International Journal of Basic and Applied Sciences, 14 (4) (2025) 439-444

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/mrn3dh08
Research paper

Performance Analysis of Hybrid Cloud Intrusion Detection Model by Using Supervised Machine Learning Based Classification Algorithms

Mr. D. Rajagopal [1] *, Dr. K. Padmanabhan [2]

[1] *Assistant Professor& Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous)(Affiliated to Periyar University), Tiruchengode, India*
[2] *Professor & Research Supervisor, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous)(Affiliated to Periyar University), Tiruchengode, India*
**Corresponding author E-mail: sakthiraj2782007@gmail.com*

Received: June 23, 2025, Accepted: July 25, 2025, Published: August 15, 2025

Abstract

Cloud Computing refers to an Internet-based infrastructure that delivers shared resources, software, and information to computers and other devices on an on-demand basis. However, it faces numerous security challenges, including issues related to availability, data confidentiality, integrity, and access control. Additionally, Cloud Computing is vulnerable to various conventional attacks. Traditional security systems are inadequate to protect Cloud services from these diverse threats. In the realm of Cloud Computing, Intrusion Detection refers to the identification and management of unauthorized access, harmful actions, and potential security threats. Intrusion Detection Systems (IDS) serve as security mechanisms that monitor network traffic and event logs to detect any anomalous activities. The Cloud Computing (CC) environment necessitates the implementation of specific Intrusion Detection Systems to safeguard each machine from potential attacks. Machine Learning and Deep Learning algorithms enhance the accuracy of Intrusion Detection Systems over time, leading to a decrease in both false positives and false negatives. In the hybrid phase, the implementation of Naïve Bayes and Decision Tree algorithms resulted in an impressive accuracy rate of 99.71%. Future research should explore additional combinations of hybrid models to achieve greater efficiency across all performance metrics.

Keywords: *Cloud IDS; Decision Trees (DT); K-Nearest Neighbors (KNN); Linear Regression (LR); Machine Learning; Neural Networks (NN); Random Forests (RF).*

1. Introduction

Cloud Computing (CC) represents an innovative technology that facilitates the on-demand access to network and computing resources, including storage and data management services. It operates on an Internet-based infrastructure that provides shared resources, software, and information to computers and other devices as needed. The National Institute of Standards and Technology (NIST) have identified five key characteristics of Cloud Computing: On-Demand Self-Service, rapid elasticity, broad network access, resource pooling, and measured service. Additionally, NIST has outlined three "Service Models" (Software, Platform, and Infrastructure) and four "Deployment Models" (Private, Community, Public, and Hybrid) that collectively define the various methods of delivering cloud services.

Cloud computing faces numerous security challenges, including issues related to availability, data confidentiality, integrity, and access control (Gulshan Kumar et.al., 2010; Hanaa Attou et.al., 2023). Additionally, it is vulnerable to a range of conventional attacks, such as Flooding Attacks, Side Channel Attacks, Port Scanning, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks (Omar Achbarou et.al., 2017). Strengthening security measures in the cloud has become a significant concern for service providers. Consequently, various strategies have been implemented, including firewall solutions, data encryption techniques, authentication protocols, and more, to enhance the protection of cloud environments against diverse threats (Gulshan Kumar et.al., 2010). The cloud platform is consistently growing and becoming increasingly integrated into our daily lives, making it essential to create an effective Intrusion Detection Systems (IDS) for this environment as well. Conversely, traditional Intrusion Detection Systems may face challenges when applied within the cloud context. An incursion or attack can be defined as "any series of actions aimed at compromising security objectives." Key security objectives include availability, integrity, confidentiality, accountability, and assurance. Attacks can be classified into four main categories: Probing, Denial of Service, User to Root, and Remote User.

Conventional systems are inadequate for safeguarding Cloud services against various limitations. Consequently, a range of Intrusion Detection methods has been suggested and implemented to identify and thwart unwanted activities in real time. Most of the security measures developed to date for Wireless Sensor Networks (WSNs) focus on packet encryption or necessitate authentication to limit access by malicious users. Additionally, numerous other security solutions for WSNs have been introduced, including authentication, key exchange, and secure routing, aimed at mitigating specific types of attacks.

