A hybrid framework for enhanced intrusion detection in cloud environments leveraging autoencoder

Abinaya Alagarsamy[1], Thenmozhi Elumalai[2], S. P. Ramesh[3], Tamilarasi Karuppiah[2], Prabu Kaliyaperumal[3], Rajakumar Perumal[3]
[1]Department of Artificial Intelligence and Machine Learning, St. Joseph's College of Engineering, Chennai, India
[2]Department of Information Technology, Panimalar Engineering College, Chennai, India
[3]School of Computer Science and Engineering, Galgotias University, Delhi NCR, India

Article Info

Article history:

Received Oct 4, 2024
Revised Nov 19, 2024
Accepted Dec 15, 2024

Keywords:

Cloud security
DBSCAN
Network security
Particle swarm optimization
Principal component analysis
Unsupervised learning

ABSTRACT

In today's world, the significance of network security and cloud environments has grown. The rising demand for data transmission, along with the versatility of cloud-based solutions and widespread availability of global resources, are key drivers of this growth. In response to rapidly evolving threats and malicious attacks, developing a robust intrusion detection system (IDS) is essential. This study addresses the imbalanced data and utilizes an unsupervised learning approach to protect network data. The suggested hybrid framework employs the CIC-IDS2017 dataset, integrating methods for handling imbalanced data with unsupervised learning to enhance security. Following preprocessing, principal component analysis (PCA) reduces the dimensionality from eighty features to twenty-three features. The extracted features are input into density-based spatial clustering of applications with noise (DBSCAN), a clustering algorithm. particle swarm optimization (PSO) optimizes DBSCAN, grouping similar traffic and enhancing classification. To address the imbalances in the learning process, the autoencoder (AE) algorithm demonstrates unsupervised learning. The data from the cluster is input into the AE, a deep learning algorithm, which classifies traffic as normal or an attack. The proposed approach (PCA+DBSCAN+AE) attains remarkable intrusion detection accuracy exceeding 98%, and outperforms five contemporary methodologies.

Corresponding Author:

Prabu Kaliyaperumal
School of Computer Science and Engineering, Galgotias University
Delhi NCR, India
Email: mega.prabu@gmail.com

1. INTRODUCTION

The information and the servers tasked with storing and disseminating it across widespread networks are invaluable resources. They possess the capability to offer crucial information, analytical perspectives, and predictive forecasts promptly [1]. These elements are essential unlocking the capabilities of interconnected systems for diverse objectives [2]. This essential framework requires careful safeguarding to avert any negative repercussions that might affect society on a broad scale. In the realm of cyber security, it is essential to recognize that digital traffic frequently travels significant distances in the real world [3]. This methodology is frequently utilized within cloud technologies too. AWS (Amazon web services), GCP (Google Cloud platform), MSA (Microsoft Azure), and other service providers enable rapid global expansion in mere minutes via their distributed content delivery network (CDN) capabilities.

By leveraging the CDN, contents are effectively distributed via local edge nodes [4], like CloudFront for AWS, resulting in faster delivery. The prolonged transfer of data across cloud platforms, spanning vast distances, depends heavily on expanded network capabilities, thereby heightening its vulnerability to potential network breaches [5]. This increased susceptibility stems from the decentralized structure and extensive coverage of the network.

Intrusion detection system (IDS) are pivotal in protecting cloud infrastructures from cyber threats and attacks, ensuring their security. Within the domain of cloud computing, as extensive data storage and processing occur across decentralized infrastructures, the vulnerability to cyber-attacks is amplified [6]. An IDS observes both network and system operations, detecting and taking action against any abnormal activities that might indicate a security risk. The dynamic and scalable nature of cloud infrastructure presents distinct hurdles for intrusion detection, given that attacks can materialize in diverse forms. The dynamic and scalable characteristics of cloud infrastructure present distinctive hurdles for intrusion detection. This is because attacks can take on diverse forms, such as distributed denial of service (DDoS), malware injections and unauthorized attempts. In the cloud environment, IDS relies on machine learning methods and sophisticated algorithms to examine large-scale datasets and detect anomalies that indicate harmful behavior [7]. Ensuring prompt and precise intrusion detection is vital for safeguarding the CIA triad confidentiality, integrity, and availability of data stored and handled in cloud environments. This significantly enhances the comprehensive security of cloud computing systems. The components illustrated in Figure 1, which constitute the IDS, collaborate synergistically to assist organizations in identifying and mitigating security incidents. This serves to strengthen their comprehensive cybersecurity position. Misuse-based IDS, relies on established standards for typical host or network behavior. The potential intrusions are identified as deviations from these predefined standards. A signature-based IDS, also referred to as a rule-based IDS, operates by using a database of known threat signatures or behavior patterns. This rule-based IDS analyzes system activities and network traffic by comparing them to known threat signatures. The majority of research efforts focus on hybrid approaches that integrate these methodologies.

