International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 3, Issue 4, July – August (2025)

RESEARCH ARTICLE

HYDEST-IOT: A HYBRID DEEP LEARNING FRAMEWORK FOR EFFICIENT INTRUSION DETECTION IN RESOURCE-CONSTRAINED IOT NETWORKS

A. P. Gopu [1, *] and S. Gokulraj [2]

[1] Assistant Professor, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India.
[2] Associate Professor, Department of Cyber Security, Dr. N.G.P. Institute of Technology, Coimbatore, India.
[*] *Corresponding e-mail: gopumecse@gmail.com*

Abstract – The rapid expansion of the Internet of Things (IoT) creates a modern infrastructure that is challenging for robust security. Vulnerability is an important issue for connected devices against various intrusion attacks. The existing systems face some challenges when considering Deep Learning (DL) methods, which include computational cost, real-time detection, and unseen threats generalization. To overcome these problems, in this paper proposes a Hybrid Intrusion Detection System for IoT (HYDEST-IoT) that can detect the cyber threats efficiently. The system is built on top of a Sparse Autoencoder (SAE) for feature extraction and Bidirectional Gated Recurrent Unit (BiGRU) for precise temporal pattern classification. The objective of this work is to provide a robust and efficient Intrusion Detection System (IDS) for resource-limited IoT deployments. This study was implemented using Python and it was trained and tested through the NSL-KDD dataset. This provided a comparison of HYDEST-IoT with existing methods including A-BiLSTM, SAE-CNN, and DCGR_IoT. The proposed HYDEST-IoT reached 99.7% accuracy, a lower False Alarm Rate (FAR) and less computational time of 4s, in which it gets both efficiency and detection performance. HYDEST-IoT was a small framework that could be used for such resource starved IoT environment.

Keywords – *Intrusion Detection System, Internet of Things, Hybrid Deep Learning, Sparse Autoencoder, Bidirectional Gated Recurrent Unit.*

1. INTRODUCTION

The Internet of Things (IoT) has become important for social progress, industrial innovation and academia in recent years [1]. It relies on the use of a network of physical objects, or "things", which are linked to the Internet and each other through sensors, software and network connectivity. With this capability, they can share information and communicate with other devices, systems, and surroundings [2]. These proxies are intelligent to decide on their own and also to undertake appropriate tasks according to the data they have collected [3]. The items include infrastructure such as smart cities, homes and everyday cellphones, wearable devices, and home appliances [4]. Additionally, technology has transformed many facets of human life, including industries, cities, agriculture, homes, transportation, the military, healthcare, and more, due to its interconnectedness and capacity for data sharing [5]. A range of wireless technologies, such as Wi-Fi, Bluetooth, Radio-Frequency Identification (RFID), and cellular networks, support this ease of remote access by improving data transfer efficiency and adding further levels of intelligence to IoT surroundings [6].

Intrusion detection mechanisms for IoT are a cornerstone of ensuring the security and health of connected things in our digital world [7]. Wearable computing devices, self-driving cars, smart home appliances and industrial machinery are some of the objects that are being connected in addition to traditional networked devices under the cause of IoT [8]. They are vulnerable to attack as they involve numerous complicated interactions when joining the overall network [9]. As it deals with the risk brought by devices being interconnected in IoT, IoT ID is an essential part of cybersecurity which concerns all area [10]. Unlike conventional computing environments, IoT networks are composed of a wide variety of devices with varying security, communication protocol, and functionality [11]. The larger number of IoT devices that is not properly secured, the bigger target market for cybercriminals. There is a need for strong IDS that can quickly detect and mitigate unauthorized access to data, breaches, and other security problems. [12]

Deep learning is necessary for IoT-ID, because it can recognize and adapt to emerging threats without explicit programming. The characteristics of IoT environments, such as resource constraints, high heterogeneity of data types, and dynamic network formations, present a challenging set of issues that need to be meticulously in order to ensure the effectiveness of DL-based ID mechanisms for securing IoT ecosystems [13]. To handle these issues, a novel Hybrid Intrusion Detection System for IoT (HYDEST-IoT) system is proposed to detect vulnerabilities in IoT devices. The contribution of this model is listed below:

- The proposed HYDEST-IoT framework introduces a hybrid deep learning architecture that integrates an SAE for dimensionality reduction and a BiGRU model for capturing sequential attack patterns in IoT network traffic.
- SAE is used for feature extraction to compress high-dimensional input into compact, noise-resistant representations.
- The BiGRU-based classification mechanism processes input sequences in both forward and backward directions, allowing accurate identification of complex temporal behaviours and reducing the FAR.
- The proposed HYDEST-IoT system was evaluated using precision, recall, F1-score, accuracy, FAR, and AUC, confirming its effectiveness for IoT-ID.