2. Literature survey

Gulshan Kumar et al. (2010) emphasize the growing need for effective security measures like Intrusion Detection Systems (IDS) due to increased connectivity and threats from malicious users. Their paper reviews various AI-based IDS techniques, highlighting the limited availability of comprehensive studies. It examines IDS based on audit data sources (host, network, or hybrid), detection methods (misuse, anomaly, or hybrid), and classification techniques (single, hybrid, or ensemble). Techniques like Neural Networks, SVM, and feature reduction are discussed to enhance detection speed and accuracy. The study advocates for a hybrid approach to improve attack detection and deepen understanding of AI's role in IDS.

Nabil Ali Alrajeh and J. Lloret (2013) emphasize the importance of Intrusion Detection Systems (IDS) in protecting networks from threats. Their work reviews several IDS techniques, including genetic algorithms, artificial immune systems, and artificial neural networks (ANN). One ANN-based method achieved over 95% accuracy in detecting energy exhaustion attacks, while a genetic algorithm-based system reported a 100% detection rate for denial of service (DoS) attacks. The study highlights the vulnerability of wireless sensor networks (WSNs) and underscores the critical need for robust security solutions.

Omar Achbarou et al. (2017) explore the security challenges in cloud computing, a paradigm that provides on-demand access to shared, configurable resources over the internet. Due to its reliance on resource sharing and networking, cloud environments are particularly vulnerable to security threats. The paper classifies common attacks such as DoS, flooding, and phishing into five categories: security standards, network, access, cloud infrastructure, and data. The study presents a review of these attack types and associated intrusion detection models aimed at mitigating them. The authors propose a layered and integrated Intrusion Detection System (IDS) for cloud environments, which combines knowledge-based and behavior-based analysis to enhance detection capabilities and overall cloud security.

Kanimozhi and Prem Jacob (2019) highlight the use of Artificial Intelligence, particularly Artificial Neural Networks (ANN), in enhancing Intrusion Detection Systems (IDS) for cyber security. Their proposed system targets Bot-net attacks in the financial sector using a dataset from the Canadian Institute for Cyber security. The ANN-based system achieves 99.97% accuracy with a false positive rate of just 0.03%, capable of analyzing both conventional and real-time network traffic. The framework runs on a CPU, with potential performance improvements using tools like TensorFlow and Apache Spark, and can be expanded to detect other types of cyber attacks.

Avinash Appasha Chormale and Arjun Ghatule (2020) propose an enhanced Intrusion Detection System (IDS) called FC-ANN, which integrates Artificial Neural Networks (ANN) with fuzzy clustering. This method addresses the limitations of traditional ANN in handling low-frequency attacks and stability issues. FC-ANN groups training data using fuzzy clustering, trains separate ANN models for each group, and combines their outputs through a fuzzy aggregation module. The system also includes a restore point feature to back up critical data, improving detection efficiency and system stability.

Suryanarayana et al. (2020) propose an AI-based intrusion detection model using the NSLKDD dataset to enhance system security. The model employs feature selection techniques and a firefly algorithm to optimize data and identify key features. A Support Vector Machine (SVM) classifier is used to distinguish between malicious and legitimate nodes, ensuring accurate data routing. The model’s effectiveness is evaluated using Quality of Service (QoS) metrics such as Packet Delivery Ratio, energy consumption, and delay within a CLOUDSIM simulation environment.

Abdel-Rahman Al-Ghuwairi et al. (2023) address the challenge of false positives in Network Intrusion Detection Systems (NIDS) for cloud computing by introducing a time series-based intrusion detection method. The approach combines a feature selection (FS) technique with the Facebook Prophet prediction model to enhance efficiency. Using anomaly detection and causality tests, the method reduces the number of predictors from 70 to 10 while improving performance metrics like Mean Absolute Error. It also significantly cuts down training, prediction, and validation times, lowering resource usage despite similar memory consumption. The study highlights the effectiveness of time series anomaly detection for early intrusion detection in cloud environments, with future work focusing on deeper causal analysis and model comparisons.

Hanaa Attou et al. (2023) address cloud computing security challenges by proposing a cloud-based Intrusion Detection System (IDS) that uses Random Forest (RF) and feature engineering to detect abnormal network activities. The model is designed to monitor cloud resources, services, and traffic for potential attacks. Evaluated on Bot-IoT and NSL-KDD datasets, the model achieves high accuracy 98.3% and 99.99%, respectively. The results demonstrate strong performance in terms of accuracy, precision, and recall, outperforming recent related approaches.

