

A hybrid deep learning approach for enhanced network intrusion detection

K. Prabu, P. Sudhakar

School of Computing Science and Engineering, Galgotias University, Greater Noida, India

Article Info

Article history:

Received Dec 20, 2023

Revised Jan 8, 2024

Accepted Jan 14, 2024

Keywords:

AutoEncoder

Cloud security

DBSCAN

Network security

Particle swarm optimization

Principal component analysis

Unsupervised learning

ABSTRACT

The contemporary era places paramount importance on network security and cloud environments, driven by increased data transmission demands, the flexibility of cloud services, and the prevalence of global resources. Addressing the escalating threat of computer malware, the development of efficient intrusion detection systems (IDS) is imperative. This research focuses on the challenges posed by imbalanced datasets and the necessity for unsupervised learning to enhance network security. The proposed hybrid deep learning method utilizes raw data from the CSE-CIC-IDS-2018 dataset, integrating imbalanced and unsupervised learning techniques. After preprocessing and normalization, feature extraction through principal component analysis (PCA) reduces dimensionality from seventy-eight fields to ten essential features. Clustering, employing the density-based spatial clustering of applications with noise (DBSCAN) algorithm optimized with particle swarm optimization (PSO), is applied to the extracted features, distinguishing between attack and non-attack packets. Addressing dataset imbalances, imbalanced learning techniques are employed, and unsupervised learning is exemplified through the AutoEncoder (AE) algorithm. The attack cluster's data is input into AE, a deep learning-based approach, yielding outputs for attack classification. The proposed technique (PCA+DBSCAN-PSO+AE) achieves an impressive 99.19% accuracy in intrusion detection, surpassing contemporary methodologies and five existing techniques. This research not only enhances accuracy but also addresses imbalanced learning challenges, utilizing the power of unsupervised learning for robust network security.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

K. Prabu

School of Computing Science and Engineering, Galgotias University

Greater Noida, Uttar Pradesh, India

Email: k.prabu@galgotiasuniversity.edu.in

1. INTRODUCTION

The data and the servers responsible for storing and delivering that data across distributed and expansive networks are paramount assets. They have the capacity to provide valuable information, analytical insights, and future predictions in a timely manner [1], [2]. These components play a crucial role in leveraging the potential of networked systems for various purposes [3]. This critical infrastructure demands meticulous protection to prevent any adverse consequences that could potentially impact society at large. When considering network security, it's crucial to acknowledge that real-world data is often transmitted across long distances [4], [5]. This approach is commonly employed in cloud technologies as well. Service providers like Google cloud platform (GCP), Azure, Amazon web services (AWS), and others facilitate global expansion within minutes through their decentralized content delivery network (CDN) capabilities.

Utilizing the CDN, content is delivered more rapidly through local distribution edge points [5], such as CloudFront in the case of AWS. The extended journey of data over the cloud, covering long distances, relies on increased network resources, making it more susceptible to potential network attacks. This heightened exposure is a consequence of the distributed nature and expansive reach of the network.

Almaiah *et al.* [6] explored intrusion detection systems (IDS) employing principal component analysis (PCA) for feature reduction and support vector machine (SVM) classifiers with diverse kernels. The study utilized KDD CUP'99 and UNSW-NB15 datasets, achieving a reported accuracy of 93.94%. In their research, Oliveira *et al.* [7] employed convolutional neural network (CNN) and long-short term memory (LSTM) on the CIDDs-001 dataset to construct an accurate model for malicious classification from a sequential perspective. The study highlights the superior accuracy of LSTM in capturing sequential information patterns, achieving an impressive 99.96% classification accuracy. Andresini *et al.* [8] introduced MINDFUL, a multi-channel deep learning approach for intrusion detection, combining supervised and unsupervised methods. They applied CNN and AutoEncoder (AE) for feature extraction, seeking patterns across channels to distinguish attack flows from regular ones. However, the technique lacks detailed assault information and requires exploration in explainable artificial intelligence. Kunang *et al.* [9], a proposal for effective attack detection in the internet of medical things is presented, incorporating security and privacy measures through deep belief neural networks. Privacy and security are critical concerns in internet of things (IoT) technology, and a detection mechanism is vital. The study suggests a deep belief network (DBN) for intrusion detection, using the CICIDS dataset to evaluate its performance, showing higher accuracy compared to other classifiers. Kunang *et al.* [9] proposed an intrusion detection method using deep learning with hyperparameter optimization. This study combines a deep neural network and a deep AE with an automated hyperparameter optimization method. The technique, incorporating grid and random search, determines optimal hyperparameter configurations for improved identification performance. The study evaluates three feature extraction methods in the pretraining phase, where the deep AE approach yields the best results. Suganya and Sisipraba [10] proposed three distinct phases: detection, authentication, and registration, applied to the enron email dataset. The evaluation employs seven quality metrics: precision (95.25%), accuracy (95.16%), recall (96.54%), F1-score (93.76%), alongside measures for encryption time, decryption time, and root mean square error (RMSE). Thilagam and Aruna [11] proposed a method that includes pre-processing and balancing, utilizing a hybrid LSTM for attack classification on the NSL-KDD dataset. The approach incorporates the lion mutated-genetic algorithm (LM-GA) with a hybridization of machine learning (ML) algorithms, including CNN and LSTM. The achieved accuracy with this method is 94.98%.

