ISSN: 2093-5374 / E-ISSN: 2093-5382

An Efficient Intrusion Detection Solution for Cloud Computing Environments Using Integrated Machine Learning Methodologies

Dr.P. Bharath Kumar Chowdary[1], Dr.R. Udayakumar[2*], Dr. Chaya Jadhav[3], B. Mohanraj[4], and Dr.V.R. Vimal[5]

[1]Assistant Professor, Department of Computer Science and Engineering, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India. bharathkumarchowdary@gmail.com, https://orcid.org/0000-0003-1793-5059

[2*]Dean, CS & IT, Kalinga University, India. rsukumar2007@gmail.com, https://orcid.org/0000-0002-1395-583X

[3]Professor, Department of Computer Engineering, Dr.D.Y. Patil Institute of Technology, Pune, India. jadhav.chaya.dpu@gmail.com, https://orcid.org/0000-0001-9180-6154

[4]Assistant Professor, Information Technology, Sona College of Technology, Salem, India. bmohanrajcse@gmail.com, https://orcid.org/0000-0001-5153-7359

[5]Professor, Institute of CSE, Saveetha School of Engineering, Saveetha Institute of Medical & Technical Sciences, Thandalam, Chennai, India. vimalraman2004@gmail.com, https://orcid.org/0000-0001-9401-4507

Received: January 06, 2024; Revised: February 15, 2024; Accepted: April 04, 2024; Published: June 29, 2024

Abstract

Cloud computing provides a range of services over the Internet using a pay-per-use model. Consequently, several firms have already used this system to entice people with its appealing characteristics. However, its architecture renders it susceptible to malicious assaults. This necessitates the implementation of an Intrusion Detection System (IDS) that can identify such assaults in a cloud environment accurately. This study presents a Machine Learning Efficient Intrusion Detection System (ML-EIDS) that integrates a Fuzzy C Means (FCM) clustering method with a Support Vector Machine (SVM) to enhance the precision of the detecting method in a cloud computing scenario. The suggested ML-EIDS system has been executed and contrasted with preexisting methods. The NSL-KDD dataset is used for conducting experiments. Through performance assessment and comparative analysis, the findings achieved by implementing the ML-EIDS hybrid method demonstrate that the suggested system can accurately detect abnormalities with high precision and a low occurrence of false alarms, surpassing current methodologies.

Keywords: Intrusion Detection, Cloud Computing, Machine Learning, Hybrid Method.

1 Intrusion Detection System

The capacity to execute cloud-based threats and assaults has empowered cyber invaders, assailants, and hackers globally, enabling them to impact the integrity of the cloud infrastructure significantly (Dutta et

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 2 (June), pp. 14-26. DOI: *10.58346/JOWUA.2024.I2.002*

*Corresponding author: Dean, CS & IT, Kalinga University, India.

al., 2022). Cloud computing is susceptible to several forms of assaults. The risks include data loss, breaches, unsecured interfaces and Application Programming Interfaces (API), malevolent insiders, unidentified risk profiles, and identity theft (Katal et al., 2023). Cloud-based attacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS), can quickly turn off a target and result in significant financial losses (Alashhab et al., 2022; Jayasree et al., 2012). Despite the abundance of conventional methods for detecting threats, there continues to be a substantial and ongoing rise in both the number and severity of threats and assaults. In cybersecurity, an attacker refers to an entity aiming to exploit a system's weaknesses. Signatures or anomalies are used to detect intrusions. Signature-based intrusion detection methods that rely on outdated methods cannot effectively identify new and innovative assaults (Muralidharan et al., 2020; Juma et al., 2023).

The anomaly-based strategy, which involves comparing user habits with established trends, has a significant drawback of often generating false identifications. This issue is resolved by using a very efficient categorization technique. Testing the efficacy of the built Intrusion Detection System (IDS) on a live dataset is sometimes impractical (Sarhan et al., 2022). A predetermined dataset, including real-time network traffic, is utilized to evaluate the effectiveness of the IDS. The KDD-CUP 99 dataset is widely recognized as the most prominent dataset of its type and has garnered significant attention from several academics (Kumar et al., 2022). The NSL-KDD dataset is the optimized rendition, among other options (Esmaeili et al., 2022; Srinivasa Rao et al., 2023). These datasets are susceptible to a limited number of attack methods.

These two datasets are plagued by a need for more characteristics, rendering them unreliable for evaluating an IDS against novel and evolving security risks and tactics used by attackers and intruders. It is essential to use IDSs on more current datasets with more characteristics and include a more comprehensive range of assaults, such as the CICIDS2018 dataset (Farhan & Jasim, 2022). Cybersecurity concerns significantly threaten the security and privacy of consumers' data. Emerging security concerns and assaults in cloud systems need more efficient and intelligent approaches to address the issue of openness. Signature-based intrusion-detecting solutions that need to be updated cannot effectively identify and react to new and innovative threats (Sivanantham et al., 2023).