The organization of the paper is structured as follows. Section 2 covers the details of the literature review. Section 3 offers a description of the developed HYDEST-IoT model. Section 4 presents the experiment's findings. Section 5 contains the future work and conclusion

2. LITERATURE REVIEW

This section offers a recent advancement of IDS in IoT environments that ensures robust cybersecurity. Numerous studies explored DL based IDS to address the cyber threats in the IoT environment. This section also highlighted key methodologies and identified the limitations in existing studies that motivated a need for more adaptive and efficient solutions.

In 2022, Banaamah and Ahmad [14] examined the effectiveness of DL-based ID techniques, several DL techniques, and determined the most effective approach for IoT-ID implementation. The DL models used in this study are based on Long Short-Term Memory (LSTM), Gated Recurrent Units (GRUs), and Convolutional Neural Networks (CNNs). To improve performance, this work can also be expanded to examine additional classifier variations, such as Genetic Algorithms (GA) and Bidirectional Long-Short Term Memory (BiLSTM).

In 2024, Alars and Kurnaz [15] introduced a traditional Network Intrusion Detection System (NIDS) that relied on a limited detection scope, predetermined signatures, and significant gaps in unanticipated intrusions and new efficient recognition. Real-time streaming data was a crucial challenge for NIDS when integrated into a continuously developing network. The result revealed that the DL based NIDS achieved 98.5% of detection accuracy compared to existing methods and effectively addressed real-world cybersecurity issues.

In 2024, Jihado and Girsang [16] developed a NIDS model by utilizing two DL methods, such as CNN and BiLSTM. Additionally, feature engineering uses Principal Component Analysis (PCA) to reduce the current features to ten dimensions and speed up model training without substantially affecting the model's performance.

In 2024, Aljehane *et al*., [17] offered the Golden Jackal Optimization Algorithm with Deep Learning-Intrusion Detection System (GJOADL-IDSNS) for network security. For tuned hyperparameter, the study applied an Attention-based Bi-directional Long Short-Term Memory (A-BiLSTM). GJOADL-IDSNS method used a BiLSTM model to train the diversity and quality data for real-world scenarios

In 2024, Alsoufi *et al*., [18] created an anomaly-based Intrusion Detection System (AIDS) for an IoT system. By computing the reconstructed error, the SAE is used to minimize the data representation and high dimension. CNN is a binary classification method. The Bot-IoT dataset is used to validate the proposed SAE-CNN technique. By minimizing training time and optimizing model complexity, it addressed resource efficiency concerns.

In 2024, Shafeiy *et al*., [19] suggested an IDS deep neural learning called Deep Complex Gated Recurrent Network-based IoT (DCGR_IoT) that protected the bidirectional network communication in an IoT environment. An advanced technique called DCGR_IoT has improved the capability of anomaly detection. Furthermore, a multidimensional feature subset created Complex Gated Recurrent Networks (CGRNs) and DCGR_IoT allowed a detailed representation of the spatial traffic network and facilitated the critical feature extraction of ID.

In 2025, Hossain [20] offered a DL-based method for detecting threats in real-time in IoT networks. It improved ID by utilizing sophisticated models like Multi-Layer Perceptrons (MLPs), CNNs, Recurrent Neural Networks (RNNs), and LSTM networks. The results enhanced the ability to identify and lessen cyberthreats in IoT systems and helped create scalable and effective DL-based security solutions.