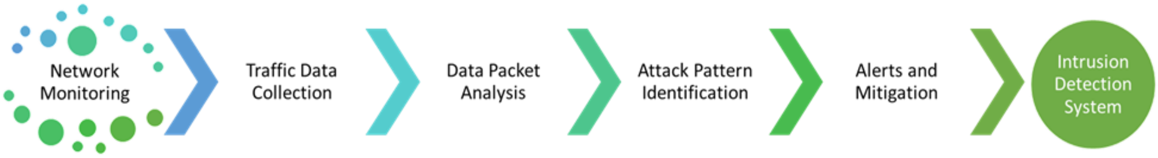


Figure 1. Key components of IDS

A denial-of-service (DoS) attack is an intentional and harmful attempt to obstruct or block authorized users from accessing a system, service, or network. During a DoS attack, an assailant inundates the intended system with a barrage of resource requests, resulting in slow performance, unresponsiveness, or potential complete unavailability [8]. The objective of a DoS is not to compromise the integrity of the system; instead, it seeks to hinder its performance and interrupt regular functionalities. DoS attacks may be executed through different techniques, such as inundating the target with traffic, taking advantage of system weaknesses, or excessively utilizing its resources [9]. Effective mitigation and prevention of DoS attacks necessitate strong security protocols, such as implementing data flow regulation, managing resources efficiently, and deploying advanced threat detection and response solutions.

DDoS attacks stand out as a more advanced and formidable cyber threat when compared to the conventional DoS attacks. During a DDoS attack, numerous infected devices, typically organized into a botnet, are coordinated to inundate a specific network or infrastructure with a substantial volume of traffic [10]. The aim is to overload the target's resources, leading to interference and making services unavailable to legitimate users. Effectively combating DDoS attacks requires a thorough defense strategy [11], which includes packet inspection and traffic management. Additionally, employing dedicated DDoS defense solutions is essential for detecting and neutralizing harmful network traffic efficiently.

Within the scope of intrusion detection, contemporary machine learning and deep learning methods, recognized for their efficacy in information security [12], encompass a variety of tools. The DBN employs multiple hidden layers to capture complex data structures [13], whereas deep neural networks (DNN) excel in learning complex features [14]. The whale optimization algorithm (WOA) is based on the behaviors exhibited by humpback whales [15]. Support vector machines (SVM), adept at distinguishing categories in high-dimensions, make significant contributions to identifying security threats [16]. Furthermore, principal component analysis (PCA) and DBSCAN help reduce dataset complexity, facilitating effective analysis and accurate threat identification [17]. Optimization techniques like PSO enhance clustering methods to achieve better results. Moreover, deep learning models such as AE significantly contribute to enhancing cybersecurity defenses by accurately recognizing attack patterns through learned representations, thus bolstering protection against emerging threats.

Andresini *et al.* [18] presented a deep learning framework with a multi-channel approach for intrusion detection, which seamlessly integrates both supervised and unsupervised learning techniques. They employed AEs for feature extraction, with convolutional neural networks (CNN) analyzing patterns across multiple channels to differentiate malicious traffic from normal traffic. However, the approach lacks comprehensive details about the attacks and necessitates further exploration in the area of explainable artificial intelligence (XAI). Almaiah *et al.* [16] investigated IDS that utilized PCA was used for dimensionality reduction, and the classifier employed was a support vector machine (SVM) with different kernel functions. The research employed the UNSW-NB15 and KDD CUP'99 datasets, resulting in an accuracy rate of 93.93%. Oliveira *et al.* [19] utilized the CIDDS-001 dataset and applied long short-term memory (LSTM) and CNN architectures to create a precise model for detecting attack traffic in a sequential manner. The research highlights LSTM's remarkable ability to identify sequential data trends, achieving an impressive accuracy rate of 99.96%.

Kunang *et al.* [20] introduced a technique for detecting intrusions that utilizes deep learning in conjunction with hyper-parameter optimization. This research integrates a deep AE and a DNN with an automated approach for hyperparameter optimization. By utilizing grid and random search techniques, the approach identifies the best hyperparameter settings to improve detection effectiveness. The study assesses three methods for feature extraction during the initial training phase, with the deep AE method demonstrating the most favorable outcomes. Suganya and Sasipraba [21] introduced a three-phase framework consisting of attack detection, authentication, and user registration, implemented using the Enron dataset. The performance evaluation incorporates seven criteria: recall (96.54%), accuracy (95.16%), precision (95.25%) and F1-score (93.76%), along with metrics for root mean square error (RMSE), encryption time and decryption time. Moore and Frye [22], a robust method for detecting attacks within the internet of medical things (IoMT) is introduced, incorporating security and privacy safeguards via deep belief networks (DBN). Given the paramount importance of privacy and security in internet of things (IoT), establishing a reliable detection system is imperative. The research proposes the utilization of a DBN for detecting the intrusions, with the CICIDS dataset evaluated to demonstrate its superior accuracy. Thilagam and Aruna [23] presented a method that comprising techniques for data balancing and preprocessing. The classification of benign and malicious attacks is evaluated on the NSL-KDD dataset using a hybrid LSTM. Their approach achieved 94.98% accuracy by integrating the lion mutated genetic algorithm (LM-GA) with a combination of CNN and LSTM.