Network Intrusion Detection Systems (NIDSs) use machine learning techniques to overcome the limitations of existing theories, and their usage is growing (Albasheer et al., 2022). Machine Learning (M]L) and Deep Learning (DL) techniques have been created to effectively identify developing cyberattacks in this categorization (Kutlu et al., 2021; Jelena et al., 2023). DL is a specialized category within ML. DL surpasses other methods due to three primary factors. Firstly, its processing capabilities have significantly improved. Another factor is the increasing affordability of computers. The third factor is the significant advancement in ML research. In (Camgözlü & Kutlu, 2023), convolutional neural network-based leaf detection algorithm was proposed. The class and image diseases can effectively be classified by CNN.

The proliferation of cloud-based risks and assaults has provided cyber intruders, criminals, and hackers worldwide with a powerful tactic capable of significantly impacting the integrity of the cloud environment. Cloud computing is susceptible to several forms of assaults. The risks included are loss of information, data violations, unsecured interfaces and APIs, malevolent insiders, unidentified risk categories, and theft of identities. Despite the abundance of conventional methods for detecting threats, there continues to be a substantial and ongoing increase in the frequency, volume, and severity of assaults.

This work proposes a Machine Learning Efficient Intrusion Detection System (ML-EIDS), an improved Fuzzy C-Means Clustering (FCM) with a Support Vector Machine (SVM) as a hypervisor inspection to attain superior precision and minimal false alarm rates for all IDS categories. The suggested approach undergoes training and testing using the NSL-KDD database, and it is contrasted with pre-existing systems (Rohit, 2022).

The remainder parts of the research are listed section 2 deals with the background and summary of the literature about IDS. Section 3 proposes the Machine Learning Efficient Intrusion Detection System for a cloud computing environment. Section 4 discusses the simulation results and outcomes compared with the existing models. Section 5 concludes the research with findings and discussions.

2 Background and Research Summary

This section focuses on the current IDS solutions suggested for cloud computing environments.

Imran et al., created an IDS that utilizes DL techniques (Imran et al., 2022). Their model has four layers: a Gated Recurring Unit (GRU), Long Short-Term Memory (LSTM), multilayered perceptron, and SoftMax extrapolation. The model underwent evaluation using two renowned datasets: KDD 99 and NSL-KDD. The identification rate obtained for the initial database was 89.42%, while for the additional dataset, it reached 89.31%. The false positive rates were 3.25% and 1.84% for both initial datasets.

A cooperative IDS based on ML is suggested by (Otoum et al., 2022). A denoising autoencoder is one of the fundamental components of the deep neural network model. The highest number of concealed units was 350. When the model was applied to the altered KDD CUB 99 database, it demonstrated a detection rate of 75%. An integrated structure plays an important role in recent days for classification application. The hybrid SVM based FFNN model is implemented in (Udayakumar et al., 2023) for finding fraud in banking sector.

The IDS used a confident neural network to extract characteristics from network information (Yan et al., 2023). Intruder types were categorized utilizing the back-propagating neural networks as the top layer. The algorithm was validated using the KDD CUP′99 database, and the findings demonstrated enhanced accuracy compared to conventional ML methods.

Cao et al., utilized conditionally random fields and a linear-correlation parameter-based feature-choosing technique in their suggested IDS to categorize features using a convolutional neural network (Cao et al., 2022; Trivedi et al., 2023). They claimed accuracy using the KDD CUP′99 database was 71.28%.

Soliman et al. introduced an IDS that utilizes multiconvolutional neural networks (Soliman et al., 2023). The feature information is categorized into four segments based on their correlation. The findings indicated that this model surpassed standard ML and current DL approaches when utilizing the NSL-KDD dataset. Radio frequency jamming detection can be tedious task in recent days. The machine learning based jamming detection was carried out in (Kasturi et al., 2020).

The technique incorporated both ML and DL, utilizing supervised and unsupervised learning. DL is implemented using Convolutional Neural Networks (CNN) to extract features. Ullah et al., utilized DL in their constructed IDS design (Ullah et al., 2022). This approach was employed to categorize both segmented and user-defined multiclasses. The algorithm achieved a 95% accuracy when tested with the UNSW-NB15 database.

Polat et al. presented the GRU and recurrent neural networks as an IDS for a software-defined network (Polat et al., 2022). The NSL-KDD database assessed the suggested model, which consisted of six characteristics. The model achieved an accuracy rate of 73%.

Feature selection is a crucial step in dealing with high-dimensional information. By reducing the model difficulty, the computing cost is minimized. It streamlines the model troubleshooting, boosting the learning outcomes' analysis. Chamishka et al. used the openSMILE toolbox to identify the low-level acoustic features better suited for the proposed speech detection system using a deep neural network (Chamishka et al., 2022). Radio frequency jamming detection can be tedious task in recent days. The machine learning based jamming detection was carried out in (Kasturi et al., 2020). A new methodology for detecting an Android app's class-level obfuscation mechanism has been proposed in this (Park et al., 2019). Using a paragraph vector, the framework vectorizes the decompiled codes of every class of Android applications.