Despite significant advancements in IDS for IoT environments using DL methods such as LSTM, BiLSTM, autoencoders, and CNN. Many existing approaches face some critical challenges, such as complexity, high computational cost, handling inefficient real-time streaming data, and modern attacks or previously unseen detection. Traditional IDS framework frequently struggles with resource-constrained IoT ecosystems, dynamic, which leads to increased FAR, poor generalization, and delayed threat responses. To address this issue, this study introduces a Hybrid Intrusion Detection System for IoT (HYDEST-IoT) framework in the next section to ensure robustness, minimize computational cost, and ensure detection accuracy

3. PROPOSED METHODOLOGY

In this section, the architecture and working flow of the proposed Hybrid Intrusion Detection System for IoT (HYDEST-IoT) are presented. Initially, the data was collected through the IoT device, which generates behavioral and traffic data. These raw data go to a preprocessing phase, which includes data cleaning to remove missing values or inconsistencies, and data normalization is used to scale the features for the balanced performance model. Then SAE is used to extract the features for essential information to reduce dimensionality, which allows a relevant and efficient representation. The extracted features are entered into the

BiGRU model to analyze the sequential data pattern for both backward and forward directions to improve the detection accuracy. Finally, the output is classified into three attacks, namely Probe, MITM, and normal. This approach ensures an accurate, scalable, and lightweight IDS solution for resource-constrained IoT environments. The proposed HYDEST-IoT architecture is shown in Figure 1

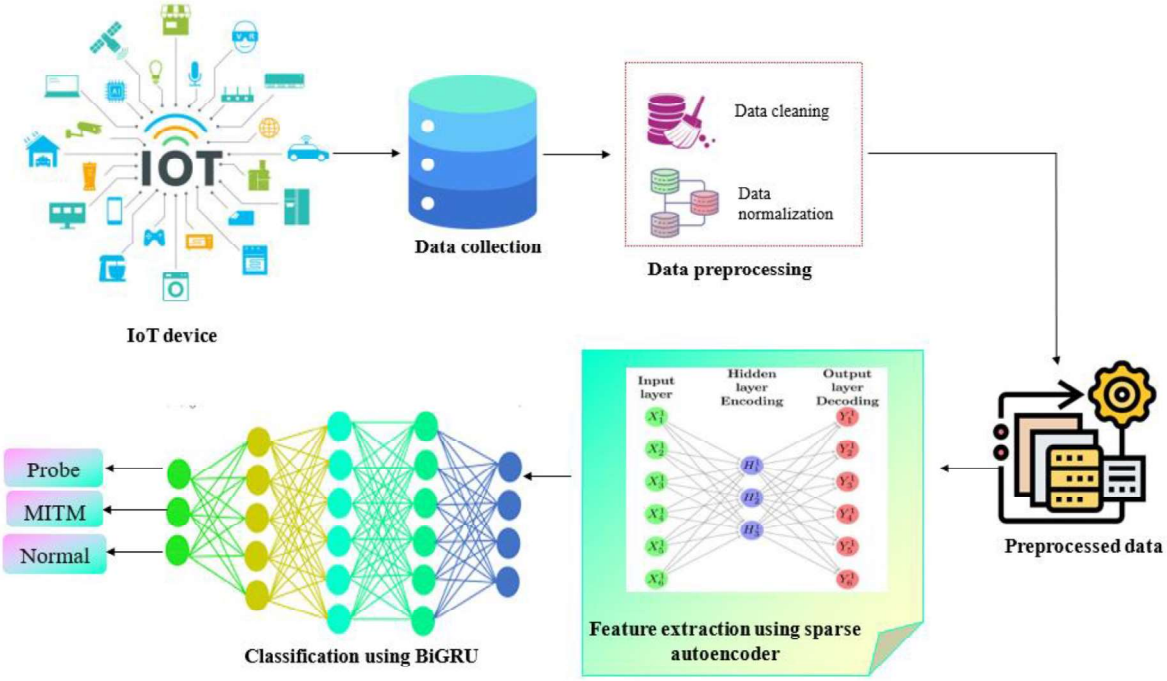

Figure 1. Overview of HYDEST-IoT architecture

3.1. Data preprocessing

The data preprocessing phase consists of two stages such as data cleaning, data normalization. The process begins with data cleaning to remove duplicates, incorrect values, and missing values in the dataset. This step is also known as data cleaning or scrubbing, which ensures the model's accuracy, reliability, effectiveness, and efficiency on IDS predictions. The third step is data normalization, which scales the imbalanced features and deteriorates the performance of the classification model. Normalization is an important feature of dominant values and is negligible into the acceptance scale. Using the minimum and maximum method, the continuous variables are converted into a range of [0,1] is expressed in Equation (1):

$$F_{norm} = \frac{F - F_{min}}{F_{max} - F_{min}} \forall f \epsilon F, \quad (1)$$

Where F_{norm} is a normalized value, and 0 and 1 are the values of F_{min} and F_{max} and remaining variables are present in the range of values. This is the base of value that makes the same range of features. To overcome the bias issue, this scaling method reduces the testing and training time of a model and ensures a fast convergence rate to improve the reliability of the classification system. Before normalization, a performance log transformation is needed for high-variance features.