A considerable amount of data and critical information has transitioned to cloud environments, offering a chance to bolster overall security measures [24]. In the domain of network security, attacks based on routing are commonplace incidents. Nonetheless, the bulk of existing research is tailored towards detecting these attacks using imbalanced learning data. The outcome hinges on the dataset; if it's imbalanced, the findings may not reliably reflect the actual situation. Hence, the current focus is on fortifying defensive mechanisms, particularly by addressing the challenge of imbalanced data through targeted strategies against routing-based attacks.

This method inherently integrates a mechanism for detecting intrusions, aimed at improving the overall security of the network. In addressing network-based attacks in cloud environments, a wide range of events can be observed in today's cloud ecosystem [25]. Notably, among thirty-seven attacks in the cloud environment, twenty-six are classified as network-based. Focusing on these twenty-six attacks, particularly those related to routing [21], The research will prioritize the major types of attacks, specifically DoS and DDoS. This choice is driven by insights from the cloud network dataset, known as CIC-IDS2017 [26]. This research employs a focused methodology that leverages algorithms to bolster security, with a specific focus on enhancing intrusion detection within the cloud environment.

The proposed method involves a combined approach based on deep learning concepts. The raw data, which represents network traffic, is processed and then used as input for clustering to group similar traffic. The similarly grouped traffic is then input into a deep learning algorithm trained on imbalanced data to accurately classify attacks. In the end, the efficacy of the classified attacks will be evaluated using refined metrics, including accuracy, recall, precision, F-measure, and mean squared error (MSE).

2. RESEARCH METHOD

The hybrid model illustrated in Figure 2 combines several techniques: PCA, DBSCAN, PSO, and AE are used for dimensionality reduction, clustering, optimization, and attack classification, respectively. By concentrating on packet data associated with the attack cluster, the model leverages the CIC-IDS2017 dataset [26]. The study prioritizes DoS, and DDoS attacks, which comprise the majority of the observed attacks in the dataset. The raw data was initially preprocessed and normalized to facilitate efficient analysis. The dataset, comprising 83 features, presents a difficulty for clustering algorithms because of its complex feature space. The proposed hybrid model, PCA+DBSCAN+AE, addresses the challenge of high dimensionality by taking into account all data attributes. Even though AE achieves high accuracy, it can result in longer processing times when used in a cloud environment. In high-demand cloud environments, swift attack detection and accurate classification are essential. The DBSCAN technique accelerates the detection of attacks, enabling the AE to focus solely on classifying the traffic data that has been attacked. This method decreases the number of input rows, resulting in faster classification with improved accuracy.

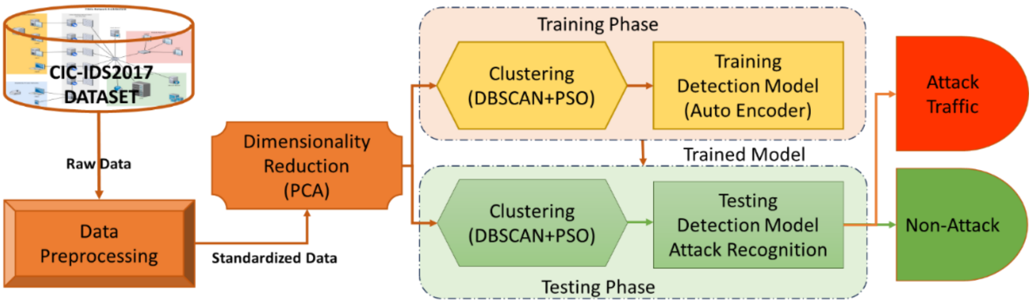


Figure 2. Operational architecture of proposed system

2.1. Data pre-processing

Data preparation has been implemented in three essential stages: pre-processing of data, normalization of features, and reducing dimensionality. Data preparation is crucial because unprocessed data frequently contains varying sets of values with different ranges and incomplete information, requiring proper data management. To address the issue of missing values, the missing data is represented by zero values, creating a complete dataset. The dataset exhibits value fluctuations across various fields, with unique ranges for each, thereby increasing complexity. To bring uniformity to these intervals, a normalization technique is implemented modifying the values according to its initial distribution. In this context, scaling adjusts the data to a range spanning from -1 to 1. The standardized data are considered as input for the PCA dimensionality reduction stage, facilitating further analysis and insights.