Numerous conclusions are drawn based on the research above on DL-based IDSs. Feature selection is given lower priority due to its role in diminishing the intricacy of real-time assault categorization and detection. Despite the False Alarm Rate (FAR) being a commonly used indication of IDS effectiveness, it is often not included as a metric in comparable studies. Conversely, those who believed it to have a high FAR estimated it to be between 2.5% and 4.23%. The performed research mainly restricts the accuracy and identification rate assessment. Enhancing the precision, along with other strategies, and decreasing the False Discovery Rate (FDR) reduce the burden of network specialists and render the system feasible and dependable for real-world application.

3 Proposed Machine Learning Efficient Intrusion Detection System

The system begins by preparing the incoming data to ensure consistency for subsequent steps, as seen in Figure 1. During preprocessing, samples containing empty values are eliminated, textual information is transformed into a uniform format, and characteristics are standardized. Following this, the subsequent phase involves feature selection. The Pearson correlation approach is used at this step. The third stage represents the central component of the framework. The input layer applies the activating function for training the information at this level. The resultant layer has four neurons using the SoftMax activation mechanism. One of the neurons represents the benign class, while the remaining three represent the attack categories.

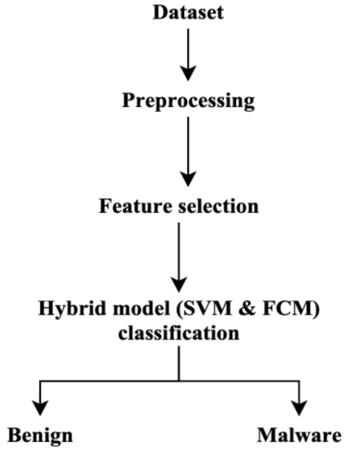

Figure 1: Proposed ML-EIDS Workflow

The dataset is partitioned randomly, with 80% allocated for training and 20% for testing. The mean outcomes of 10 iterations of the sample information are considered to mitigate any potential bias in the findings. After dividing the info, the ML-EIDS framework is used for the training procedure. After completing the training, the model learned is used for the validation step, using the other twenty percent. It is employed for forecasting and assessing performance.

Intrusion Detection System

The plan employs a three-step procedure to satisfy the study goals. The first step involves establishing a cluster grouping by using the function for membership with the NSL-KDD database. It fully understands the functioning of fuzzy logic in the suggested system. Fuzzy logic encompasses all methods and gadgets that use a set of fuzzy values. A multivalued logic enables the definition of intermediate numbers that lie among typical binary states, such as true or false, white/black, and yes or no. It also allows for representing degrees of truth ranging from 0 to 1. Intrusion Detection Model of ML-EIDS in shown figure 2.

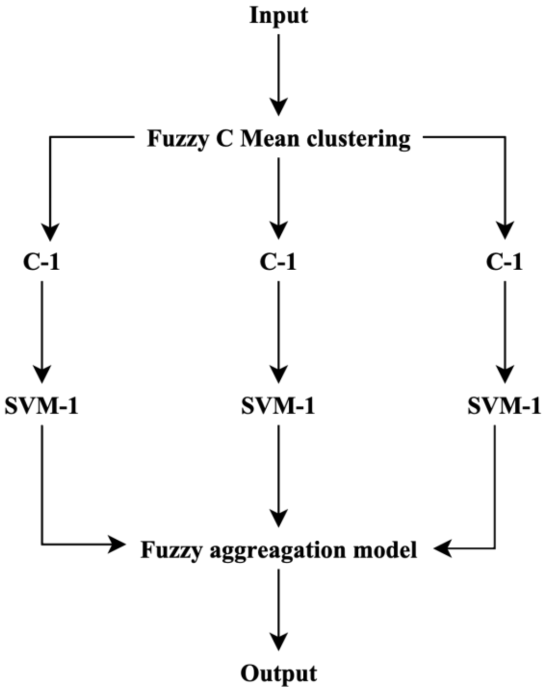

Figure 2: Intrusion Detection Model of ML-EIDS

The point at the midpoint between the focal points of the two groupings is considered to have ongoing membership. The FCM method assigns a distinct cluster to every information point based on its membership rating. This approach demonstrates that the data point can belong to many groups simultaneously. The letter "c" represents the number of clusters. All groups must possess a uniform size, and the quantity of groups is predetermined and regulated. The FCM method partitions x data points, represented as m-dimensional matrices u_x $(x = 1,2,\cdots,n)$, into c fuzzy groups. The FCM algorithm determines the centroid of each group by minimizing the objective variable. This method distinguishes itself from the FCM by including a fuzzy partitioning approach. The components of the M membership vector vary from 0 to 1.

The second stage will use these groups to train and evaluate the Genetic Programming (GP) and SVM methods. The third phase will assess the efficacy of the FCM by using several computational techniques to contrast the discrepancies produced by each approach.

Cloud computing operates on virtualization. Therefore, the current study aims to identify irregularities in a simulated network and events inside the system by examining several virtual computers. The ML-EIDS-trained hypervisor inspection is designed to monitor virtual servers and their activities. Fuzzy linguistic metrics, also known as fuzzy categories, are determined by a set of fuzzy collections.