3.2. Feature extraction

After preprocessing, feature extraction is used with an SAE for handling high-dimensional IoT data and retaining the most informative characteristics. This raw input data was compressed using an unsupervised neural network to decrease the encoding of feature space and then recreated the original input through decoding. For input SAE, ensure a neuron subset activity that allows noise-resistant representations, and is compact to improve the process of subsequent classification.

Input, a few outputs, and a hidden layer are the autoencoder features is an unsupervised neural network. Its objective is to reduce dimension; it avoids the curse of dimensionality by making the extracted features represent the raw data; it can be trained to produce various output features that can improve classification performance; and it can be divided into two stages such as encoding and decoding, which are represented by Equations 2 and 3:

The encoding process of the input layer to the hidden layer is expressed in Equation (2):

$$h = cO_1 * h + b_1 \quad (2)$$

The decoding process from the hidden layer to the output layer is presented in Equation (3):

$$x' = cO_2 * h + b_2 \quad (3)$$

Where h is either a linear or nonlinear transfer function, W_1 and b_1 represent the encoder's bias matrix and weight matrix, and O_2 and b_2 represent the decoder's bias matrix and weight matrix.

In the traditional autoencoder, SAE adds regularization terms and sparse constraints to the loss function to accomplish the suppression effect. It limits the neurons'

average activation value in the hidden layers. The SAE's entire function is expressed in Equation (4):

$$J_{SAE}(O,b) = J(O,b) + \beta\left(\sum_{j=1}^{h} KL(\rho \parallel \hat{\rho})\right) \quad (4)$$

where the weight factor regarding the sparse item's strength is β, and h is the number of hidden units. The difference between the average activation $\hat{\rho}$ and the constant ρ is measured by the Kullback-Leibler (KL) divergence.

3.2. Classification of the BiGRU model

The extracted features are entered into the BiGRU model, which is suitable for sequential data. The BiGRU processes the data in both backward and forward directions to capture attack patterns in the network traffic. It allows accurate detection of temporal anomaly and cyber-attack in the IoT environments, which offers a balance between classification precision and computational efficiency

BiGRU is a sequence-processing model that is composed of two GRUs. The input is sent to one GRU in a forward direction and the other in a backward manner. The RNN has been updated to become the GRU. The primary benefits of GRU are its simplified structure, training efficiency, and lower computing cost.

The underlying computation mechanism of the GRU is defined by equation (5).

$$\begin{cases} l_v = \sigma(B_l y_v + V_l k_{v-1}) \\ z_v = \sigma(B_z y_v + V_z k_{v-1}) \\ k_v = tanh\left(B_{\check{k}} y_v + V_{\check{k}}(l_v \Theta k_{v-1})\right) \\ k_v = (1 - z_v)\Theta k_{v-1} + z_v \Theta k_v \end{cases} \quad (5)$$

Intermediate states are converted to the range [0,1] using the sigmoid activation function [0,1], k_{v-1} and k_v, which are the outputs at times $v - 1$ and v, respectively. The value of the input arrangement at time v is denoted by y_v. The output is $\check{k}_v$; the reset and update gates are l_v and z_v; the coefficient matrices of the weight in each section are $B_l, B_z, B_{\check{k}}, V_l, V_z$, and $V_{\check{k}}$; $tanh$ is a hyperbolic tangent function; and Θ is the element-wise multiplication. Each time step t's output, k_v, contains two vectors from forward propagation $\overrightarrow{k_v}$ and backward propagation $\overleftarrow{k_v}$, $H_v = [\overrightarrow{k_v}, \overleftarrow{k_v}]$. Finally, the BiGRU model classifies the data into normal, probe, MITM attacks, with high accuracy, and high false positive rate.

