Advances in Computer Engineering and Science (ACES) (2026)
Volume -1, Issues – 3 (July–September)

Anomaly-Based Detection of Distributed Denial of Service Attacks in Internet of Things Using Deep Autoencoder

B. FATHIMAMARY
Department of Commerce (Computer Applications)
St.Joseph's College (Autonomous), Tiruchirappalli, TamilNadu, India
fathimamary_cc2@mail.sjctni.edu

N SUBBAREDDY RAMIREDDY
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India – 522302
rnsreddi@gmail.com

K VIJAYAKUMARI
Department of Computer Science
Trinity College for Women, Namakkal, Tamilnadu, India
k.vijikumari@gmail.com

Abstract: ***The rapid expansion of the Internet of Things (IoT) has introduced unprecedented levels of connectivity and automation, but it has also increased susceptibility to cyber threats, particularly distributed denial of service (DDoS) attacks. Traditional detection systems often struggle to adapt to the dynamic and resource-constrained nature of IoT environments. This research investigates the application of deep learning (DL) -based unsupervised learning methods, such as various autoencoder (AE) architectures, for effective anomaly detection of DDoS attacks in IoT networks. We evaluate four autoencoder variants, such as conventional AE, denoising AE (DAE), sparse AE (SAE), and variational AE (VAE), to model and reconstruct normal traffic behaviour. Any significant deviation, measured via reconstruction error, is flagged as a potential anomaly. Experimental results on benchmark IoT datasets demonstrate that VAE achieves the highest detection performance, with improved precision and robustness in identifying diverse DDoS patterns. The finding underscores the effectiveness of deep AE for unsupervised DDoS and offers valuable insights for developing lightweight, scalable, and adaptive security frameworks for IoT systems.***

Keywords: Deep learning; Autoencoder; DDoS attack detection; Internet of Things; Feature selection;

I. INTRODUCTION

The IoT is an enormous network of objects that may be linked to the internet and to one another to share information and services. According to formal definitions, it is a network of connected devices, or things, that can be individually recognized and communicate data. In contrast to other conventional networks, it allows us to communicate, participate, and work together on projects without joining the activity itself [1, 2]. The number of connected devices is expected to be 75 billion by 2030. The primary reasons why IoT is better are its scalability, non-interference, and more extensive coverage [3]. The IoT has revolutionized the digital world by enabling unified connectivity between billions of smart devices [4]. While this advancement fosters innovation in smart cities, healthcare, manufacturing, and automation, it also introduces critical security challenges. One of the most severe threats in IoT environments is the DDoS attack, which can flood the network with illegitimate traffic and paralyze connected services. DDoS attack detection plays a dangerous part in securing IoT environments, which are fundamentally vulnerable due to their significant, heterogeneous, and resource-constrained nature [5]. IoT systems often support real-time applications where continuous availability is crucial. Hence, DDoS attack detection avoids resource collapse by detecting and filtering malicious traffic before it overwhelms the system. Traditional DDoS attack detection methods are often ineffective in such scenarios due to the heterogeneous, dynamic, and resource-constrained nature of IoT devices [6]. To develop intelligent, well-organized, and scalable detection mechanisms that can precisely recognize and mitigate DDoS attacks in IoT networks to confirm service availability, security, and system flexibility.