The degree of uncertainty among data points is within the bounds of $[1, n]$ based on the fuzzification settings. Fuzzy grouping is a method that groups data points into cluster groups by giving a fuzzy membership value. The FCM method partitions a set of n elements $E = \{e_1, e_2, \cdots, e_n\}$ into groups of comparable sizes based on the membership value. The method returns the partition matrices $m = {m_{xy}}^{TM}[0,1]$ and a set of c clustered cores $cc = \{cc_1, cc_2, \cdots, cc_n\}$ where $x = 1,2, \cdots, n$ and $y = 1,2, \cdots, n$.

m_{xy} is the numerical value of the fuzzy membership function that assigns a degree of relevance to the data item. The structure of the ML-EIDS structure, which consists of three distinct stages:

- In Phase 1, Fuzzy clustering is employed to partition extensive datasets into smaller clusters based on the membership metrics.
- During Phase 2, the SVM is trained based on different clusters.
- In Phase 3, the fuzzy aggregation component is employed to merge the outcomes of the hypervisor inspector to restrict various SVM mistakes.

Implementation and Results

The research utilized the Weka simulation to develop the suggested hybrid method based on FCM and SVM. The ML-EIDS method is trained and evaluated using the Weka simulator. FCM is assessed compared to other enhanced soft computing methods like SVM. The discovered factors that impact various assaults on the cloud, including DoS and regular, are used to create a hybrid IDS that combines FCM and SVM.

A comprehensive digital network was established, consisting of several switches and a router, and then deployed inside the server infrastructure. The assault coordinating system functioned as both the Master client and the Handler.

The Weka simulation yields enhanced outcomes of the ML-EIDS method. A binary classification generates output by assigning one of two category values or tags, such as Yes or No or 1/0, to a given set of input information. The interest group is often called positive, whereas the opposing group is called negative.

Performance Evaluation

The research utilized the NSL-KDD test datasets to evaluate efficiency. It encompasses the recorded labels for every data occurrence. The actual labels are employed for performance assessment following categorization by comparing them with the predicted categories. Attacks often target networks since they exploit account vulnerabilities with easily guessable login and password configurations. It utilized nine algorithms from the Weka software to perform the categorization assignment. All strategies used a

10-fold cross-validation for testing. NSL-KDD is proposed to address some issues in the initial KDD99 database. A significant drawback of the KDD database is its extensive redundancy, leading to a bias in the learning methods favoring the more frequent entries. Figure 3 illustrates the categorization procedure of the NSL-KDD database.

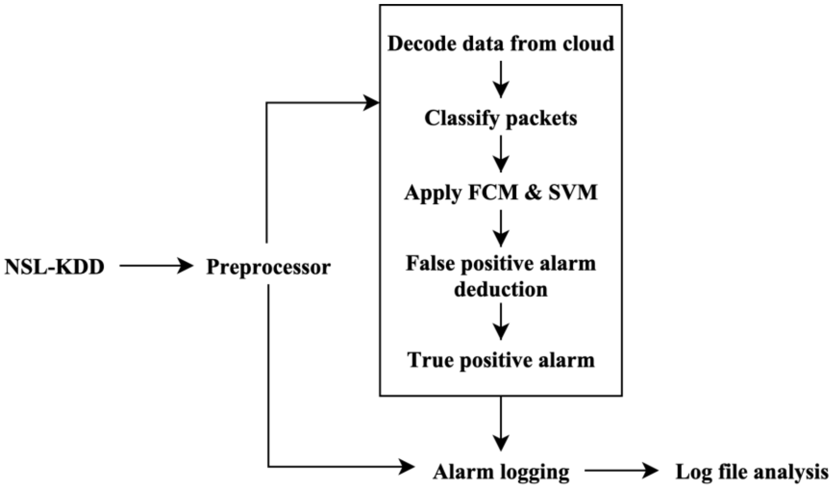

Figure 3: Workflow of the Intrusion Classification of ML-EIDS

The database included 9 million records of regular traffic and 4 million entries of assault traffic. Each entry has 41 attributes that describe various flow characteristics, along with a label indicating whether it is classified as an attack variety or regular. The characteristic information, including the usual name, includes type information for all 41 characteristics in the NSL-KDD dataset. These properties include information on the several categories of network connecting vectors, specifically classified into one normal category and four attack categories.

4 Simulation Analysis and Outcomes

The HP server has an Intel CPU, 8GB of RAM, and a 2TB hard drive. The system is fitted with an HP Ethernet 1 GB Adapter and runs on Debian 9.2 with Linux Kernel version 4.9. This configuration offers a resilient and effective computing infrastructure for various workloads. Various measures to assess performance include accuracy, precision, detection rate, false positive rate, and F1-score.