Mohsin Ali et al. (2023) propose a novel intrusion detection approach using Artificial Neural Networks (ANN) for deep packet inspection. Their model, trained on diverse benign and malicious traffic data including files from exploitdb achieves an average accuracy of 99%, an AUC-ROC of 0.99, and a false positive rate below 2% across multiple cross-validations. The approach effectively distinguishes between normal and malicious traffic, showing strong potential for use in both traditional networks and cyber-physical systems like smart grids. Additionally, they introduce an enhanced IDS combining a Multilayer Perceptron (MLP) with Artificial Bee Colony (ABC) optimization and fuzzy clustering. The model is validated using the NSL-KDD dataset and CloudSim, showing superior performance based on metrics such as MAE, RMSE, and the kappa statistic compared to existing methods.

Anupam Rathore and Tripti Sahu (2024) highlight the need for effective intrusion detection systems (IDS) in cloud environments, where traditional IDS often fall short due to increased detection demands. They propose a neural network-based IDS that optimizes resource usage without overloading cloud servers. The study emphasizes feature selection as key to improving anomaly detection accuracy, with Information Gain identified as the most effective method for evaluating data importance. Feature sets 52, 57, and 77 performed well in detecting communication-based threats. Future work will explore additional feature selection strategies to further reduce false positives and enhance security.

Chaimae Saadi et al. (2024) explore the enhancement of cyber security by integrating Artificial Intelligence (AI) into Intrusion Detection Systems (IDS), addressing the shortcomings of traditional IDS in handling modern cyber threats. The study reviews AI-based IDS approaches using machine learning techniques like decision trees and linear regression, applied to datasets such as KDD99 and NSL-KDD. Their proposed architecture uses supervised learning to detect network anomalies, showing improved accuracy, reduced false positives, and better detection of zero-day attacks. The research emphasizes the importance of quality data, continuous model refinement, and suggests future work on real-time adaptive AI systems for stronger threat detection.

Kalpana Verma (2024) addresses the growing cyber security challenges in an increasingly connected world, highlighting the need for effective intrusion detection systems (IDS), especially in cloud environments. Traditional IDS may strain cloud servers, prompting the proposal of a neural network-based IDS that uses machine learning to detect emerging threats efficiently. The study investigates the impact of feature selection on anomaly detection accuracy, identifying Information Gain as the most effective method. Feature sets 52, 57, and 77 also performed well with the J48 classifier, helping to reduce false positives. Future research will explore additional feature selection techniques to further improve detection performance.

Muhammad Sajid et al. (2024) present a hybrid intrusion detection model combining machine learning and deep learning techniques to address rising security threats from increased network data due to cloud computing and IoT. The model uses XGBoost and convolutional neural networks (CNN) for feature extraction and long short-term memory (LSTM) networks for classification. Trained on four datasets, the model outperforms traditional IDS by achieving high detection rates and a low False Acceptance Rate. However, challenges remain in reducing training time and improving detection of minority classes, which will be the focus of future research.

Nishtha Singh (2024) highlights the growing need for effective network security due to increasing online threats and the widespread use of cloud platforms. Traditional Intrusion Detection Systems (IDS) often struggle in cloud environments due to high resource demands. To address this, a neural network-based IDS using machine learning is proposed to efficiently detect emerging threats without overloading cloud servers. Experiments show that feature selection significantly affects anomaly detection accuracy, with Information Gain identified as the most effective method for certain feature sets, and J48 performing well with others. Future research will focus on refining feature selection techniques and analyzing the impact of specific feature subsets on threat detection.

Salman Muneer et al. (2024) examine various modern approaches to intrusion detection (ID), including machine learning (ML), deep learning (DL), federated learning (FL), and explainable AI (XAI). DL offers high accuracy but requires extensive labeled data and computing power, while ML is more resource-efficient but less effective against unknown threats. FL enables collaborative model training without sharing data, enhancing privacy but demanding more communication and computation. XAI improves transparency by making AI decisions understandable. The paper highlights the lack of detailed guidance on when each method is most suitable and seeks to fill this gap by providing recommendations based on factors like network size, data availability, and privacy needs. Organizations are advised to choose ID techniques according to their specific requirements.

Vadetay Saraswathi Bai and Sudha (2024) address the security challenges in cloud computing by enhancing intrusion detection systems (IDS) through dimensionality reduction techniques. Using Principal Component Analysis (PCA) and Singular Value Decomposition (SVD), they reduce feature complexity to improve accuracy and speed in cloud forensics. Tested on the UNSW-NB15 dataset, their deep learning-based IDS particularly the proposed 1D-CNN NIDCNN model achieved 100% accuracy with low processing requirements. The study demonstrates that combining PCA and SVD with deep learning significantly boosts real-time intrusion detection performance in cloud environments.