DL algorithms play a transformative role in enhancing the security of IoT networks, especially for detecting DDoS attacks. DL methods can learn patterns automatically, generalize from data, and adapt to new threats, making them highly effective for real-time detection. AE is an unsupervised method that has emerged as a promising method for anomaly detection to address the above challenges. AE is a kind of unsupervised DL method that is widely used for anomaly detection, making it particularly suitable for identifying DDoS attacks in an IoT environment. IoT networks produce massive volumes of diverse and dynamic data, and AE-based models are effective in learning normal behavioural patterns and detecting deviations caused by malicious traffic. AE ability to learn normal network behaviour and identify deviations indicative of malicious activity based on reconstruction error. The work carried out various AE methods such as AE, DAE, SAE, and VAE for identifying DDoS attacks in an IoT environment. Different activation functions such as Sigmoid, ReLU, and Tanh are considered for identifying the optimal method. The major aim of the research is to develop and compare the performance of various AE methods for DDoS attack detection with a specific focus on how various activation functions impact detection performance. The goal is to identify the most efficient detection model and activation function for making a more efficient, robust, and scalable detection method. AE method variants have several benefits over current models. These models are notable for their minimal resource consumption and short execution time, in addition to their competitive performance in anomaly detection. Because of these characteristics, it is a useful and effective solution in circumstances where resources might be few. AE is especially useful in situations where speed and efficiency are crucial since it achieves a decent balance between performance

and resource requirements when compared to other models that have used the same data. The contributions are as follows,

- A comprehensive comparative study of five AE variants for anomaly-based DDoS attack detection in IoT environments.
- A feature selection approach helps enhance performance by eliminating irrelevant features.
- Detailed analysis is conducted to identify the impact of the activation function on each model.
- Experimental validation using the BoT-IoT dataset is used to indicate the superiority of the detection method in terms of accuracy and robustness.
- A flexible and lightweight framework suitable for real-time deployment in resource-constrained IoT infrastructures.
- Recommendations for selecting appropriate autoencoder architectures and activation functions in future IoT security systems.

The remaining parts of the paper are organized as follows: Section 2 discusses the related work, Section 3 shows the research methods, Section 4 shows the experimental results and analysis, and Section 5 shows the conclusions of the research work.

II. RELATED WORKS

Role of related work focussed on recent research paper focused on DDoS attack detection method for analyse the limitations and research gaps. The following paragraphs discuss some recent research papers. F. S. Alrayes et al.(2024) [7] developed a new detection method for DDOS attacks in IoT using denoising AE (DAE). The developed approach can identify and stop DDoS attacks in real-time. The results show how efficiently the developed method prevents unauthorized users from gaining access to IoT devices, reducing the opportunity of problems with security, privacy, and system integrity. A. L. Yaser et al.(2024) [8] suggest a hybrid approach that combines feedforward neural networks (FFNN) as AE and DL to detect DDoS attacks. For the training and testing models, two datasets were examined, initially statically and subsequently iteratively. Each self-encoding model uses a hidden layer, and the input and hidden layers of these models are stacked layer by layer to create the auto-encoding model. M. K. Tanati et al.(2025) [9] developed Dense Capsule SAE (DCSAE) to detect the presence of DDoS attacks. Improved Fire Hawks Optimization (IFHO) is used to optimise the DCSAE. The Hybrid Remora Whale Optimization (HRWO) is used to assign the bandwidth once the attack is distinguished. Then, Improved Osprey Optimization (IOO) is used to recognize a well routing path by taking into account features such as drop, delay, and energy usage. G. Sugitha et al.(2025) [10] developed an SAE-based DNN method for detection. The optimal features are selected using the GEO (Golden eagle optimization). Then, the selected features are employed for detection purposes using a detection algorithm for classifying either normal or anomalies.

Basati et al.(2022)[11] presents a new and parallel deep AE (PDAE) method for detecting DDoS attacks. The developed method separates the features, which allows for growth in accuracy while significantly dropping the number of parameters and the requirement for processing power. R. Savithramma et al.(2024)[12] propose a novel method for attack detection by combining two alterations based on the Adaptive Neuro-Fuzzy Inference System (ANFIS). Relational AE (RAE) is used for feature extraction to enhance the performance of ANFIS. Parameters of ANFIS are optimized with the help of Gaussian kernel membership functions and the Enhanced Osprey optimization algorithm (EOOA). H. Wasswa et al.(2023) [13] developed a leveraged VAE for botnet detection to enhance the detection of attacks of the minority class. The developed method is analysed on a multiclass classification problem on highly imbalanced datasets.