Significant volumes of data and crucial information have been migrated to the cloud environment, presenting an opportunity to enhance overall security [12]. In the realm of network security, routing-based attacks are frequent occurrences. However, the majority of current research is designed with imbalanced learning data for detecting these attacks. The outcome is contingent upon the data; should the data be imbalanced or skewed, the results will not accurately portray the real scenario. Therefore, the current emphasis lies in enhancing defensive mechanisms, specifically addressing the imbalanced data by targeting routing-based attacks. This approach inherently incorporates an intrusion detection mechanism with the goal of enhancing overall network security. When tackling network-based attacks within the cloud environment, a broad spectrum of incidents is evident in the current cloud landscape [13]. Specifically, out of a total of 37 significant attacks within the cloud network environment, 26 are categorized as network-based attacks. Within the scope of these 26 attacks based on routing [9], the research emphasis will be directed towards distributed denial of service (DDoS) and denial of service (DoS). This decision stems from the motivation derived from the dataset pertaining to AWS cloud network, identified as CSECICIDS-2018 [14]. Enhancements to the current protective measures can be achieved through two avenues: i) optimizing the algorithm for minimizing time and space complexity and ii) refining the algorithm to enhance overall security measures. The focused methodology of this research involves utilizing the algorithm to enhance security, targeting intrusion detection specifically in the AWS cloud.

The suggested approach entails a hybrid algorithm derived from deep learning principles. It begins by processing input data in its raw form, representing traffic and subsequently employs a mechanism for clustering to distinguish between non-attack and attack data. The identified clustered attack data is then processed by the imbalanced data-trained deep learning algorithm to achieve accurate attack classification. Ultimately, the effectiveness of the categorized attacks will be validated through improved accuracy metrics such as accuracy, mean squared error (MSE), precision, recall, and F-measure.

2. THE COMPREHENSIVE THEORETICAL BASIS

Intrusion detection systems (IDS) play a vital role in ensuring the security of cloud-based environments against cyber threats and attacks. In the context of cloud computing, where vast amounts of

data are stored and processed on distributed servers, the risk of security breaches is heightened [2], [15]. An IDS monitors network and system activities, identifying and responding to unusual behavior that could signal a potential security threat [4]. The cloud infrastructure's dynamic and scalable nature poses unique challenges for intrusion detection, as attacks can manifest in various forms, including DDoS, unauthorized access attempts, and malware injection [16]. IDS in the cloud relies on advanced algorithms and machine learning techniques to analyze massive datasets and detect patterns indicative of malicious activity. Timely and accurate intrusion detection is essential for ensuring the confidentiality, integrity, and availability (CIA) of data stored and processed within cloud environments, contributing to the overall security posture of cloud-based systems [17], [18]. The elements comprising the IDS, as depicted in Figure 1, work in tandem to aid organizations in detecting and addressing security incidents, thereby fortifying their overall cybersecurity stance. Anomaly-based IDS, alternatively labeled misuse data-based IDS, depends on predefined norms for regular network or host behavior. It recognizes any deviations from these norms as potential intrusions [19]. Signature-based IDS, also recognized as rule-based IDS, utilizes a database containing predefined attack signatures or patterns. It scrutinizes network traffic or system activity in comparison to these signatures. Most research endeavors are geared towards integrated approaches that combine these methods.

