springer, 2026, pp. 89–101, doi: 10.1007/978-3-032-05159-2_6.
[33] M. A. Hossain, "Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach," *EURASIP Journal on Information Security*, vol. 2025, no. 1, Sep. 2025, doi: 10.1186/s13635-025-00202-w.

BIOGRAPHIES OF AUTHORS



Dr. K. Venkata Subba Reddy is working as a professor in the Department of Information Technology at Vidya Jyothi Institute of Technology, Hyderabad, since June 2024. He has 21 years of experience in teaching and research. His research areas of interest is software reliability engineering, cloud computing, and quantum machine learning. He can be contacted at email: kvsreddy2012@gmail.com.



Dr. Shirisha Kasireddy is awarded a Ph.D. in Computer Science and Engineering from JNTUH, M.Tech. in Software Engineering from SIT, JNTUH, and a B.Tech. in CSIT from JNTU, Hyderabad, in 2005, respectively. She is now working as an associate professor and HoD for the Department of Computer Science and Engineering (AI&ML) in Vignana Bharathi Institute of Technology, Hyderabad, India. She has 21 years of experience. Her research interests include machine learning, deep learning, natural language processing, AI, large language models, and quantum computing. She can be contacted at email: kshirishacse@vbithyd.ac.in.



Dr. Venugopal Gaddam is working as an associate professor in the Department of Computer Science and Engineering (AI&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 has published 11 Scopus-indexed papers, 7 conference papers, and 3 book chapters. In addition, 3 SCI-indexed papers were published, and 3 more book chapters are being communicated. His research areas include machine learning, cybersecurity, quantum computing, IoT, and data mining. He can be contacted at email: venugopal.gaddam@gmail.com.



Dr. Jagirdar Srinivas is currently working as an associate professor in the Department of Information Technology at Matrusri Engineering College. He received his Ph.D. in CSE from JNTUA, Anantapuramu in 2020. He has 20 years of teaching experience. He has published 25 research papers in various reputed journals and conference proceedings. He is the author of two books and has been granted 1 patent. He received Google Cloud and Nvidia Academic grants. His areas of interest are machine learning, cloud computing, and computer algorithms. He is guiding 2 scholars from SR University. He can be contacted at email: jagirdar.srinivas@gmail.com.



Yadavalli Suresh Kumar received the B.Tech. degree in Computer Science and Engineering from West Godavari Institute of Science and Technology, Andhra Pradesh, India, in 2013 and the M.Tech degree in Computer Science and Technology specialization from SRKR Engineering College, Visakhapatnam, India, in 2018. Currently, he is pursuing a Ph.D. at Aditya University. He is an assistant professor at the Department of Computer Science and Engineering, Aditya University, Surampalem, Andhara Pradesh, India. His research interests include AI and ML, cybersecurity, data science and big data, computer vision, and distributed systems and cloud computing. He can be contacted at email: ysureshkumar24@gmail.com.



M. Madhusidhana Subramanyam received his master of computer applications (MCA) from Osmania University, India, in 1998 and earned his Ph.D. in Computer Science from Sunrise University in 2015. He is currently an associate professor in Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Narsipatnam, India. His academic and research interests include software engineering, data science, distributed systems, cloud computing, and AI. He can be contacted at email: mmsnaidu@gmail.com.