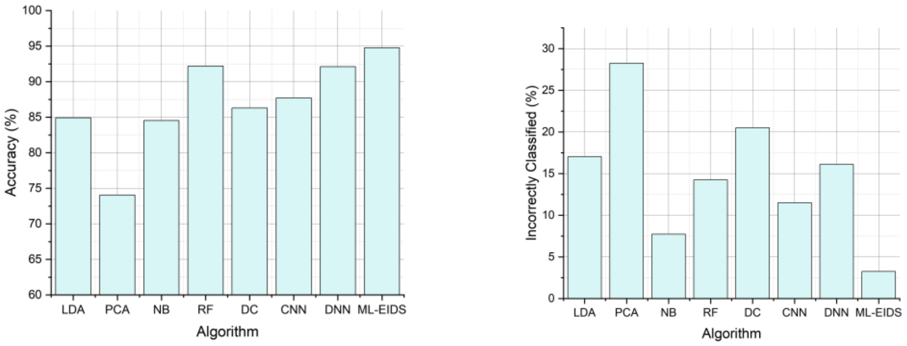

Figure 4(a): Accuracy Analysis and Figure 4(b): Incorrectly Classified Results

Figure 4(a) presents the accuracy results, demonstrating that ML-EIDS is the leading model with an accuracy of 94.75%. Figure 4(b) displays the examples that were miscategorized. ML-EIDS outperforms other algorithms in this regard, obtaining a meager rate of 3.25%. The suggested technique demonstrates a significant improvement in accuracy compared to other methods, outperforming LDA, PCA, NB, RF, DC, CNN, and DNN by 9.83%, 20.7%, 10.21%, 2.55%, 8.45%, 7.02%, and 2.63% respectively. The significant improvement is credited to the combined use of FCM clustering and SVM in ML-EIDS, which optimizes the representation of features and substantially improves intrusion-detecting abilities in cloud settings.

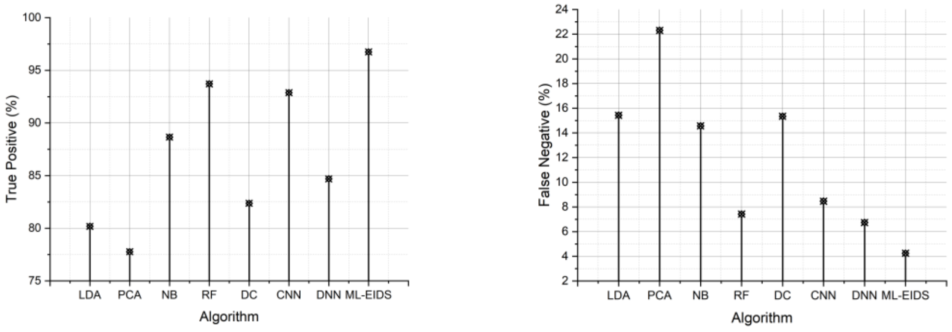

Figure 5(a): True Positive and Figure 5(b): False Negative Analysis

Figure 5(a) shows the true positive rates, with ML-EIDS achieving the highest accuracy of 96.75%. Figure 5(b) demonstrates the false negative rates, with ML-EIDS doing very well at just 4.25%. ML-EIDS shows a significant improvement in the rates of correctly identified positive instances when compared to other methods, outperforming LDA, PCA, NB, RF, DC, CNN, and DNN by 16.57%, 19.98%, 8.09%, 3.04%, 14.38%, 4.87%, and 12.06%, correspondingly. The exceptional performance of ML-EIDS in cloud computing settings is due to the successful combination of FCM clustering and SVM. This integration optimizes feature representation and reduces false negatives, resulting in a highly reliable IDS.

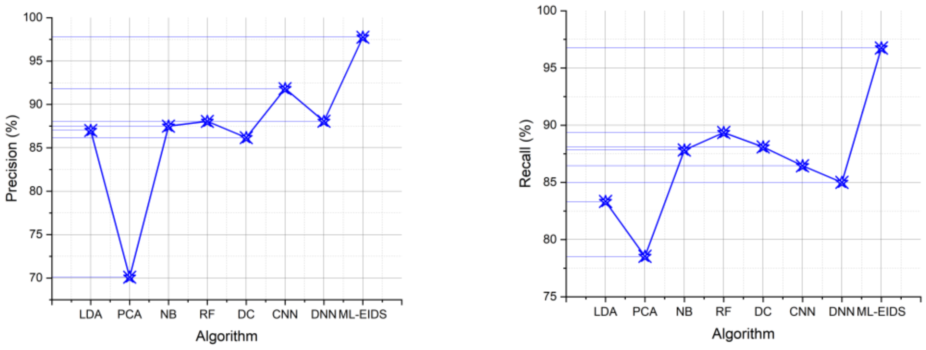

Figure 6(a): Precision and Figure 6(b): Recall Analysis

Figure 6(a) shows the precision results, with ML-EIDS achieving the highest accuracy rate of 97.75%. Figure 6(b) simultaneously presents recall percentages, showcasing the remarkable achievement of ML-EIDS with a score of 96.75%. ML-EIDS exhibits a significant improvement in accuracy when compared to other methods such as LDA, PCA, NB, RF, DC, CNN, and DNN, exceeding them by 10.74%, 27.65%, 10.25%, 9.7%, 11.57%, 6.93%, and 9.69%, correspondingly. The ML-EIDS algorithm demonstrates a superior recall compared to LDA, PCA, NB, RF, DC, CNN, and DNN, with improvements of 13.42%, 18.21%, 8.92%, 7.39%, 8.65%, 10.3%, and 11.75% correspondingly. This highlights its strong ability to identify positive cases accurately.