A. Kalidindi et al.(2023) [14] developed a new detection technique which is accomplished with deep SAE (DSAE). The information gain method is used to extract more informative information from the traffic dataset, which is used to detect abnormal activities. Parameters of DSAE are adjusted using the Adam average subtraction method (AAS). K. Saranya et al. (2025) [15] developed a cross-layer detection technique based on the Multi-Layered DAE (M-LDAE). M-LDAE can extract latent representations by utilizing DAE's hierarchical simplification capabilities. This technique successfully protects against a range of cyberthreats. The M-LDAE uses DL to enhance detection and adjust to new attack techniques. A. Kalidindi et al. (2025) [16] created a DL model to detect IoT botnets. First, the Internet of Things network is emulated, and the log data is used to build attack detection. Quantile normalization is the next step in the data pre-processing process, which uses the log data as input. Then, City Block Distance and Information Gain (IG) are used to implement feature selection. Following feature selection, data augmentation is carried out by increasing the number of samples through oversampling. Finally, by combining DSA with Convolutional Neural Network (CNN), the suggested CNN with DSAE (CNN-FDSA) is used to detect Botnet attacks [17]. H. Rhachi et al. (2025) [18] developed a new technique based on AE to categorize anomalous communications. The ANOVA F-Test is used for feature selection.

A. Alqahtani [19] (2025) suggests a hybrid DAE and BiLSTM to keep energetic networks from rapid and effective threat detection. The SSOA (Sparrow Search Optimization) is implemented to improve model hyperparameters. The suggested optimization strategy proved to be effective across a range of platforms, flexible enough to adjust to evolving needs, and able to manage heavier workloads. P. Pajila et al. (2025) suggested a security scheme based on AE and a DNN to detect DDoS attacks. It is quite challenging to distinguish between malicious and legitimate network traffic using conventional approaches. As a result, some attacks will continue for a while. Different types of attacks can impact the network. AE-DNNs are used in tandem to address these issues; AE is primarily used for feature extraction, while DNN is used for classification. However, recent method demonstrated considerable progress in AE-based DL methods for DDoS attack detection. However, real-time deployment, lightweight design for IoT nodes, adaptability, robustness, and comprehensive evaluation with different datasets are remarkable challenges that are identified limitation the need for more

efficient, scalable, and interpretable models tailored for heterogeneous IoT networks.

III. Research Methods

The present section discusses the different AE methods such as conventional AE, DAE, SAE, and VAE.

A. Autoencoder (AE)

An encoder and a decoder that have been trained to replicate their input while minimizing the reconstruction error comprise autoencoders. By employing fully connected layers and placing certain restrictions on the learning process, the encoder can extract features from the input vector, and the decoder uses the learned features to try to replicate the same input. This makes them appropriate for anomaly detection. Given an input sample $x_i^{m\times n}$ (m – data samples and n – is the number of features, where $l < n < n$ is the dimension of the learned features. Note that between the encoder and decoder levels, there could be several hidden layers. It is called a deep AE if there are several hidden layers. Through a non-linear mapping, the encoder converts the input vector x into a hidden representation h_j $(j = 1, \dots, l)$ as follows:

$$h_j = \sigma(\sum_{i=1}^{n} W_{ij} \times x_i + b_j) \quad (1)$$

where σ is a $sigmoid$ or $tan\ h$, W_{ij} is the weight between input and output layers. b_j is the bias in the hidden layer. The input layer is represented as follows,

$$\tilde{x_\iota} = \sigma(\sum_{j=1}^{l} \hat{W}_{ij} \times h_j + \hat{b}_j) \quad (2)$$

The autoencoder uses the average error, which is considered the MSE between the original and reconstructed input, to try to optimize the hyperparameters to minimize the reconstruction loss between x and its reconstruction $\tilde{x}$

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\|x_i - \tilde{x_i}\|^2 \quad (3)$$

B. Denoising AE (DAE)

DAE model captures the important features of the input data to improve them for supervised classification tasks. Through the integration of representation learning and classification, the model seeks to enhance intrusion detection capabilities in IoT systems by efficiently identifying and mitigating potential security threats. The DAE, a DL model, is the primary innovative technique used in our methodology. A DAE is a kind of DL model that learns to reproduce the original data to eliminate noise from damaged or noisy data. Reducing the difference between the original and recreated data is the aim of the training process. DAE can be layered to create deep networks, which will increase efficiency[7].