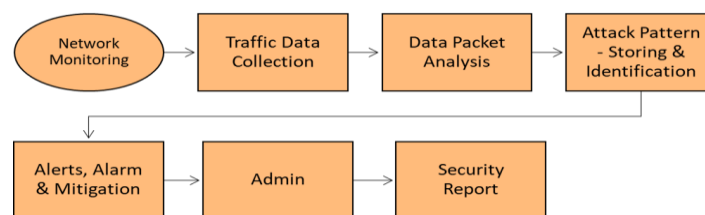


Figure 1. Components of IDS

2.1. DoS

A DoS attack is a deliberate and malicious attempt to disrupt or deny legitimate users access to a computer system, network, or service. In a DoS attack, the attacker overwhelms the targeted system with an influx of traffic or resource requests, causing it to become slow, unresponsive, or even completely unavailable [13]. The goal of a DoS attack is not to breach the system's security but rather to hinder its functionality and disrupt normal operations. DoS attacks can be executed using various methods, such as flooding the target with traffic, exploiting vulnerabilities in the system, or consuming its resources excessively [20]. Mitigating and preventing DoS attacks require robust security measures, including traffic filtering, resource management, and the use of specialized intrusion detection and prevention systems.

2.2. DDoS

DDoS attacks represent a more sophisticated and potent form of cyber threat compared to traditional DoS attacks. In a DDoS attack as shown in Figure 2, a multitude of compromised computers, frequently coalescing into a botnet, are planned to flood a target network or system, this involves orchestrating a substantial volume of traffic [21]. The objective is to overwhelm the resources of the target, causing disruption and making services inaccessible to authorized users. DDoS attacks are challenging to mitigate because they exploit the distributed nature of the assault, making it difficult to trace and block the multitude of sources simultaneously [22]. Attackers leverage diverse techniques, including amplification, reflection, and application-layer exploits, to maximize the impact. Mitigating DDoS attacks necessitates a comprehensive defense strategy [13] involving traffic filtering, rate limiting, and the utilization of specialized DDoS mitigation services to identify and thwart malicious traffic effectively.

2.3. Machine learning based intrusion detection techniques

In the realm of intrusion detection, contemporary deep learning and machine learning techniques, recognized for their effectiveness in cybersecurity [23], encompass diverse tools. Deep belief network (DBN) employs layered hidden units for intricate data representation [18], while DNN excels in complex feature learning [19]. The whale optimization algorithm (WOA), inspired by humpback whale behavior [21], and SVM adept at separating classes in high-dimensional spaces, contribute significantly to threat detection [6]. Additionally, PCA and clustering algorithms like DBSCAN reduce dataset complexity, aiding efficient processing and accurate threat detection [24]. Optimization methods such as particle swarm optimization (PSO) refine clustering algorithms for improved performance. Furthermore, classification techniques like

AE, a deep learning model, play a pivotal role in accurately identifying attack patterns based on learned representations, fortifying the defense against evolving cybersecurity threats [25].

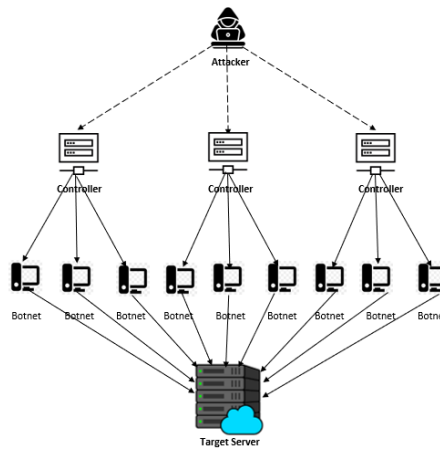


Figure 2. Structure of DDoS attack

3. RESEARCH METHOD

Explaining this hybrid model, PCA+DBSCAN-PSO+AE, integrates PCA for dimensionality reduction, DBSCAN for clustering, PSO for optimized clusters, and AE for attack classification is shown in the Figure 3. Focused on packet data within the attack cluster, it employs the CSE-CIC-IDS-2018 [14] dataset from AWS in 2018. The study prioritizes DDoS, DoS, covering majority of the dataset’s observed attacks.