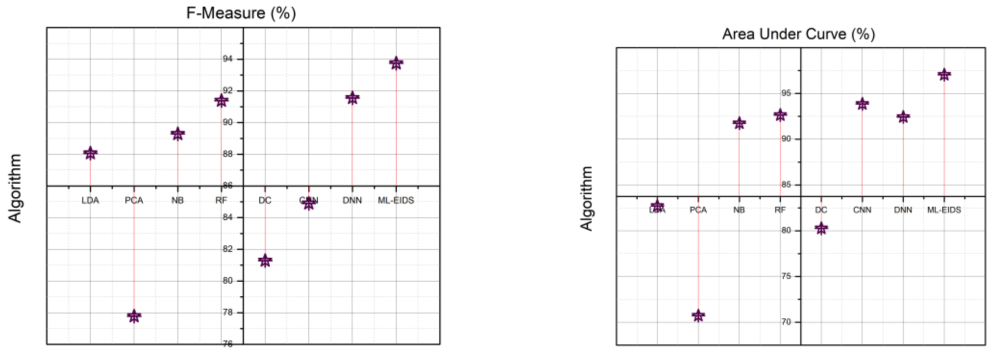

Figure 7(a): F Measure and Figure 7(b): The Area Under Curve Analysis

Figure 7(a) displays the results of the F-Measure, with ML-EIDS achieving the highest score of 93.75%. Figure 7(b) shows the percentages of the Area Under the Curve (AUC), with ML-EIDS reaching an outstanding 97.05%. ML-EIDS exhibits a significant enhancement in F-Measure compared to other methods such as LDA, PCA, NB, RF, DC, CNN, and DNN. It outperforms these methods by 5.68%, 15.97%, 4.46%, 2.36%, 12.46%, 8.85%, and 2.19%, correspondingly. The ML-EIDS algorithm performs better than other methods, such as LDA, PCA, NB, RF, DC, CNN, and DNN. It outperforms these methods by 14.33%, 26.32%, 5.3%, 4.41%, 16.79%, 3.19%, and 4.62%, indicating its resilience in reaching a balanced performance between accuracy and recall.

5 Conclusion and Discussion

This study presents an ML-EIDS system explicitly designed for cloud environments. This technique implements an intrusion-detecting system inside the surveillance layer of the virtual computer. Hypervisor inspection is developed using a hybrid methodology combining SVM and FCM clustering. The ML-EIDS model is partitioned into three stages. The first stage involves implementing the FCM clustering component, which is used to partition large datasets into smaller clusters. This allows the SVM to acquire knowledge efficiently within a reasonable timeframe. The fuzzy clustering module improves the SVM performance using this procedure. Several SVM components are trained based on the provided clustering values during the subsequent phase. The third module, the fuzzy aggregation component, consolidates the outcomes obtained from the hypervisor inspection. The suggested ML-EIDS methodology is evaluated against current methodologies utilizing a range of assessment criteria, including accuracy, erroneous classifying rate, false negative rate, true positive rate, precision, recall, and F-1 score, across different types of assaults. The performance outcomes of ML-EIDS demonstrate its superiority over the current techniques. Therefore, the suggested ML-EIDS method is well-suited for accurately detecting a wide range of assaults with few false alarms. As a result, it is implemented to identify abnormalities in a cloud environment.

References

[1] Alashhab, Z. R., Anbar, M., Singh, M. M., Hasbullah, I. H., Jain, P., & Al-Amiedy, T. A. (2022). Distributed denial of service attacks against cloud computing environment: survey, issues, challenges and coherent taxonomy. *Applied Sciences*, *12*(23), 12441. https://doi.org/10.3390/app122312441

[2] Albasheer, H., Md Siraj, M., Mubarakali, A., Elsier Tayfour, O., Salih, S., Hamdan, M., & Kamarudeen, S. (2022). Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: a survey. *Sensors*, *22*(4), 1494. https://doi.org/10.3390/s22041494

[3] Camgözlü, Y., & Kutlu, Y. (2023). Leaf Image Classification Based on Pre-trained Convolutional Neural Network Models. *Natural and Engineering Sciences, 8*(3), 214-232.

[4] Cao, B., Li, C., Song, Y., & Fan, X. (2022). Network intrusion detection technology based on convolutional neural network and BiGRU. *Computational Intelligence and Neuroscience*, *2022*.

[5] Chamishka, S., Madhavi, I., Nawaratne, R., Alahakoon, D., De Silva, D., Chilamkurti, N., & Nanayakkara, V. (2022). A voice-based real-time emotion detection technique using recurrent neural network empowered feature modelling. *Multimedia Tools and Applications*, *81*(24), 35173-35194.

[6] Dutta, A., Bose, R., Kumar Chakraborty, S., & Roy, S. (2022). A security provocation in cloud-based computing. In *Pattern Recognition and Data Analysis with Applications*, 343-355. Singapore: Springer Nature Singapore.