Zhiyan Chen et al. (2024) propose a hybrid intrusion detection system that combines Network-based (NIDS) and Host-based (HIDS) approaches to address challenges in detecting Advanced Persistent Threats (APT) and encrypted traffic. The system uses BERT, a language processing model, to convert host data (like logs and files) into numerical form for analysis alongside network data. A two-stage collaborative classifier employing both binary and multi-class learning enhances detection accuracy. Compared to the baseline XGBoost model, the proposed system shows improved performance, particularly in detecting specific types of attacks.

Anuja Beatrice and Aasheka (2025) propose an AI-driven Intrusion Detection System using machine learning and deep learning models (Random Forest, SVM, LSTM, CNN-LSTM) to improve threat detection. Their approach shows higher accuracy and fewer false positives than traditional IDS, with future work focusing on performance optimization and potential block chain integration for enhanced security.

Tirumala Ashish Kumar Manne (2025) explores the role of AI in addressing security challenges in hybrid cloud environments. The study highlights how AI techniques like machine learning and predictive analytics enhance threat detection, automate responses, and improve threat intelligence. While AI offers real-time, accurate threat identification, it also introduces challenges such as vulnerability to attacks, ethical concerns, and high computational demands. The paper compares AI-based and traditional security approaches and recommends combining AI with human expertise for more effective cyber defense.

Usama Ahmed et al. (2025) focus on improving network security through machine learning and deep learning-based intrusion detection systems. The study evaluates models such as SVM, KNN, Random Forest, Decision Tree, LSTM, and ANN. Results show that SVM and Random Forest perform well overall, making them suitable for IDS use, while LSTM and ANN are effective in detecting complex intrusions.

3. Intrusion detection system in cloud

Cloud Computing refers to an Internet-based infrastructure that provides shared resources, software, and information to computers and other devices on an on-demand basis. The Internet serves as a conduit for accessing the services offered by the Cloud, which also represents a significant source of threats that can compromise Cloud systems and resources. Within the realm of Cloud Computing, Intrusion Detection involves identifying and responding to unauthorized access, malicious actions, and security vulnerabilities. Intrusion constitutes any unauthorized activity that may threaten the confidentiality, integrity, and availability of information. An Intrusion Detection System is an advanced mechanism designed to monitor network traffic and identify anomalous activities, while also generating alerts when such activities are detected within systems.

An Intrusion Detection System is designed to monitor and analyze data in order to detect potential intrusions into a system or network. Due to the vast volume, diversity, and rapid generation of data within networks, conventional methods for identifying network attacks have become increasingly complex. IDS are security mechanisms that monitor network traffic and event logs to pinpoint suspicious activities. Traditionally, these systems depend on established rules to recognize known attack patterns. In a Cloud Computing environment, it is essential to implement various Intrusion Detection Systems to safeguard each machine from potential attacks. Conversely, while firewalls are employed by Cloud providers to detect intrusions, this technology is limited in its ability to identify insider threats.

4. Machine learning for ids

Machine Learning (ML) based Intrusion Detection Systems are increasingly gaining traction. This study presents an Intrusion Detection System that leverages Cloud Computing and distributed Machine Learning. The edge network components of cloud providers will be integrated with the proposed Cloud system. The methodology for data collection and storage facilitates the distinction between two categories of IDS: Host-based IDSs, which collect data from a host. For the purposes of this research, the dimensionality of the features was reduced through Principal Components Analysis (PCA). The integration of these two approaches may yield low-dimensional features suitable for developing classifiers such as Bayesian networks, Random Forests, Linear Discriminant Analyses (LDA), and Quadratic

Discriminant Analyses (QDA). Machine learning algorithms possess the capability to analyze extensive datasets and detect patterns and anomalies that may signify security breaches, thereby serving as essential instruments for maintaining the security and integrity of cloud-based systems and applications. Furthermore, Machine Learning and Deep Learning algorithms enhance the performance of intrusion detection systems by improving accuracy over time, which in turn minimizes both false positives and false negatives. Deep Learning, a subset of Machine Learning, focuses on learning data representations and is primarily driven by algorithms based on artificial neural networks. Among the most recognized supervised learning algorithms are k-nearest neighbors (KNN), decision trees (DT), linear regression (LR), neural networks (NN), and random forests (RF). A classification-based machine learning approach is employed to identify Distributed Denial of Service attacks in cloud computing, utilizing three methods: KNN, RF, and naive Bayes (NB).