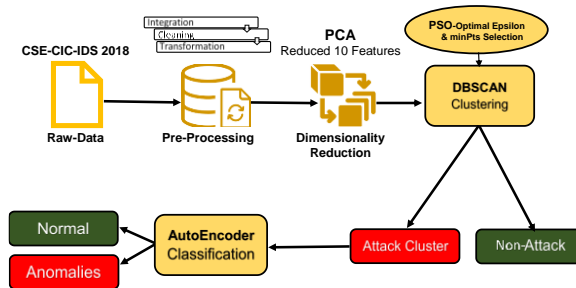


Figure 3. Proposed PCA+DBSCAN-PSO+AE IDS model

The raw data underwent preprocessing and normalization initially to enable efficient processing. With 78 features, the dataset presents a challenge for clustering algorithms due to its high dimensionality. The proposed model, PCA+DBSCAN-PSO+AE, is designed to address this issue by including all field values. While AE ensures high accuracy, it can extend processing time in a cloud environment. In extreme cloud scenarios, rapid attack detection and precise classification are crucial. The DBSCAN algorithm expedites attack detection, allowing the AE to exclusively classify attacked traffic data. This approach reduces input rows, leading to quicker classification with enhanced accuracy.

3.1. Data preparation

Data preparation involves three crucial stages: data pre-processing, feature normalization, and dimensionality reduction. Data pre-processing is essential as raw data often lacks completeness, requiring the handling of missing values. To address this, zero values represent missing data, resulting in a comprehensive data table. The pre-processed dataset exhibits variations in values across fields, each with distinct ranges, adding complexity. To standardize these ranges, normalization is applied, adjusting data based on its original distribution. Here, normalization scales data to a range of-1 to 1. The normalized data serves as input for the dimensionality reduction process, optimizing the dataset for subsequent analysis.

3.2. Dimensionality reduction

During the phase of dimensionality reduction, principal component analysis (PCA) is utilized to decrease data dimensionality. Two distinct methods are employed for dimensionality reduction: i) filtering out less significant features, or ii) compressing all features into a reduced set. This article opts for the second approach, utilizing PCA with four internal submodules: mean, standard deviation, co-variance, and eigenvalue/eigenvector. Ultimately, ten dimensionality-reduced features are generated as shown in Figure 4 for subsequent steps adhering to a 92% of threshold.

3.3. Cluster formation

The data, reduced in dimensionality, undergoes DBSCAN processing, identifying clusters based on packet feature density and grouping similar characteristics. This paper proposes a method involving varied learning percentages, from 60% to 90%, representing the cluster's knowledge acquisition from the dataset. When inserting the first packet, it's assigned to a cluster, optimized using PSO. DBSCAN's key parameters, Epsilon (ϵ -0.15) and MinPts-5, influencing cluster shape and density, are optimized by PSO. PSO, treating these parameters as particles, optimizes weights for dataset features based on a defined fitness function.

3.4. Attack classification

The AE, a deep learning-based classifier, receives its input from the clustered attack data points with reduced dimensionality. Importantly, to address imbalanced learning, the AE is trained exclusively on 100% benign data. This unique training strategy aims to overcome challenges posed by imbalanced datasets, ensuring that the model is well-equipped to classify both benign and attack instances effectively. The AE demonstrates optimal performance when dealing with lower-dimensional data, producing accurate results, especially in the context of clustered presentation. Specializing in classifying attack packet data, the AE employs backpropagation during training to learn patterns from the training dataset. During training, information flows from the decoder and is subsequently utilized in forward propagation, mirroring the encoder's functionality. Ultimately, the AE algorithm achieves a reduction in the mean-square error, resulting in the generation of the classified attack output.

4. RESULTS AND DISCUSSION

For this research, the designated execution environment is "Python version 3.0," and the suggested algorithm (PCA+DBSCAN-PSO+AE) is deployed within the AWS cloud. The execution is carried out under diverse environment configurations, specifically utilizing training-testing ratios of 60:40, 70:30, 80:20, and 90:10. The high dimensionality is reduced into ten features as shown in the scree plot in Figure 4 pointed in the elbow curve.