2.2. Dimensionality reduction

In the dimensionality reduction stage, PCA is leveraged to select principal components as the reduced dimensions. Dimensionality reduction involves employing two distinct methods: (i) eliminating features with less weightage, (ii) condensing all features into a smaller subset. This research selects the second method, employing PCA with standard deviation and mean, eigenvalue and covariance. In the end, twenty-three reduced feature space are produced, as illustrated in the scree plot in Figure 3, meeting a threshold of 92% for subsequent procedures.

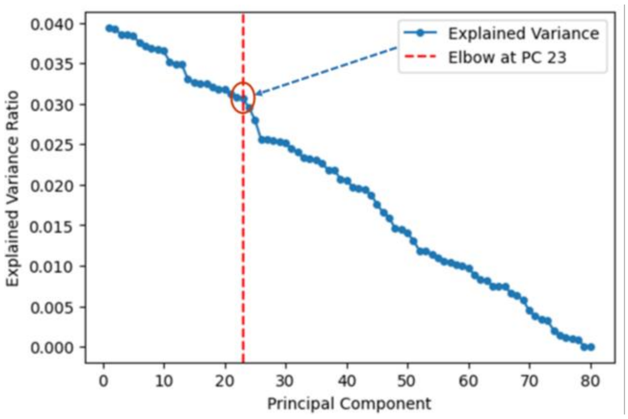


Figure 3. Selection of principal components in scree plot

2.3. Cluster formation

The reduced feature space processed through DBSCAN to form clusters by analyzing packet feature density, thereby grouping together features with similar characteristics. This research article proposes a method that utilizes varying proportions 70% and 80% for training to illustrate how the cluster assimilates information from the dataset. Upon inserting the initial packet, it gets allocated to a group, which is then optimized using PSO. PSO optimizes DBSCAN's pivotal parameters, Epsilon and MinPts, which impact both cluster shape and density. PSO optimizes feature weights for dataset parameters by treating them as particles and utilizing a specified fitness function.

2.4. Attack classification

The clustered data points are taken as input to the AE, which functions as a deep learning classifier and has been reduced in dimensionality. Crucially, the AE is trained solely on benign data in order to address the challenge of imbalanced learning. The aim of this novel training method is to surmount the difficulties inherent in imbalanced datasets. This approach ensures the model's capability to effectively classify both benign traffic and attack traffic instances. The AE excels in a reduced feature space, yielding precise results, particularly in clustered scenarios. The AE is adept at classifying attack packet data, employing backpropagation in its training process to learn patterns from the given dataset. During the training process, information from the decoder is utilized in forward propagation, emulating the functions of the encoder. As a result, the AE algorithm reduces the mean squared error, subsequently classifying the output as attack traffic.

3. RESULTS AND DISCUSSION

The execution environment for this research utilizes "Google Colab with Python version 3.0", incorporating the proposed algorithm PCA+DBSCAN+AE implemented on the cloud environment. The implementation is carried out across different configuration settings, specifically using learning-evaluation ratios of 70:30 and 80:20. In Figure 3, the scree plot illustrates the reduction of high dimensionality to a twenty-three-feature space, as indicated by the elbow curve. Four positive evaluation metrics, as shown in (1) to (4), are used to compare the existing methods with the proposed method for both learning-evaluation ratios. Among the existing methodologies, five were examined as shown in Table 1, with each comparison incorporating the proposed approach. This research experiment concentrates on two major attack types, DoS and DDoS, with 48 statistical analyses. A grand total of 96 comparisons were analyzed, encompassing 2 test cases, 4 metrics, 6 methods, and 2 attacks.