5. Research work

In the proposed study aimed at detecting intrusions in cloud environment, machine learning-based supervised learning algorithms, including Naïve Bayes, Decision Tree, k-nearest neighbor, and Linear Regression, have been applied to the dataset for classifying users as either Anomalous or Normal. The analysis utilized a Kaggle dataset which comprising 17,634 records which includes duration, source bytes, destination bytes, number of failed login, number of login, number of login compromised, root shell, number of roots, number of files creation, number of files access, is host login, error rate, destination host count, destination host server difference, destination host same source port rate, destination host difference server rate, protocol type, accessing mode, IP, flag, service, port id, file process id, accessing time etc.. The testing and evaluation process was divided into three distinct phases: Individual Evaluation Phase, Individual Testing Phase, and Hybrid Phase analysis.

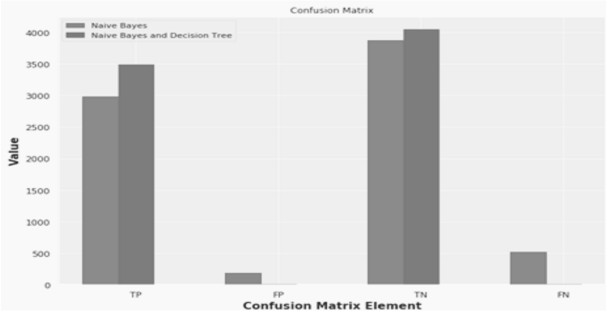
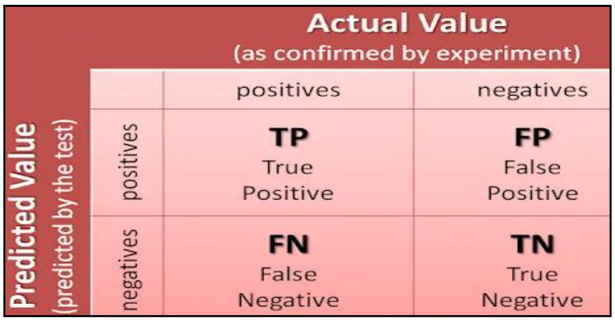


Fig. 1: Confusion Matrix Analysis between Naïve Bayes and Proposed Hybrid Model.

The Naïve Bayes algorithm demonstrated strong performance with high dimensional data, exhibiting rapid processing and enhanced efficiency. The Decision Tree algorithm was employed to manage both numerical and categorical data. Consequently, in the Hybrid Phase, both Naïve Bayes and Decision Tree algorithms were utilized. Table 1 presents an analysis of the evaluation and testing phase datasets. In that, the cross-validation is a method for evaluating a machine learning model's performance on unseen data by repeatedly splitting the data into training and testing sets. It provides a more accurate performance estimate by averaging results across multiple iterations. The advantages are reduces over-fitting, helps in model selection, useful for hyper-parameter tuning and makes efficient use of data and the disadvantages are computationally expensive, time-consuming and involves bias-variance tradeoff. A confusion matrix is a table used to evaluate the performance of a classification model by summarizing the number of correct and incorrect predictions for each class. During the Individual Evaluation Phase, the classifiers DT, KNN, and LR achieved accuracies of 100%, 99.37%, and 95.46%, respectively. In the Individual Testing Phase, the accuracies for DT, KNN, and LR were 99.47%, 99.16%, and 95.55%, respectively. The Hybrid Phase yielded an accuracy of 96.87% from the combined classifiers NB+DT. Figure 1 illustrates the Confusion Matrix Element Analysis comparing Naïve Bayes with the Proposed Hybrid Model and Figure 2 describes the structure of Confusion Matrix. The Figure 1 describes the Naïve Bayes algorithm produced values during testing phase. The values of TP, FP, TN and FN are 2981, 188, 3872 and 517 respectively. Along this value the hybrid phase values are displayed as a bar chart for making the view of performance efficiency. During the hybrid phase the values of TP, FP, TN and FN are 3498, 13, 4047 and 9 respectively.



Predicted Value (predicted by the test)	Actual Value (as confirmed by experiment)	
	positives	negatives
positives	**TP** True Positive	**FP** False Positive
negatives	**FN** False Negative	**TN** True Negative

Fig. 2: Structure of Confusion Matrix.

6. Performance analysis

The performance analysis of the model involves identifying key parameters such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). The metrics for performance analysis are categorized into five distinct types: (i) Accuracy, (ii) Misclassification, (iii) Precision, (iv) Sensitivity also known as Recall, and (v) Specificity. A total of 7,558 records have been utilized in the model for this analysis.