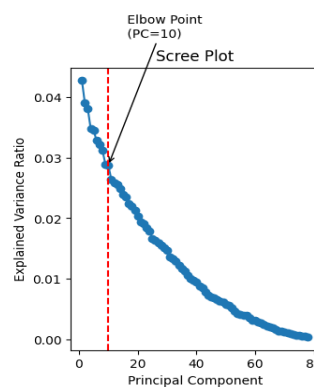


Figure 4. Principal component selection

A comparative analysis has been carried out between the current method and the suggested approach (PCA+DBSCAN-PSO+AE) across 4 evaluation criteria in each of the four test cases. A total of 16 comparisons were generated, covering 96 statistics. Among the existing methodologies, five were taken into consideration: DBN, DNN, DBN with WAO, LSTM, and SVM. Additionally, one approach from the proposed technique is included in each comparison. The experiments focus on DoS and DDoS attacks, generating a cumulative total of 192 statistics. The positive metrics considered for comparison include

precision, recall, F-measure, and accuracy. The corresponding equations for each metric are presented as (1) to (4), respectively.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (1)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (2)$$

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

$$\text{Accuracy} = \frac{TP+TN}{TP+TN +FP +FN} \quad (4)$$

Where,

TP - true positive,

TN- true negative,

FP- false positive,

FN- false negative

From Figure 5, it is evident that a larger training dataset leads to a significantly reduced false positive rate (FPR) compared to the conventional 70:30 split, highlighting the advantages of utilizing a substantial volume of data for training. The occurrences of intrusion detected in the network-based dataset within the AWS cloud for learning percentages of 60%, 70%, 80%, and 90% are illustrated in Figures 5(a) to 5(d) respectively. The respective confusion matrices for each learning percentage have been visually presented in these Figure 5.

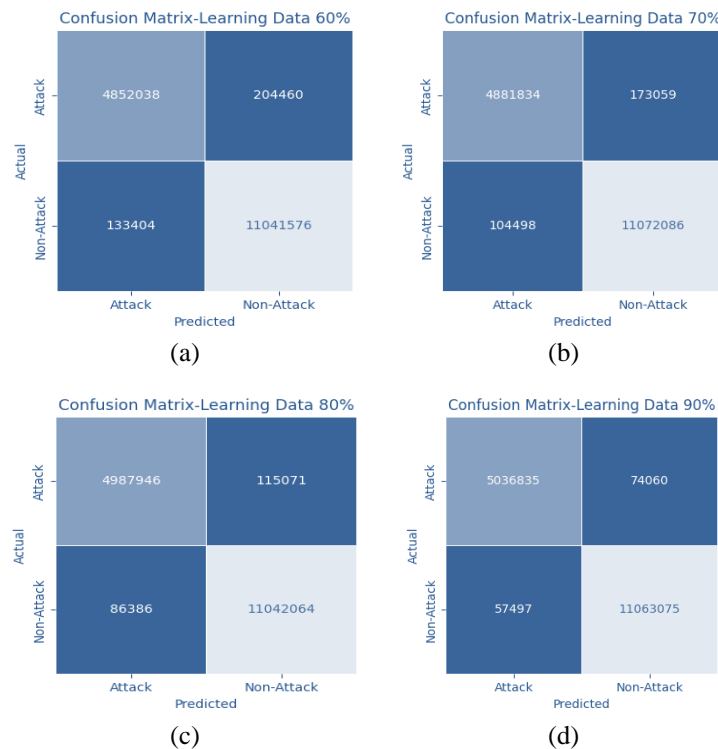


Figure 5. Confusion matrix: (a) 60% learning, (b) 70% learning, (c) 80% learning, and (d) 90% learning

The proposed approach evaluates detection accuracy through MSE. Figure 6 illustrates testing accuracy across different learning sets, emphasizing the model's effectiveness. Models constructed from 'Normal' and 'Attack' data in CSECICIDS2018 exhibit notable performance. AE model consistently achieves superior results, especially on 90% learning.