4. RESULTS AND DISCUSSIONS

In this section NSL-KDD dataset is used to assess the proposed HYDEST-IoT model. It includes comparing both proposed and existing models across various metrics such as detection rate, computational cost, ROC Curve, FAR, accuracy, F1-score, precision, and recall. These results displayed that the proposed HYDEST-IoT achieves better than existing models like such as A-BiLSTM [17], SAE-CNN [18], and DCGR_IoT [19]. Thus, the proposed approach achieved higher detection accuracy with low computational time and lower FAR. So, the proposed model of FAR, training-validation trends, and ROC curve showed scalability, robustness, and are suitable for ID in dynamic IoT settings

4.1. Comparative Analysis

This section shows the experimental results of performance comparison for the proposed HYDEST-IoT with several existing methods, such as A-BiLSTM [17], SAE-CNN [18], and DCGR_IoT [19], for designing IDs in IoT networks.

4.2. Dataset description

The NSL-KDD is used to train and evaluate the IDM for generating new IIoT/IoT datasets for the traffic network conditions and operating the system. It includes 22,544 for testing and 125,973 for training. Each sample contains 41 attributes, either attacks or normal. This dataset consists of two attacks, namely MITM, Probe.

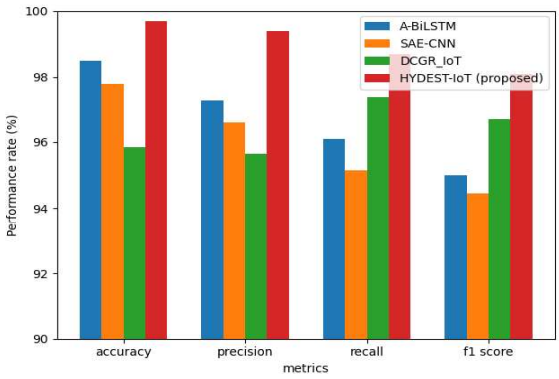

Figure 2. Performance Comparison of IDS Models Across Key Metrics

Figure 2 illustrates the performance comparison of the proposed HYDEST-IoT with three existing approaches for ID, like A-BiLSTM [17], SAE-CNN [18], and DCGR_IoT [19], across various metrics such as precision, F1-score, recall, and accuracy. By comparing the proposed and existing model, the proposed HYDEST-IoT performs better in all metrics, like 99.40% precision, 99.70% accuracy, 98.10% F1-score, and 98.70% recall, compared to the DCGR_IoT model, 95.65% precision, 95.85% accuracy, 96.70% F1-score, and 97.40% recall. These results confirm that the proposed HYDEST-IoT effectively detects the intrusion with higher reliability than the existing method of classification quality.

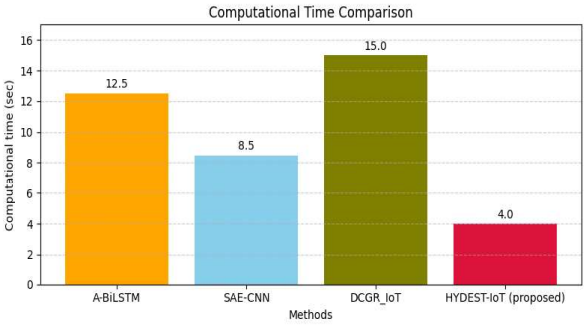

Figure 3. Computational Time Comparison for IDS Models

Figure 3 presents the computational time for each IDS. HYDEST-IoT displayed a significant outperform with the lowest computational cost of 4 seconds than existing models

such as A-BiLSTM [17], SAE-CNN [18], and DCGR_IoT [19]. Thus, the proposed HYDEST-IoT is efficient and lightweight, so it is suitable for ID in a resource-constrained IoT environment.

Figure 4 shows the value of the ROC and AUC curve across three classes. The AUC score of class 1 and class 0 achieves 0.94, and class 2 achieves 0.98 score. These results show that the HYDEST-IoT has a high AUC value across various classes, which shows a strong discriminative ability for anomalous and normal behavior. Thus, it confirms the robustness of the multi-class classification setting.