C. Sparse AE (SAE)

The SAE extracts sparse data characteristics by supplementing the conventional AE with a sparse penalty term. SEA employs a nonlinear transformation to retrieve the hidden dispersed features from the input samples after learning the data. Additionally, to increase feature extraction accuracy and efficiency, SEA uses a sparse penalty to extract sparse data features. Compared to the typical AE that cannot extract features, a SAE effectively extracts features [20, 21]. This implies that the input size, also known as the sparse auto-encoder, may be smaller than the size of the hidden layers.

D. Variational AE (VAE)

VAE does not require a balanced datasets that can learning any training data size and do not require a balanced data set. Two neural networks are combined to create a VAE [22]. The encoder, the initial neural network, receives inputs and expresses them in a reduced-dimensional latent space. Only a joint probability distribution of the key variables represents the hidden space. The Kullback-Leibler (KL) divergence must be minimized for the distribution to be considered normal. The second neural network aims to rebuild the initial input data by using samples from the latent space as input. The loss that should be kept to a minimum is the difference or dissimilarity between the original input and the reconstructed output. The loss function minimizes the total of the reconstruction and KL loss during training. Under restrictions such as lower hidden layers and the requirement that the joint probability distribution of features be Gaussian, a VAE tries to replicate the input.

IV. Experimental Results and Analysis

Experimental results play a vital role in assessing the performance of the detection method. AEs with their variant such as AE, DAE, SAE, and VAE [23]are used for detection due to their ability to learn compact representations and highlight deviations in network traffic. Experimental evaluation provides the necessary empirical evidence to determine how effectively each model can distinguish between benign and malicious traffic in a real-time IoT network. The results can determine which model offers superior detection ability for DDoS attacks based on these metrics across different AE variants. The present research work was carried out on different activation functions and variants of AE methods for DDoS attacks. The following subsections discuss in detail the dataset, performance measures, and results.

A. Dataset details

The UNSW established the BoT-IoT dataset by producing a genuine network. Regular and Botnet traffic were separated [24] ("https://research.unsw.edu.au/projects/bot-iot-dataset"). The dataset was first divided into two parts, or the train and test split. 20% of the data was set aside for the testing dataset, which enabled us to evaluate the models using extra, unseen data, while the remaining 80% of the data was used for training and evaluating the selected machine learning approaches. Table 1 shows the parameter settings

B. Preprocessing

- *Data encoding:* The dataset has several qualities that can be categorized. The category attributes must be converted into numerical values. This was accomplished via one-hot encoding. In this work, label encoding is used to alter categorical attributes. '0' and '1'.
- *Eliminating features:* Since date, time, and timestamp may lead to overfitting of the training set in certain machine learning methods, they were eliminated from feature vectors.

- *Normalization:* The dataset's maximum and minimum values vary for each feature. Normalizing all of the data in the range [0,1] increases the classifier's efficiency. The attribute values are converted to fall inside the range [0.1] using min-max normalization. The following equation provides the formula for min-max scaling [25, 26],

$$z = \frac{x - min(x)}{max(x) - min(x)} \quad (4)$$

where z, x, $max(x)$ and $min(x)$ are the normalization, presented maximum and maximum values, respectively.

- *Feature selection:* the BoT-IoT contains many features derived from network traffic, many of which may be irrelevant for the detection process. Hence, feature selection is an important process to enhance the accuracy of detection methods. XGBoost, an advanced implementation of gradient boosting, provides internal metrics that evaluate predictive performance. In applying XGBoost to the BoT-IoT dataset, the model is trained using all available features, and then feature importance scores are extracted—most effectively using the gain metric, which reflects how much each feature reduces error when it is used in a split during the construction of decision trees. These scores can be visualized through bar charts to identify the most impactful features easily. After ranking, a subset of top-ranked features can be selected to retrain the model, leading to reduced complexity, improved training speed, and often enhanced accuracy. This selection process also helps in better understanding which features are most indicative of attack behaviors in IoT traffic.