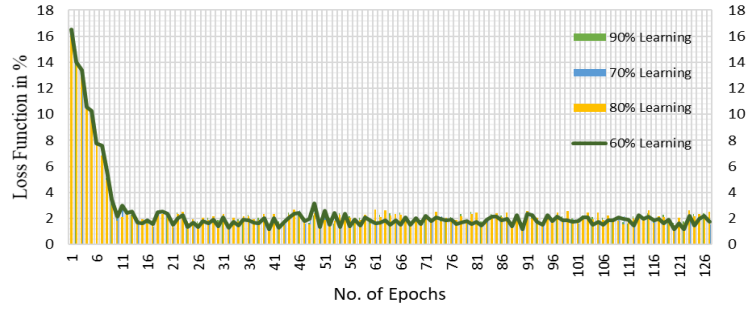


Figure 6. Autoencoder detetion model’s loss function

The results of the experiments, outlining various metrics at different learning percentages, are presented in Tables 1 and 2. The comparison of accuracy among existing methods is illustrated in Figure 7. Tables 1 and 2 illustrate the superiority of the proposed PCA+DBSCAN-PSO+AE compared to existing models in intrusion detection. With precision at 0.9856, recall at 0.9888, F-measure at 0.9871, and an impressive accuracy of 0.9919, the model excels across diverse training scenarios, notably achieving exceptional performance with a 90% training split. The results highlight its effectiveness in handling imbalanced data. Notably in Figure 7, the accuracy of the proposed technique, stands at 99.1%, surpassing existing methods such as DBN+WOA by 7.95%, LSTM by 9.67%, DNN by 10.90%, and SVM by 12.21%. These results highlight the effectiveness of the proposed technique, showcasing its superiority over existing state of the art protocols.

Table 1. Experimental outcomes-learning data 60% and 70%

Methods	Training data-60%: testing data-40%				Training data-70%: testing data-30%			
	Precision	Recall	F-measure	Accuracy	Precision	Recall	F-measure	Accuracy
SVM [6]	0.8197	0.8278	0.8337	0.8237	0.8293	0.8314	0.8403	0.8304
LSTM [26]	0.8489	0.8387	0.8437	0.8398	0.8578	0.8518	0.8547	0.8571
DNN [27]	0.8187	0.8102	0.8144	0.8217	0.8347	0.8213	0.8279	0.8317
DBN [28]	0.8587	0.8478	0.8532	0.8499	0.8747	0.8611	0.8678	0.8741
DBN+WOA [29]	0.8689	0.8652	0.8670	0.8714	0.8874	0.8798	0.8835	0.8997
PCA+DBSCAN-PSO+AE	0.9601	0.9736	0.9668	0.9792	0.9661	0.9795	0.9727	0.9829

Table 2. Experimental outcomes-learning data 80% and 90%

Methods	Training data-80%: testing data-20%				Training data-90%: testing data-10%			
	Precision	Recall	F-measure	Accuracy	Precision	Recall	F-measure	Accuracy
SVM [6]	0.8438	0.8497	0.8565	0.8467	0.8918	0.8898	0.9018	0.8907
LSTM [26]	0.8653	0.8592	0.8622	0.8793	0.8835	0.8847	0.8841	0.8829
DNN [27]	0.8424	0.8248	0.8335	0.8348	0.8745	0.8578	0.8660	0.8698
DBN [28]	0.8849	0.8628	0.8737	0.8952	0.8849	0.8628	0.8737	0.8952
DBN+WOA [29]	0.9057	0.8954	0.9005	0.9124	0.9187	0.9089	0.9137	0.9124
PCA+DBSCAN-PSO+AE	0.9778	0.9828	0.9802	0.9876	0.9856	0.9888	0.9871	0.9919

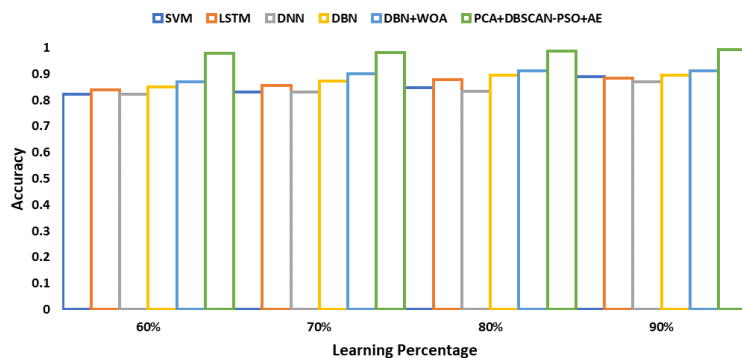


Figure 7. Accuracy comparison with existing system

The study's insights, emphasizing the success of the proposed intrusion detection technique and the importance of a larger training dataset with 100% benign data in AE, are crucial for advancing cybersecurity. Researchers can utilize these findings to develop more effective intrusion detection systems, overcoming imbalanced data challenges and improving overall network security. The identified superior accuracy of the proposed technique sets a benchmark for innovative approaches in addressing cybersecurity challenges.