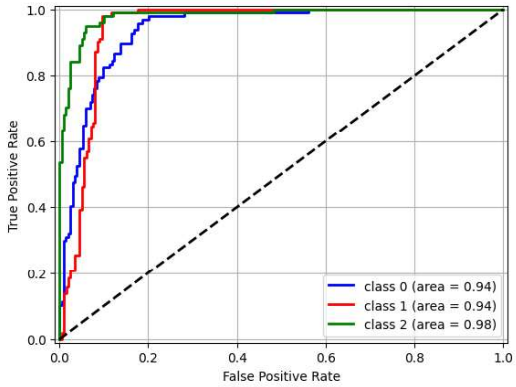

Figure 4. ROC Curve and AUC Scores for Multi-class Classification

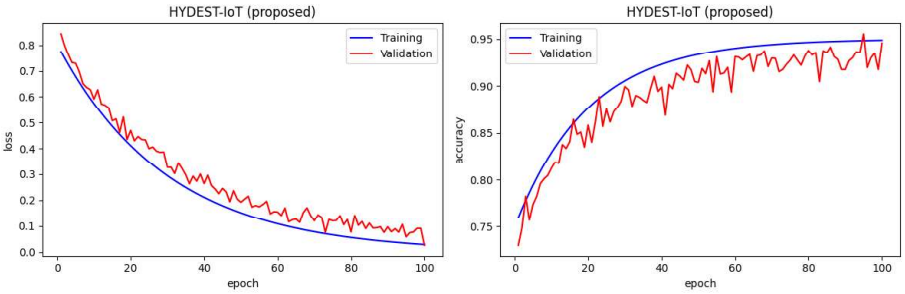

Figure 5. Training and Validation Performance of HYDEST-IoT Over Epochs

Figure 5 shows the validation and training of the dual plot of 100 epochs. For both training and validation, the left plot shows a consistent decline in loss, and the right plot shows a rise in accuracy of validation exceeding about 95%, and training occurs at 100%. These results confirm that the proposed HYDEST-IoT converges on the effectiveness of training and generalizes without the sign of overfitting

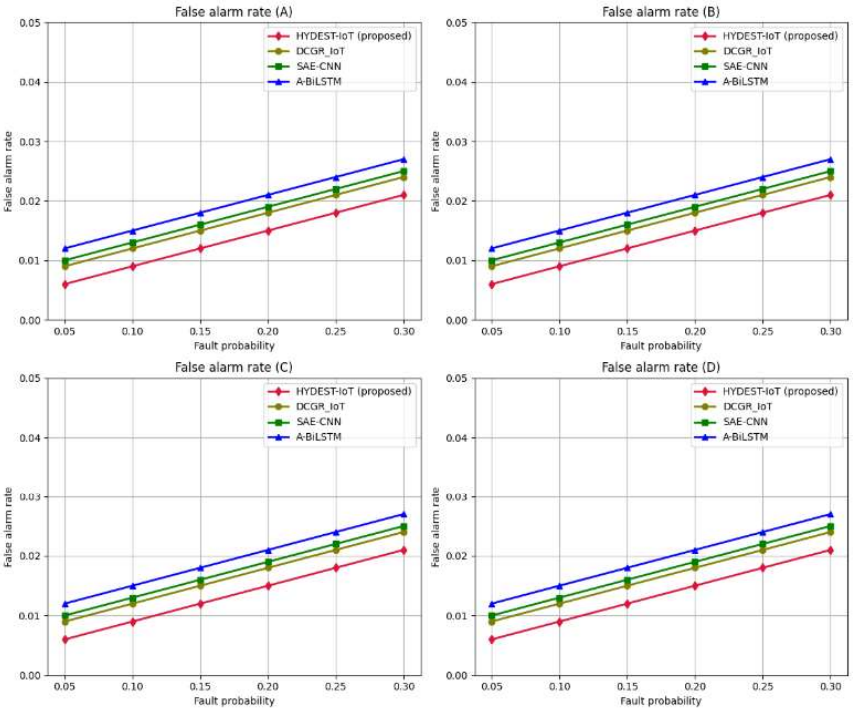

Figure 6. False Alarm Rate vs. Fault Probability

Figure 6 presents the FAR of the proposed HYDEST-IoT and existing models like A-BiLSTM [17], SAE-CNN [18], and DCGR_IoT [19] across four testing scenarios (A to D) under varying fault probability (0.05 to 0.30). In all the scenarios proposed, HYDEST-IoT shows the lowest FAR, which maintains high reliability under the fault probability. Thus, it is a critical feature of deployment in a dynamic IoT environment