Table 1. Parameters settings

Parameter	Values
Epoch	100
Batch	32
Activation Function	Sigmoid
Optimizer	Adam
Loss Function	Binary cross-entropy
No of HL	2
Hidden size	60/30

C. Performance analyser

Performance measures are used to measure the capability of DDoS attacks. The accuracy, precision, recall, and F-measure are used, which are determined as follows,

- The accuracy is measured by the number of properly recognized examples and the total number of samples, which is defined as follows,

$$Accuracy = \frac{TP+TN}{TP+FP+TN+F} \quad (5)$$

- Precision is well-defined as the ratio of correctly considered samples to projected positive samples, which is defined as follows,

$$Precision = \frac{TP}{FP+TP} \quad (6)$$

- Recall is well-defined as the ratio of likely positives to the sum of genuine positives and false negatives, which is defined as follows,

$$Recall = \frac{TP}{TP+FN} \quad (7)$$

- F-measures calculate the harmonic mean of precision and recall, which is defined as follows,

$$F - Measures = \frac{2 \times Recall \times Precision}{Recall + Precision} \quad (8)$$

False positive (FP) means an incorrectly predicted sample. False negative (FN) indicates a wrongly projected sample. True positive (TP) specifies a positively predicted sample. True Negative (TN) specifies a properly identify samples.

D. Results analysis

The results evaluation of the detection method in IoT environments reveals significant patterns and enhancements associated with feature selection and activation functions. The models evaluated include AE, DAE, SAE, and VAE. FS contributed to a noticeable enhancement in detection performance, affirming its critical role in reducing dimensionality and enhancing relevant feature representation in high-dimensional IoT traffic data. Tables 2, 3, 4, and 5 and Figures 1,2,3, and 4 show the results analysis of different variants of AE based on different activation functions (Sigmoid, ReLU, Tanh) before and after feature selection. Across all models, applying FS improved accuracy for each activation. VAE with ReLU method achieved high accuracy (92%) after FS, indicating strong detection performance. VAE with ReLU activation achieved the highest accuracy (92%) after FS, indicating strong detection performance.

Table 2: Performance analysis based on accuracy

Methods	Before FS			After FS		
	Sigmoid	ReLU	Tanh	Sigmoid	ReLU	Tanh
AE	0.82	0.84	0.80	0.85	0.86	0.83
DAE	0.85	0.87	0.84	0.88	0.89	0.86
SAE	0.83	0.85	0.82	0.86	0.87	0.84
VAE	0.88	0.90	0.87	0.90	0.92	0.89

Table 3: Performance analysis based on precision

Methods	Before FS			After FS		
	Sigmoid	ReLU	Tanh	Sigmoid	ReLU	Tanh
AE	0.80	0.82	0.78	0.83	0.84	0.80
DAE	0.83	0.85	0.82	0.86	0.87	0.84
SAE	0.81	0.83	0.80	0.84	0.85	0.82
VAE	0.86	0.88	0.85	0.88	0.90	0.87

Table 4: Performance analysis based on recall

Methods	Before FS			After FS		
	Sigmoid	ReLU	Tanh	Sigmoid	ReLU	Tanh
AE	0.75	0.79	0.74	0.78	0.81	0.76
DAE	0.80	0.82	0.79	0.82	0.84	0.81
SAE	0.78	0.80	0.77	0.80	0.82	0.79
VAE	0.83	0.85	0.82	0.85	0.87	0.84