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \tag{1}$$

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \tag{2}$$

$$F - Measure = \frac{2 * (Precision * Recall)}{Precision + Recall} \tag{3}$$

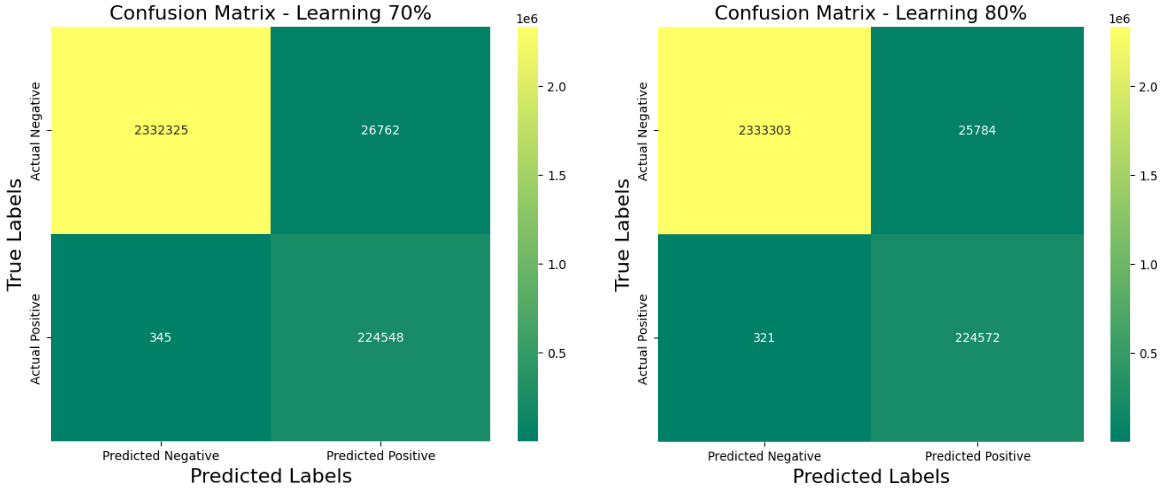
$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \tag{4}$$

Table 1. Results of the experiments for a learning rate of 70%

Approaches	Learning data-70%: testing data-30%			
	Precision	Recall	F1-score	Accuracy
SVM [16]	0.8281	0.8302	0.8391	0.8292
LSTM [27]	0.8566	0.8505	0.8534	0.8558
DNN [14]	0.8335	0.8202	0.8266	0.8304
DBN [13]	0.8735	0.8607	0.8665	0.8729
DBN+WOA [15]	0.8862	0.8787	0.8822	0.8985
Proposed model	0.8935	0.9984	0.9430	0.9895

Figure 4 depict the detected instances of intrusion in the CIC-IDS2017 network-based dataset within the cloud for the two learning test cases. These figures visually represent the confusion matrices for each test case with learning proportions of 70:30 and 80:20. Observing Figures 4(a) and 4(b), it becomes apparent that training with benign data on a larger dataset significantly reduces the false positive and false negative rates compared to conventional imbalanced learning. This underscores the benefits of utilizing a considerable amount of benign data for learning purposes.

The proposed method assesses detection accuracy using mean square error (MSE). Figure 5 showcases the testing accuracy across both learning sets, highlighting the efficacy of the proposed hybrid model. The models built using ‘benign traffic’ and ‘attack traffic’ data from CIC-IDS2017 demonstrate significant performance. The AE model consistently delivers superior results, as evident in both learning scenarios.



(a) (b)

Figure 4. Confusion matrix for the proposed hybrid model (a) learning proportion at 70% and (b) learning proportion at 80%

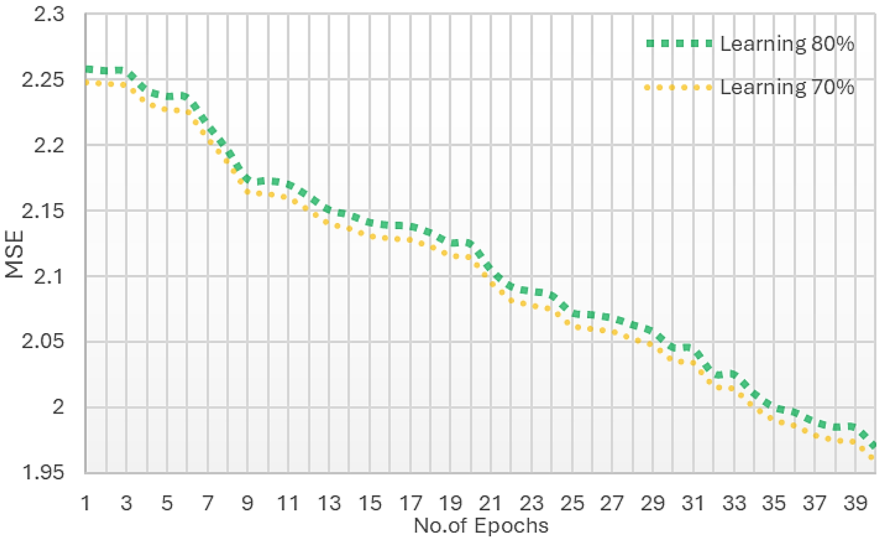


Figure 5. Loss function of the detection model

The findings from the experiments, detailed in Tables 1 and 2, present various metrics across different learning proportions. Figure 6 compares and illustrates the accuracy of existing methods with the proposed method. The learning percentages of the two test cases, 70% and 80%, presented in Tables 1 and 2, demonstrate the superior performance of the proposed hybrid model in intrusion detection compared to existing models. Boasting a precision of 0.8935 and 0.8970, a recall of 0.9984 and 0.9985, an F1-score of 0.9430 and 0.9451, and notable accuracy levels of 0.9895 and 0.9898, the proposed hybrid model demonstrates exceptional performance across both training scenarios, excelling when trained on benign data. The outcomes underscore its effectiveness in addressing the challenges posed by imbalanced data.