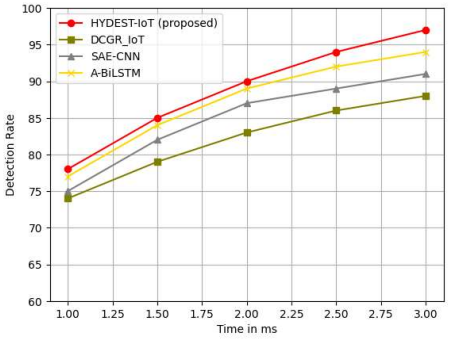

Figure 7. Detection Rate Over Time for Various IDS Models

Figure 7 displays the contrast of the proposed HYDEST-IoT with other models like A-BiLSTM [17], SAE-CNN [18], and DCGR_IoT [19] over different time intervals (1.0 ms to 3.0 ms). HYDEST-IoT starts with a higher detection rate of 78%, then it steadily improves to reach over 97% at 3.0 ms. While the other model shows a lower detection rate but HYDEST-IoT offers a lower computational cost and a favourable trade-off with a lower FAR, thus it is suitable and crucial for efficiency and precision for time-sensitive IoT applications

5. CONCLUSION

This study introduced a Hybrid Intrusion Detection System for IoT (HYDEST-IoT) to detect cyber threats effectively. SAE for reduced noise reduction, compact with BiGRU for rich temporal classification. This study was implemented using Python, which was evaluated and trained using the NSL-KDD dataset. This showed a comparison of proposed HYDEST-IoT and existing methods like A-BiLSTM [17], SAE-CNN [18], and DCGR_IoT [19]. The proposed HYDEST-IoT achieved an accuracy of 99.7%, a lower FAR, and computational time of 4s, which gains both efficiency and detection performance. HYDEST-IoT was a lightweight framework which is suitable for resource-constrained IoT deployments. In future work edge edge-based computing and federated learning extend the system for real-time Python-based deployment for IoT networks across heterogeneous environments to enhance the adaptability, privacy, and scalability to emerging threats

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] D. Javeed, M.S. Saeed, M. Adil, P. Kumar, and A. Jolfaei, "A federated learning-based zero trust intrusion detection system for Internet of Things". *Ad Hoc Networks*, vol. 162, pp. 103540, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] A.A. Wardana, G. Kołaczek, and P. Sukarno, "Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things". *Applied Sciences*, vol. 14, no. 10, pp. 4109, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Q. Zeng and Y. Hara-Azumi, "Hardware/Software Codesign of Real-Time Intrusion Detection System for Internet of Things Devices," *in IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 22351-22363, 2024[CrossRef] [Google Scholar] [Publisher Link]

[4] K. Alemerien, S. Al-Suhemat, and M. Almahadin, "Towards optimized machine-learning-driven intrusion detection for Internet of Things applications", *International Journal of Information Technology*, pp.1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] S. Jamshidi, A. Nikanjam, K.W. Nafi, F. Khomh, and R. Rasta, "Application of deep reinforcement learning for intrusion detection in Internet of Things: A systematic review", *Internet of Things*, pp. 101531, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] B. Isong, O. Kgote, and A. Abu-Mahfouz. Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems. Electronics, vol. 13, no. 12, pp. 2370, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] A. Kaushik, and H. Al-Raweshidy. "A novel intrusion detection system for internet of things devices and data". *Wireless Networks*, vol. 30, no. 1, pp. 285-294, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] 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. [CrossRef] [Google Scholar] [Publisher Link]

[9] M.A. Qathrady, S. Ullah, M.S. Alshehri, J. Ahmad, S. Almakdi, S.M. Alqhtani, M.A. Khan, and B. Ghaleb. SACNN-IDS: A self-attention convolutional neural network for intrusion detection in industrial internet of things. CAAI Transactions on Intelligence Technology, vol. 9, no. 6, pp. 1398-1411, 2024[CrossRef] [Google Scholar] [Publisher Link]

[10] U. Otokwala, A. Petrovski, and H. Kalutarage, "Optimized common features selection and deep-autoencoder (OCFSDA) for lightweight intrusion detection in Internet of things". *International Journal of Information Security*, vol. 23, no. 4, pp. 2559-2581, 2024[CrossRef] [Google Scholar] [Publisher Link]

[11] A. Biju, and S.W. Franklin. "Network intrusion detection system with an edge based hybrid feature selection approach". *computing*, vol. 9, pp. 10, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] J. Arshad, M.A. Azad, M.M. Abdeltaif, and K. Salah. "An intrusion detection framework for energy constrained IoT devices". *Mechanical Systems and Signal Processing*, vol.