Table 5: Performance analysis based on F1-Score

Methods	Before FS			After FS		
	Sigmoid	ReLU	Tanh	Sigmoid	ReLU	Tanh
AE	0.77	0.80	0.75	0.80	0.82	0.78
DAE	0.81	0.83	0.80	0.84	0.85	0.82
SAE	0.79	0.81	0.78	0.82	0.83	0.80
VAE	0.84	0.86	0.83	0.86	0.88	0.85

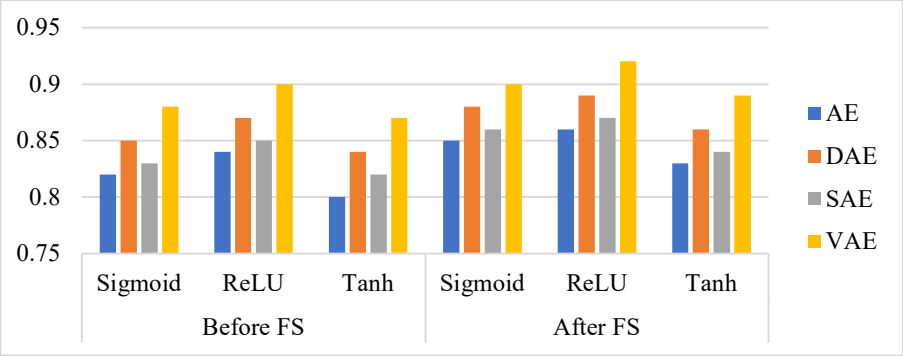

Figure 1 : Performance analysis based on accuracy

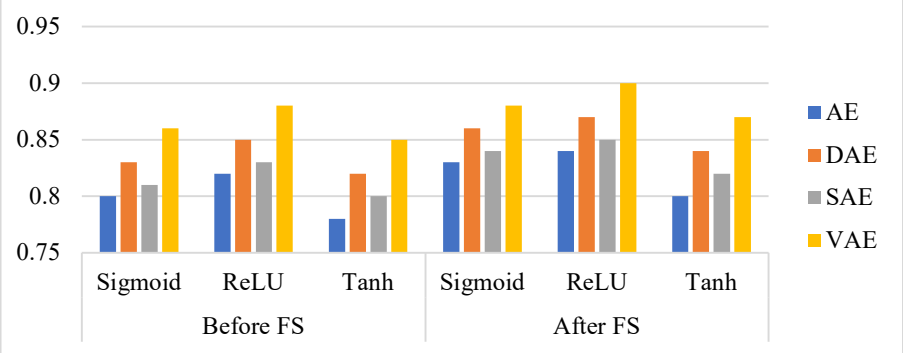

Figure 2 : Performance analysis based on precision

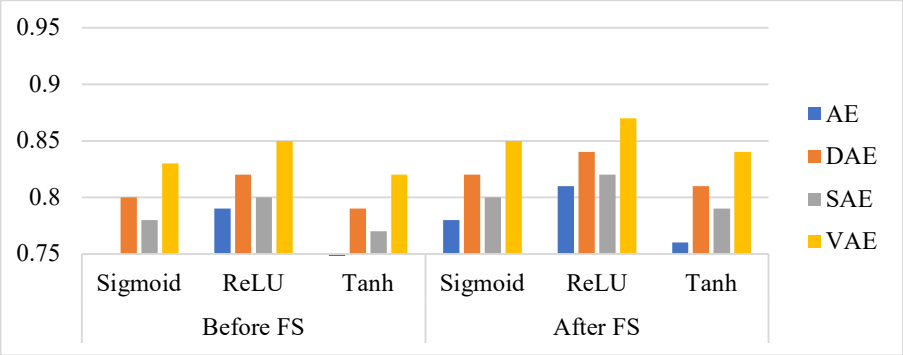

Figure 3 : Performance analysis based on recall

According to precision, the VAE with ReLU method achieved high precision values (90%) which is indicating superior prediction accuracy.