5. CONCLUSION

The proposed approach processes data from the dataset CSE-CIC-IDS-2018 by initially conducting data preprocessing, including the handling of missing values. Subsequently, the data's dimensionality is reduced to mitigate complexity. The dimensionality-reduced data is then input into the clustering module, utilizing the DBSCAN clustering technique with PSO, resulting in the segregation of data into non-attack and attack clusters. The attack classifier module receives the data values from the attack cluster, utilizing the AE deep learning algorithm for accurate attack classification, specifically categorizing attacks into DDoS and DoS attacks. The proposed technique, denoted as PCA+DBSCAN-PSO+AE, demonstrates outstanding performance in positive measures, boasting precision at 98.5%, recall at 98.88%, F-measure at 98.71%, and accuracy at 99.19%. This remarkable achievement surpasses state-of-the-art techniques, establishing the proposed method as superior, achieving a 99.19% accuracy in predicting attack classifications over the CSE-CIC-IDS-2018 dataset. The study underscores the success of the proposed intrusion detection technique, emphasizing the importance of a larger training dataset with 100% benign data in AE. Crucial for advancing cybersecurity, it guides effective intrusion detection system development, enhancing accuracy, addressing imbalanced learning, and utilizing unsupervised learning for robust network security.




REFERENCES

- [1] Z. M. Fadli, S. S. Yong, L. K. Kee, and G. H. Ching, "Cyber attack awareness and prevention in network security," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 11, no. 2, p. 105, Aug. 2022, doi: 10.11591/ijict.v11i2.pp105-115.
- [2] V. Chang *et al.*, "A survey on intrusion detection systems for fog and cloud computing," *Future Internet*, vol. 14, no. 3, Mar. 2022, doi: 10.3390/fi14030089.
- [3] H. Attou *et al.*, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing," *Applied Sciences (Switzerland)*, vol. 13, no. 17, Sep. 2023, doi: 10.3390/app13179588.
- [4] Z. Liu, B. Xu, B. Cheng, X. Hu, and M. Darbandi, "Intrusion detection systems in the cloud computing: a comprehensive and deep literature review," *Concurrency and Computation*, vol. 34, no. 4, p. e6646, 2022, doi: 10.1002/cpe.6646.
- [5] A. Devarakonda, N. Sharma, P. Saha, and S. Ramya, "Network intrusion detection: a comparative study of four classifiers using the NSL-KDD and KDD'99 datasets," *Journal of Physics: Conference Series*, vol. 2161, no. 1, p. 12043, Jan. 2022, doi: 10.1088/1742-6596/2161/1/012043.
- [6] M. A. Almaiah *et al.*, "Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels," *Electronics (Switzerland)*, vol. 11, no. 21, Nov. 2022, doi: 10.3390/electronics11213571.
- [7] N. Oliveira, I. Praça, E. Maia, and O. Sousa, "Intelligent cyber attack detection and classification for network-based intrusion detection systems," *Applied Sciences (Switzerland)*, vol. 11, no. 4, pp. 1–21, Feb. 2021, doi: 10.3390/app11041674.
- [8] 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.
- [9] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprpto, "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization," *Journal of Information Security and Applications*, vol. 58, p. 102804, 2021, doi: 10.1016/j.jisa.2021.102804.
- [10] 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, Dec. 2023, doi: 10.1186/s13677-023-00442-6.
- [11] T. Thilagam and R. Aruna, "LM-GA: a novel IDS with AES and machine learning architecture for enhanced cloud storage security," *Journal of Machine and Computing*, vol. 3, no. 2, pp. 69–79, Apr. 2023, doi: 10.53759/7669/jmc202303008.
- [12] P. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 11, no. 2, pp. 504–515, Jun. 2022, doi: 10.11591/ijai.v11i2.pp504-515.
- [13] S. Sokkalingam and R. Ramakrishnan, "An intelligent intrusion detection system for distributed denial of service attacks: a support vector machine with hybrid optimization algorithm based approach," *Concurrency and Computation*, vol. 34, no. 27, p. e7334, 2022, doi: 10.1002/cpe.7334.
- [14] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, SciTePress, 2018, pp. 108–116, doi: 10.5220/0006639801080116.
- [15] P. K. Chouhan, A. Beard, and L. Chen, "Intrusion response systems: past, present and future," *ArXiv Preprint*, vol. abs/2303.03070, 2023.
- [16] R. Zhao, Y. Mu, L. Zou, and X. Wen, "A hybrid intrusion detection system based on feature selection and weighted stacking classifier," *IEEE Access*, vol. 10, pp. 71414–71426, 2022, doi: 10.1109/ACCESS.2022.3186975.
- [17] R. S. Abujassar, M. Sayed, and H. Yaseen, "A new algorithm to enhance security against cyber threats for internet of things application," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 4, pp. 4452–4466, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4452-4466.