136, pp. 106436, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] I. Rasheed, F. Hu, and L. Zhang. "Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN". *Vehicular Communications,* vol. 26, pp. 100266, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] A.M. Banaamah, and I. Ahmad. "Intrusion detection in IoT using deep learning". Sensors, vol. 22, no. 21, pp. 8417, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] E.S.A. Alars, and S. Kurnaz. "Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: deep learning and IoT perspective". *Discover Computing*, vol. 27, no. 1, pp. 39, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] K. Mala, S. Renuka, K. Lavanya, and M. YM. "Hybrid Deep Learning Approach for Efficient Intrusion Detection Using DCNN and BiLSTM", *In 2025 3rd International Conference on Data Science and Network Security (ICDSNS),* pp. 1-6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] N.O. Aljehane, H.A. Mengash, M.M. Eltahir, F.A. Alotaibi, S.S. Aljameel, A. Yafoz, R. Alsini, and M. Assiri. "Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security". *Alexandria Engineering Journal*, vol. 86, pp. 415-424, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] M.A. Alsoufi, M.M. Siraj, F.A. Ghaleb, M. Al-Razgan, M.S. Al-Asaly, T. Alfakih, and F. Saeed, "Anomaly-based intrusion detection model using deep learning for IoT Networks". *Computer Modeling in Engineering & Sciences*, vol. 141, no. 1, pp. 823-845, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] E. El-Shafeiy, W.M. Elsayed, H. Elwahsh, M. Alsabaan, M.I. Ibrahem, and G.F. Elhady. "Deep Complex Gated Recurrent Networks-Based IoT Network Intrusion Detection Systems". *Sensors*, vol. 24, no. 18, pp. 5933, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] M.A. Hossain. "Deep Learning-Based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach", 2025[CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

A. P. Gopu is currently serving as an Assistant Professor in the Department of Computer Science and Engineering at Velalar College of Engineering and Technology, Erode, Tamil Nadu. He holds a Ph.D. in Computer Science and Engineering from Anna University, Chennai, with his research focusing on "Next-Generation Solutions for Secure Data Transmission: Improved CGAN and Federated Learning with PPGAN." With over 14 years of academic experience, Dr. Gopu has contributed extensively to teaching, research, and academic administration. His areas of specialization include Network Security, Deep Learning, and Cloud Computing. Throughout his career, he has been actively involved in mentoring students and guiding research, having supervised 15 undergraduate and 3 postgraduate projects. Dr. Gopu has authored over 10 research papers published in reputed international journals and presented 17 papers at national and international conferences. He has also published two books and has completed seven online certification courses related to his domain.

S. Gokulraj is currently serving as an Associate Professor in the Department of Cyber security at Dr.N.G.P.Institute of Technology, Coimbatore, and Tamil Nadu. He holds a Ph.D. in Computer Science and Engineering from Anna University, Chennai, with his research focusing on "Next-Generation Solutions for Secure Data Transmission: Improved CGAN and Federated Learning with PPGAN." Dr. S.Gokulraj has completed his Bachelor of Engineering Degree in CSE from Paavai Engineering College, Anna University, Chennai; he did his Master of Engineering in Computer Science and Engineering from Paavai Engineering, College, Anna University, Chennai. He received his doctor of philosophy in Computer Science and Engineering from Anna University, Chennai with Cloud Computing and Optimization as his research realm. He has guided more than 100 Post and Undergraduate students. He has published as many as 20 papers in reputed International Journals, International and National Conferences. He also has published 5 patents in Indian patent journal and 1 Copyrights. His notable publications include research on secure Cost Optimization, Security in Cloud, Block chain integration in cloud computing, and healthcare data classification using AI and machine learning.

Arrived: 02.07.2025
Accepted: 05.08.2025