Similarly, the VAE with ReLU methods is produced the highest recall, which indicates strong sensitivity, and the highest F1 score, which reflects better overall balance between recall and precision. These findings highlight the combined effectiveness of feature selection and ReLU in optimizing autoencoder-based DDoS detection in IoT networks. The evaluation of the detection method in IoT demonstrated that the FS and activation functions significantly influence model performance. The tested models showed consistent improvement in detection accuracy after using FS, which helps to enhance detection accuracy. Results shown in Tables exposes that across all activation functions, better-quality correctness. In particular, the VAE with ReLU activation achieved higher generalization performance.

V. CONCLUSIONS

We investigated the performance of multiple AE variants such as AE, DAE, SAE, and VAE for detecting DDoS attacks in an IoT environment. We evaluated each model using three activation functions. The results highlight that VAE with ReLU activation constantly outperformed other methods. This method finding underscore the significance of VAE and activation functions. The present study confirms that the VAE and ReLU can significantly

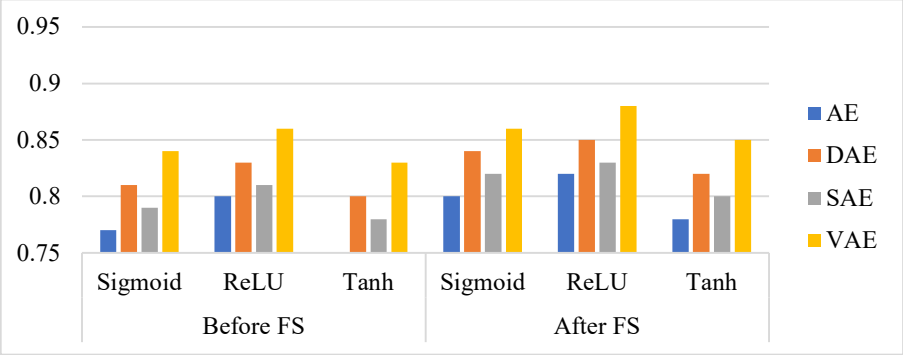

Figure 4 : Performance analysis based on f1-score

enhance detection capabilities, making it more feasible for deployment in real-time and resource-limited IoT networks. The hybridization of AE with other DL modes may capture both spatial and temporal features for improved detection.

The study was conducted in a controlled environment, which may not fully reflect real-world IoT environments. Additionally, the models mainly focused on spatial features, lacking the ability to capture temporal dependencies in traffic. This may affect their performance in detecting complex, evolving attacks over time. Future work can explore hybrid methods such as AE with LSTM or a transformer to capture both spatial and temporal features. Analysing the model on diverse, real-world datasets would enhance reliability, and optimizing for low-latency and low-power environments is crucial for real-time IoT deployments.

REFERENCES

[1] M. Lefoane, I. Ghafir, S. Kabir, and I.-U. Awan, "Internet of Things botnets: A survey on Artificial Intelligence based detection techniques," *Journal of Network and Computer Applications,* p. 104110, 2025.

[2] R. Kavitha, K. Saravanan, S. A. Jebakumari, and K. Velusamy, "Machine learning algorithms for IoT applications," in *Artificial Intelligence for Internet of Things*: CRC Press, 2022, pp. 185-214.

[3] R. Sardar *et al.*, "Challenges in detecting security threats in WoT: a systematic literature review," *Artificial Intelligence Review,* vol. 58, no. 7, p. 196, 2025.

[4] T. Al-Shurbaji *et al.*, "Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review," *IEEE Access,* 2025.

[5] B. Fathimamary, M. Nasreen, and K. Velusamy, "An Efficient DDoS Attack Detection Using Optimized Long Short-Term Optimization Based on Improved Brainstorm Optimization," *Indian Journal of Science and Technology,* vol. 19, no. 5, pp. 298-312, 2026.

[6] U. V. Menon *et al.*, "AI-Powered IoT: A Survey on Integrating Artificial Intelligence with IoT for Enhanced Security, Efficiency, and Smart Applications," *IEEE Access,* 2025.