Table 2. Results of the experiments for a learning rate of 80%

Approaches	Learning data-80%: testing data-20%			
	Precision	Recall	F1-score	Accuracy
SVM [16]	0.8426	0.8485	0.8553	0.8455
LSTM [27]	0.8641	0.8579	0.8609	0.8780
DNN [14]	0.8412	0.8237	0.8322	0.8335
DBN [13]	0.8837	0.8617	0.8724	0.8940
DBN+WOA [15]	0.8945	0.8943	0.8992	0.9112
Proposed model	0.8970	0.9985	0.9451	0.9898

Especially evident in Figure 6, the proposed hybrid approach achieves an accuracy of 98.96%, outperforming benchmarked techniques such as SVM by 15.23%, LSTM by 12.27%, DNN by 15.77%, DBN by 10.62%, and DBN+WOA by 8.48%. These findings underscore the advantages of the proposed hybrid model, demonstrating its superiority compared to current leading methods. The findings of the study underscore the effectiveness of the proposed hybrid model for intrusion detection and highlight the importance of utilizing a more extensive training dataset containing entirely benign traffic data within the autoencoder framework. These insights are pivotal for the progression of cybersecurity. These findings can be leveraged by researchers to create IDSs that are more effective, tackling imbalanced data hurdles and enhancing network security on the whole. The superior accuracy demonstrated by the proposed hybrid approach establishes a benchmark for advanced solutions in combating cybersecurity challenges in the realm of intrusion detection. Additionally, future research could investigate multiclass classification techniques to address a wider range of attack patterns, thereby enhancing the overall defense framework.

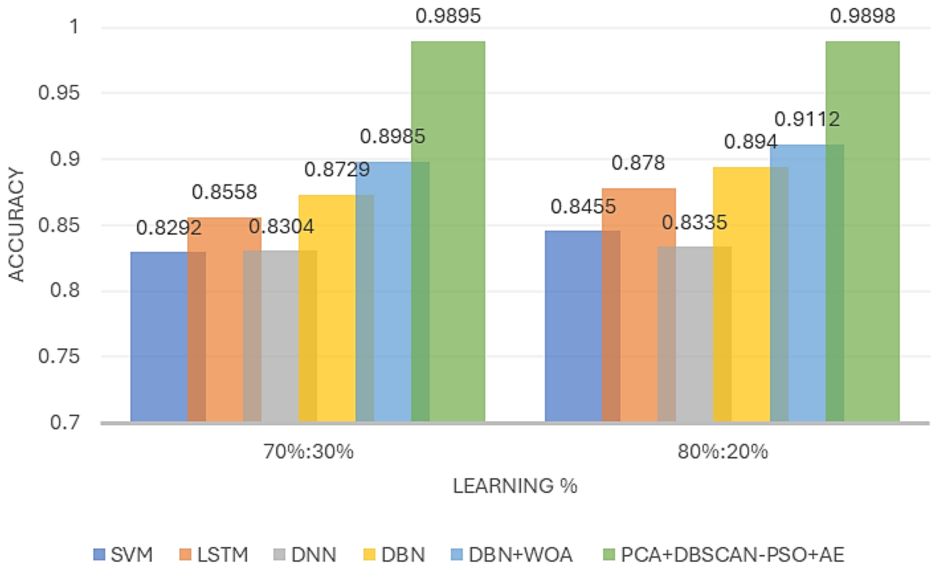


Figure 6. Performance comparison of the proposed hybrid model

4. CONCLUSION

The proposed hybrid method begins by processing the network traffic data from the CIC-IDS2017 intrusion dataset, starting with data preprocessing steps such as standardization. Following this, the data's complexity is mitigated through dimensionality reduction techniques. The reduced-dimensional data is subsequently fed into the clustering stage, employing DBSCAN with PSO. This process leads to the classification of data into attack instances and benign instances. The detection module processes the grouped data extracted from the clusters, employing the autoencoder, a neural network model, to ensure precise attack classification. This method accurately distinguishes between benign instances and attacks. The proposed hybrid method, labeled as PCA+DBSCAN+AE, exhibits remarkable performance across key metrics, achieving a precision above 89%, a recall above 99%, an F1-score above 94%, and an accuracy above 98%. This exceptional accomplishment surpasses existing techniques, solidifying the proposed method's excellence, with accuracy exceeding 98% in detecting attacks on the CIC-IDS2017 intrusion dataset. This research work highlights the effectiveness of the proposed hybrid intrusion detection approach, emphasizing the importance of using a more extensive training dataset with benign data to improve the autoencoder's performance. Essential for the progression of cybersecurity, it steers the advancement of effective IDSs by improving overall performance, addressing imbalanced data issues, and utilizing unsupervised learning to enhance network security resilience.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Abinaya Alagarsamy	✓			✓		✓		✓		✓			✓	
Thenmozhi Elumalai		✓		✓	✓				✓		✓	✓		
S. P. Ramesh		✓	✓		✓				✓		✓		✓	
Tamilarasi Karuppiah		✓		✓		✓				✓		✓		
Prabu Kaliyaperuma	✓				✓		✓		✓		✓		✓	
Rajakumar Perumal	✓		✓		✓		✓			✓	✓			

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

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [P.K], upon reasonable request.