[7] Esmaeili, M., Goki, S. H., Masjidi, B. H. K., Sameh, M., Gharagozlou, H., & Mohammed, A. S. (2022). Ml-ddosnet: Iot intrusion detection based on denial-of-service attacks using machine learning methods and nsl-kdd. *Wireless Communications and Mobile Computing*, *2022*.

[8] Farhan, B. I., & Jasim, A. D. (2022). Performance analysis of intrusion detection for deep learning model based on CSE-CIC-IDS2018 dataset. *Indonesian Journal of Electrical Engineering and Computer Science*, *26*(2), 1165-1172.

[9] Hemasree, V., & Kumar, K. S. (2022). Facial Skin Texture and Distributed Dynamic Kernel Support Vector Machine (DDKSVM) Classifier for Age Estimation in Facial Wrinkles. *Journal of Internet Services and Information Security (JISIS)*, *12*(4), 84-101.

[10] Imran, M., Haider, N., Shoaib, M., & Razzak, I. (2022). An intelligent and efficient network intrusion detection system using deep learning. *Computers and Electrical Engineering*, *99*, 107764. https://doi.org/10.1016/j.compeleceng.2022.107764

[11] Jayasree, V., Nithya, M., & Prabaharan, S. (2012). Cloud Data Retrieval for Multi related keyword based on Clustering Technology. *International Journal of Communication and Computer Technologies (IJCCTS), 1*(1), 60-66.

[12] Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. *Archives for Technical Sciences, 2*(29), 11-22.

[13] Juma, J., Mdodo, R. M., & Gichoya, D. (2023). Multiplier Design using Machine Learning Alogorithms for Energy Efficiency. *Journal of VLSI Circuits and Systems, 5*(1), 28-34.

[14] Kasturi, G. S., Jain, A., & Singh, J. (2020). Detection and Classification of Radio Frequency Jamming Attacks using Machine learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 11*(4), 49-62.

[15] Katal, A., Dahiya, S., & Choudhury, T. (2023). Energy efficiency in cloud computing data centers: a survey on software technologies. *Cluster Computing*, *26*(3), 1845-1875.

[16] Kumar, S., Gupta, S., & Arora, S. (2022). A comparative simulation of normalization methods for machine learning-based intrusion detection systems using KDD Cup'99 dataset. *Journal of Intelligent & Fuzzy Systems*, *42*(3), 1749-1766.

[17] Kutlu, Y., & Camgözlü, Y. (2021). Detection of coronavirus disease (COVID-19) from X-ray images using deep convolutional neural networks. *Natural and Engineering Sciences, 6*(1), 60-74.

[18] Muralidharan, J. (2020). Wideband Patch Antenna for Military Applications. *National Journal of Antennas and Propagation (NJAP), 2*(1), 25-30.

[19] Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: a deep learning–based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies, 33*(3), e3803. https://doi.org/10.1002/ett.3803

[20] Park, M., You, G., Cho, S. J., Park, M., & Han, S. (2019). A Framework for Identifying Obfuscation Techniques applied to Android Apps using Machine Learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 10*(4), 22-30.

[21] Polat, H., Türkoğlu, M., Polat, O., & Şengür, A. (2022). A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks. *Expert Systems with Applications*, *197*, 116748. https://doi.org/10.1016/j.eswa.2022.116748

[22] Rohit. (2022). Research Performance of Central University of Haryana: A Bibliometric Analysis. *Indian Journal of Information Sources and Services, 12*(2), 16–21.

[23] Sarhan, M., Layeghy, S., & Portmann, M. (2022). Towards a standard feature set for network intrusion detection system datasets. *Mobile networks and applications*, 1-14.

[24] Sivanantham, S., Mohanraj, V., Suresh, Y., & Senthilkumar, J. (2023). Rule precision index classifier: an associative classifier with a novel pruning measure for intrusion detection. *Personal and Ubiquitous Computing*, 1-9.

[25] Soliman, S., Oudah, W., & Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal*, *81*, 371-383.

[26] Srinivasa Rao, M., Praveen Kumar, S., & Srinivasa Rao, K. (2023). Classification of Medical Plants Based on Hybridization of Machine Learning Algorithms. *Indian Journal of Information Sources and Services, 13*(2), 14–21.

[27] Trivedi, J., Devi, M. S., & Solanki, B. (2023). Step Towards Intelligent Transportation System with Vehicle Classification and Recognition Using Speeded-up Robust Features. *Archives for Technical Sciences, 1*(28), 39-56.

[28] Udayakumar, R., Chowdary, P. B. K., Devi, T., & Sugumar, R. (2023). Integrated SVM-FFNN for Fraud Detection in Banking Financial Transactions. *Journal of Internet Services and Information Security (JISIS), 13*(3), 12-25.