[7] F. S. Alrayes, M. Zakariah, S. U. Amin, Z. I. Khan, and M. Helal, "Intrusion detection in IoT systems using denoising autoencoder," *IEEE Access,* 2024.

[8] A. L. Yaser, H. M. Mousa, and M. Hussein, "Improved DDoS detection utilizing deep neural networks and feedforward neural networks as autoencoder," *Future Internet,* vol. 14, no. 8, p. 240, 2022.

[9] M. K. Tanati and M. Ponnusamy, "Dense Capsule Stacked Auto-Encoder Model based DDoS Attack Detection and Hybrid Optimal Bandwidth Allocation with Routing in VANET Environment," *Vehicular Communications,* p. 100888, 2025.

[10] G. Sugitha, B. Preethi, and G. Kavitha, "Intrusion detection framework using stacked auto encoder based deep neural network in IOT network," *Concurrency and Computation: Practice and Experience,* vol. 34, no. 28, p. e7401, 2022.

[11] A. Basati and M. M. Faghih, "PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders," *Information Sciences,* vol. 598, pp. 57-74, 2022.

[12] R. Savithramma, C. Anitha, N. Sanjay Kumar, S. Kamble, and B. Ashwini, "Automatic attack detection in IOT environment using relational auto encoder with enhanced ANFIS," *International Journal of Information Technology,* vol. 16, no. 8, pp. 5307-5315, 2024.

[13] H. Wasswa, T. Lynar, and H. Abbass, "Enhancing iot-botnet detection using variational auto-encoder and cost-sensitive learning: A deep learning approach for imbalanced datasets," in *2023 IEEE Region 10 Symposium (TENSYMP)*, 2023: IEEE, pp. 1-6.

[14] A. Kalidindi and M. B. Arrama, "Botnet attack detection in IoT using hybrid optimisation enabled deep stacked autoencoder network," *International Journal of Bio-Inspired Computation,* vol. 22, no. 2, pp. 77-88, 2023.

[15] K. Saranya and A. Valarmathi, "A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms," *Scientific Reports,* vol. 15, no. 1, p. 10246, 2025.

[16] 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, p. 109984, 2025.

[17] M. T. Hussan, G. V. Reddy, P. Anitha, A. Kanagaraj, and P. Naresh, "DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization," *Cluster Computing,* vol. 27, no. 4, pp. 4469-4490, 2024.

[18] H. Rhachi, Y. Balboul, and A. Bouayad, "Enhanced Anomaly Detection in IoT Networks Using Deep Autoencoders with Feature Selection Techniques," *Sensors,* vol. 25, no. 10, p. 3150, 2025.

[19] A. Alqahtani, "Optimized deep autoencoder and bilstm for intrusion detection in iots-fog computing," *Multimedia Tools and Applications,* vol. 84, no. 8, pp. 4907-4943, 2025.

[20] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud," *Ieee Access,* vol. 8, pp. 181916-181929, 2020.

[21] X. Han, Y. Liu, Z. Zhang, X. Lü, and Y. Li, "Sparse auto-encoder combined with kernel for network attack detection," *Computer Communications,* vol. 173, pp. 14-20, 2021.

[22] A. Kandiero, P. Chiurunge, and J. Munodawafa, "Detection of DDoS attacks using variational autoencoder-based deep neural network," in *Privacy Preservation and Secured Data Storage in Cloud Computing*: IGI Global, 2023, pp. 365-404.

[23] E. M. Bårli, A. Yazidi, E. H. Viedma, and H. Haugerud, "DoS and DDoS mitigation using variational autoencoders," *Computer Networks,* vol. 199, p. 108399, 2021.

[24] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems,* vol. 100, pp. 779-796, 2019.

[25] K. Velusamy and R. Amalraj, "Cascade correlation neural network with deterministic weight modification for predicting stock market price," in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1110, no. 1: IOP Publishing, p. 012005.

[26] K. Velusamy and R. Amalraj, "Performance of the cascade correlation neural network for predicting the stock price," in *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2017: IEEE, pp. 1-6.