REFERENCES

[1] H. Attou *et al.*, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing," *Applied Sciences*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[2] D. Srilatha and N. Thillaiarasu, "Implementation of intrusion detection and prevention with deep learning in cloud computing," *Journal of Information Technology Management*, vol. 15, pp. 1–18, 2023, doi: 10.22059/jitm.2022.89407.

[3] A. R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," *Journal of Cloud Computing*, vol. 12, no. 1, Dec. 2023, doi: 10.1186/s13677-023-00491-x.

[4] H. Sadia *et al.*, "Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach," *IEEE Access*, vol. 12, pp. 52565–52582, 2024, doi: 10.1109/ACCESS.2024.3380014..

[5] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311–320, Sep. 2023, doi: 10.26599/BDMA.2022.9020038.

[6] U. Ahmed *et al.*, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Sci Rep*, vol. 15, no. 1, p. 1726, 2025, doi: 10.1038/s41598-025-85866-7.

[7] J. R. Beulah, C. P. D. Cyril, S. Geetha, and D. S. Irene, "Towards improved detection of intrusions with Constraint-Based Clustering (CBC)," *International Journal of Computer Networks and Applications*, vol. 8, no. 1, pp. 28–43, Feb. 2021, doi: 10.22247/IJCNA/2021/207980.

[8] R. Alshamy and M. A. Akcayol, "Intrusion detection model using machine learning algorithms on NSL-KDD dataset," *International Journal of Computer Networks and Communications*, vol. 16, no. 6, pp. 75–88, Nov. 2024, doi: 10.5121/ijcnc.2024.16605.

[9] A. Almotairi, S. Atawneh, O. A. Khashan, and N. M. Khafajah, "Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models," *Systems Science & Control Engineering*, vol. 12, no. 1, p. 2321381, Dec. 2024, doi: 10.1080/21642583.2024.2321381.

[10] S. Sureshkumar, G. K. D. P. Venkatesan, and R. Santhosh, "Detection of DDOS attacks on cloud computing environment using altered convolutional deep belief networks," *International Journal of Computer Network and Information Security*, vol. 15, no. 5, pp. 63–72, Oct. 2023, doi: 10.5815/ijcnis.2023.05.06.

[11] E. Benmohamed, A. Thaljaoui, S. El Khediri, S. Aladhadh, and M. Alohali, "DDoS Attacks Detection with Half Autoencoder-Stacked Deep Neural Network," *Int J Coop Inf Syst*, vol. 33, no. 03, p. 2350025, 2024, doi: 10.1142/S0218843023500259.

[12] R. Harwahyu, F. H. E. Ndolu, and M. V. Overbeek, “Three layer hybrid learning to improve intrusion detection system performance,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 2, pp. 1691–1699, Apr. 2024, doi: 10.11591/ijece.v14i2.pp1691-1699.

[13] O. Belarbi, A. Khan, P. Carnelli, and T. Spyridopoulos, “An intrusion detection system based on deep belief networks,” in *International Conference on Science of Cyber Security*, 2022, pp. 377–392, doi: 10.1007/978-3-031-17551-0_25.

[14] S. D. Alotaibi *et al.*, “Deep Neural Network-Based Intrusion Detection System through PCA,” *Math Probl Eng*, vol. 2022, no. 1, p. 6488571, 2022, doi: https://doi.org/10.1155/2022/6488571.

[15] C. Edwin Singh and S. Maria Celestin Vigila, “WOA-DNN for intelligent intrusion detection and classification in MANET services,” *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 1737–1751, 2023, doi: 10.32604/iasc.2023.028022.

[16] M. A. Almaiah *et al.*, “Performance investigation of principal component analysis for intrusion detection system using different support vector machine Kernels,” *Electronics*, vol. 11, no. 21, p. 3571, Nov. 2022, doi: 10.3390/electronics11213571.

[17] H. Harintaka and C. Wijaya, “Automatic point cloud segmentation using RANSAC and DBSCAN algorithm for indoor model,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 6, pp. 1317–1325, Dec. 2023, doi: 10.12928/telkomnika.v21i6.25299.