[29] Ullah, S., Khan, M. A., Ahmad, J., Jamal, S. S., e Huma, Z., Hassan, M. T., & Buchanan, W. J. (2022). HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles. *Sensors*, *22*(4), 1340. https://doi.org/10.3390/s22041340

[30] Yan, F., Zhang, G., Zhang, D., Sun, X., Hou, B., & Yu, N. (2023). TL-CNN-IDS: transfer learning-based intrusion detection system using convolutional neural network. *The Journal of Supercomputing*, *79*(15), 17562-17584.

Authors Biography

Dr.P. Bharath Kumar Chowdary is currently working in Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology (VNR VJIET), Hyderabad as an Assistant Professor in Department of Computer Science and Engineering (CSE). He received his Ph.D in CSE from Bharath Institute of Higher Education and Research (BIHER), Chennai in the year 2022. Also, he received Bachelor degree in CSE in the year 2008 from Jawaharlal Nehru Technological University, Hyderabad and Master degree in CSE in the year 2012 from Jawaharlal Nehru Technological University, Anantapur. With a total teaching experience of 15 years, he has published 12 papers in various reputed Journals and conferences. He has filed a Patent. Currently he is also working for a consultancy project worth Rs.25 Lakhs with a US based firm. He has received the prestigious BEE Best Teacher Award from Chairman-APSCHE and the COO- AICTE for the year 2022.cHe is also involved in working towards Trainings, Placements and Competency Development among students' community. He has been nominated as a Faculty Advisor for Google Developers Club. He has guided more than 40 projects for Bachelor and Masters students. His research interest includes Bigdata analytics, Software Engineering Artificial Intelligence, Deep Learning and Machine Learning.

Professor & Dean. Dr. Udayakumar Ramanathan completed his M.S (Information Technology and Management) from A.V.C. College of Engineering and Awarded Ph.D. in the year 2011. He is serving in Teaching & Research community for more than two decades, he successfully produced 5 Doctoral candidates, he is a researcher, contribute the Research work in inter disciplinary areas. He is having h-index of 27, citation 2949(Scopus). He is associated as Dean –Department of computer science and Information Technology, Kalinga University, Raipur, Chhattisgarh.

Dr. Chaya Jagtap (Jadhav) holds master's from Govt. College of Engineering, COEP Pune and she Completed her Ph.D. in Electronics and Communication Engineering in 2019 from Vignan University, Guntur, A.P. Recognition as a Ph.D. Research Guide at SPPU. Guiding 3 research scholars. Recognized as a Approved as PG Teacher at SPPU. Working as a Subject Chairman for SE computer subject "Digital Electronics and Logic Design" (for 2015 Course & 2019 Course). Currently doing research in the field of medical image processing and Machine learning. Working at Dr.D.Y. Patil Institute of Technology (DIT), Pimpri, Pune since 2001, presently she is working as a professor in department of Computer Engineering. Total teaching experience is more than 25 years. Presently chairman for new syllabus framing (2019 Course) for Digital Electronics and Logic Design under SPPU Pune. She is a life member of Professional bodies, Indian society of Technical Education (ISTE), Computer Society of India (CSI), Association of Computer Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE) and International Association of Engineers (IAENG). She has published more than 25 research articles in Various journals, Web of Science, Springe (Scopus indexed) and SCI, international and National journals and Conferences. Published one Australian and three Indian Patent, and three Copyrights. She actively participated in various faculty development programs and STTPs over the years. For better teaching skills Mission 10X certification is also done.

B. Mohanraj is a seasoned expert in the field of computer science and engineering, with a strong focus on compiler design and optimization. He possesses remarkable proficiency in Compiler Design and a notable research focus in Blockchain technology. Currently, he is a diligent Ph.D. candidate in Information and Communication Engineering at Anna University Chennai, conducting pioneering research on a part-time basis. For over a decade, he has been sharing his extensive knowledge with aspiring minds in the computing field. Presently, he holds a pivotal role as an Assistant Professor in the Department of Information Technology at Sona College of Technology, Salem. Throughout his academic journey, his fervent passion for unraveling intricate programming challenges has driven him to develop innovative solutions that push the boundaries of technology. His exceptional skills were acknowledged by NASSCOM and Anna University, as he achieved the prestigious status of a certified master trainer for the course "Foundation Skills in Product Development". He has made significant strides in disseminating knowledge through scholarly publications. His work has graced the pages of renowned Scopus Indexed International conferences and journals. His legacy as an educator, researcher, and visionary underscores his invaluable contributions to the field of computer science and engineering.

Dr.V.R. Vimal has received his B.E., degree from the Manonmaiam Sundaranar University, Tirunelveli, India in 2005, M.E., degree from Anna University, Chennai, India, in 2007, and Ph.D., degree from Anna University, Chennai, India, in 2022. For past 16 years from 2007, he has worked at different positions like Assistant Professor, Associate Professor, Professor & HOD in various reputed engineering colleges across India. He is currently working as an Professor in the Department of Computer Science and Engineering at Saveetha School of Engineering, SIMATS, Chennai, India. His research interests include Network Security, Image Processing and Machine Learning. He has published more than 20 research articles in various international journals and conference proceedings. He is acting as a reviewer in various national and international journals. He has chaired various international and national conferences. He is a life time member of ISTE and CSI.