- [18] T. A. J. Ali and M. M. T. Jawhar, "Detecting network attacks model based on a convolutional neural network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 3, pp. 3072–3078, Jun. 2023, doi: 10.11591/ijece.v13i3.pp3072-3078.
- [19] P. M. John and R. M. B. K. Nagappasetty, "An intelligent system to detect slow denial of service attacks in software-defined networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 3, pp. 3099–3110, Jun. 2023, doi: 10.11591/ijece.v13i3.pp3099-3110.
- [20] J. K. Jain and A. A. Waoo, "An artificial neural network technique for prediction of cyber-attack using intrusion detection system," *Journal of Artificial Intelligence, Machine Learning and Neural Network*, no. 32, pp. 33–42, Feb. 2023, doi: 10.55529/jaimlenn.32.33.42.
- [21] H. Hindy *et al.*, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," *IEEE Access*, vol. 8, pp. 104650–104675, 2020, doi: 10.1109/ACCESS.2020.3000179.
- [22] A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: a survey on strategies and defense," *Future Internet*, vol. 15, no. 2. MDPI, Feb. 01, 2023, doi: 10.3390/fi15020062.
- [23] 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.
- [24] A. S. Alfoudi *et al.*, "Hyper clustering model for dynamic network intrusion detection," *IET Communications*, 2022, doi: 10.1049/cmu2.12523.
- [25] J. Figueiredo, C. Serrão, and A. M. de Almeida, "Deep learning model transposition for network intrusion detection systems," *Electronics (Switzerland)*, vol. 12, no. 2, Jan. 2023, doi: 10.3390/electronics12020293.
- [26] 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, 2022, doi: 10.1007/s41870-022-01015-7.
- [27] S. P. Thirimanne, L. Jayawardana, L. Yasakethu, P. Liyanaarachchi, and C. Hewage, "Deep neural network based real-time intrusion detection system," *SN Computer Science*, vol. 3, no. 2, Mar. 2022, doi: 10.1007/s42979-022-01031-1.
- [28] O. Belarbi, A. Khan, P. Carnelli, and T. Spyridopoulos, "an intrusion detection system based on deep belief networks," in *Science of Cyber Security, C. Su, K. Sakurai, and F. Liu, Eds., Cham: Springer International Publishing*, 2022, pp. 377–392, doi: 10.1007/978-3-031-17551-0_25.
- [29] C. E. Singh and S. M. C. Vigila, "WOA-DNN for intelligent intrusion detection and classification in MANET services," *Intelligent Automation and Soft Computing*, vol. 35, no. 2, pp. 1737–1751, 2023, doi: 10.32604/iasc.2023.028022.

BIOGRAPHIES OF AUTHORS



K. Prabu    is an Assistant Professor in the School of Computing Science and Engineering at Galgotias University, bringing 15 years of teaching experience. Currently pursuing a Ph.D. in Computer Science and Engineering at Galgotias University, he holds an M. Tech in CSE (with Distinction) from SRM University and an MBA from Anna University. Alongside his academic pursuits, he has achieved notable milestones, publishing 4 patents and 6 research papers in esteemed international journals and conferences. His expertise spans cybersecurity, networks, cloud computing, software engineering, and machine learning. He can be contacted at email: k.prabu@galgotiasuniversity.edu.in.



Dr. P. Sudhakar    is a Professor and Program Chair in the School of Computing Science and Engineering at Galgotias University, accumulating 18 years of teaching experience. He earned his Ph.D. in CSE and M. Tech in CSE (with Distinction) from Anna University. P. Sudhakar has a prolific research record with 7 patents, 5 book chapters, and 18 research papers published in esteemed international journals and conferences. His expertise spans cyber security, networks, cloud computing, and machine learning. He can be contacted at email: p.sudhakar@galgotiasuniversity.edu.in.