[18] G. Andresini, A. Appice, N. Di Mauro, C. Loglisci, and D. Malerba, “Multi-channel deep feature learning for intrusion detection,” *IEEE Access*, vol. 8, pp. 53346–53359, 2020, doi: 10.1109/ACCESS.2020.2980937.

[19] N. Oliveira, I. Praça, E. Maia, and O. Sousa, “Intelligent cyber attack detection and classification for network-based intrusion detection systems,” *Applied Sciences*, vol. 11, no. 4, p. 1674, Feb. 2021, doi: 10.3390/app11041674.

[20] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, “Attack classification of an intrusion detection system using deep learning and hyperparameter optimization,” *Journal of Information Security and Applications*, vol. 58, p. 102804, May 2021, doi: 10.1016/j.jisa.2021.102804.

[21] M. Suganya and T. Sasipraba, “Stochastic gradient descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment,” *Journal of Cloud Computing*, vol. 12, no. 1, p. 74, May 2023, doi: 10.1186/s13677-023-00442-6.

[22] W. Moore and S. Frye, “Review of HIPAA, Part 1: history, protected health information, and privacy and security rules,” *Journal of Nuclear Medicine Technology*, vol. 47, no. 4, pp. 269–272, Dec. 2019, doi: 10.2967/jnmt.119.227819.

[23] T. Thilagam and R. Aruna, “Intrusion detection for network based cloud computing by custom RC-NN and optimization,” *ICT Express*, vol. 7, no. 4, pp. 512–520, Dec. 2021, doi: 10.1016/j.icte.2021.04.006.

[24] S. R. Bharamagoudar and S. V. Saboji, “Location-aware hybrid microscopic routing scheme for mobile opportunistic network,” *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 12, no. 2, pp. 785–793, Jun. 2023, doi: 10.11591/ijai.v12.i2.pp785-793.

[25] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, “Cloud-based intrusion detection approach using machine learning techniques,” *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311–320, Sep. 2023, doi: 10.26599/BDMA.2022.9020038.

[26] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116, doi: 10.5220/0006639801080116.

[27] S. Karthic, S. M. Kumar, and P. N. S. Prakash, “Grey wolf based feature reduction for intrusion detection in WSN using LSTM,” *International Journal of Information Technology*, vol. 14, no. 7, pp. 3719–3724, Dec. 2022, doi: 10.1007/s41870-022-01015-7.

BIOGRAPHIES OF AUTHORS

Abinaya Alagarsamy assistant professor, Department of Artificial Intelligence and Machine Learning, St. Joseph’s College of Engineering. She holds an M.E in CSE from Anna University. She has published 2 patents and 8 research papers in international journals and conferences. Her expertise includes machine learning, cyber security, networks, and cloud computing. She can be contacted at email: abinayaalagar1992@gmail.com.

Dr. Thenmozhi Elumalai is a professor in the Department of Information Technology at Panimalar Engineering College. With 22 years of teaching experience, she holds a Ph.D. and has authored 7 patents, 8 book chapters, and 19 research papers in renowned international journals and conferences. Her areas of expertise include cyber security, networks and machine learning. She can be contacted at email: ethenmozhi22.pec@gmail.com.

S. P. Ramesh assistant professor in School of Computer Science and Engineering at Galgotias University, holds 15 years of teaching experience and also worked one year in Indian Institute of Information Technology (IIIT). With an M.E CSE from Anna University, he has published 8 patents and 7 research papers, specializing in artificial intelligence, machine learning, internet of things, wireless sensor networks, network security, cryptography and security, cyber security. He can be contacted at email: spramesh.me@gmail.com.

Dr. Tamilarasi Karuppiah associate professor in Department of Information Technology at Panimalar Engineering College, accumulating 24 years of teaching experience. She earned her Ph.D. record with 7 patents, 5 book chapters, and 19 research papers published in esteemed international journals and conferences. Her expertise spans cyber security, networks, cloud computing, and machine learning. She can be contacted at email: thamizhanna@gmail.com.

Prabu Kaliyaperumal assistant professor in School of Computer Science and Engineering at Galgotias University, has 16 years of teaching experience. Currently pursuing a Ph.D., he holds an M.Tech. in CSE from SRM University and MBA from Anna University. He has published 4 patents and 11 research papers in international journals and conferences. His expertise includes cyber security, networks, cloud computing, and machine learning. He can be contacted at email: mega.prabu@gmail.com.

Rajakumar Perumal assistant professor in School of Computer Science and Engineering at Galgotias University, holds 22 years of teaching experience and is pursuing a Ph.D. in computer science and engineering at Shri Venkateshwara University. With an M.E CSE from Anna University, he has published 4 patents and 8 research papers, specializing in networks, cloud computing, software engineering, and machine learning. He can be contacted at email: rajkumar.jcet@gmail.com.