Table 2 provides a detailed overview of the performance analysis for the proposed Hybrid Cloud Intrusion Detection System (IDS) model. In addition, Fig. 3 illustrates the comparative performance metrics between the existing model and the proposed Hybrid model.
The Accuracy has been computed by using

Accuracy (all correct/all) = TP+TN/TP+TN+FP+FN (1)

The Misclassification has been computed by using

Misclassification (all incorrect/all) = FP+FN/TP+TN+FP+FN (2)

The Precision has been computed by using

Precision (TPs/predicted positives) = TP/TP+FP (3)

The Sensitivity has been computed by using

Sensitivity aka Recall (TPs/all actual positives) = TP/TP+FN (4)

The Specificity has been computed by using

Specificity (TNs/ all actual negatives) =TN/TN+FP (5)

Table 1: Evaluation and Testing Phase Dataset Analysis

Algorithm	Intrusion	Precision	Recall	F1-Score	Support	Confusion Matrix	Cross Validation Mean Score	Model Accuracy
Individual Evaluation Phase Analysis								
NB Classifier	Anomaly	0.95	0.85	0.9	8245	[[7000 1245]	0.9072	0.9072
	Normal	0.88	0.96	0.92	9389	[392 8997]]		
DT Classifier	Anomaly	1	1	1	8245	[[8245 0]	0.9960	1
	Normal	1	1	1	9389	[0 9389]]		
KNN Classi-	Anomaly	1	0.99	0.99	8245	[[8168 77]	0.9914	0.9937
fier	Normal	0.99	1	0.99	9389	[33 9356]]		
LR	Anomaly	0.96	0.94	0.95	8245	[[7757 488]	0.9539	0.9546
Classifier	Normal	0.95	0.97	0.96	9389	[313 9076]]		
Individual Testing Phase Analysis								
NB Classifier	Anomaly	0.94	0.85	0.89	3498	[[2981 517]	-	0.9067
	Normal	0.88	0.95	0.92	4060	[188 3872]]		
DT Classifier	Anomaly	0.99	1	0.99	3489	[[3483 15]	-	0.9947
	Normal	1	0.99	1	4060	[25 4035]]		
KNN Classi-	Anomaly	0.99	0.99	0.99	3498	[[3458 40]	-	0.9916
fier	Normal	0.99	0.99	0.99	4060	[23 4037]]		
LR	Anomaly	0.96	0.94	0.95	3498	[[3298 200]	-	0.9555
Classifier	Normal	0.95	0.97	0.96	4060	[136 3924]]		
Hybrid Phase Analysis								
NB + DT	Anomaly	0.98	0.98	0.98	517	[[508 9]	-	0.9687
Classifier	Normal	0.95	0.93	0.94	188	[13 175]]		

Table 2 : Performance Analysis of Proposed Model

Classification Model	TP	FP	TN	FN	Accuracy	Misclassification	Precision	Sensitivity	Specificity
Individual Testing Phase Performance Analysis									
NB Classifier	2981	188	3872	517	0.9067	0.0933	0.9407	0.8522	0.9537
DT Classifier	3483	25	4035	15	0.9947	0.0053	0.9929	0.9957	0.9938
KNN Classifier	3458	23	4037	40	0.9917	0.0083	0.9934	0.9886	0.9943
LR Classifier	3298	136	3924	200	0.9555	0.0445	0.9604	0.9428	0.9665
Hybrid Phase Performance Analysis									
NB - > DT Classifier	508	13	175	9	0.9688	0.0312	0.9750	0.9826	0.9309
NB + DT Classifier	3498	13	4047	9	0.9971	0.0029	0.9963	0.9974	0.9968

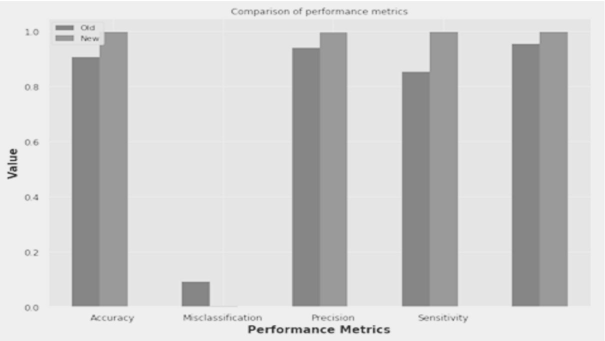


Fig. 3: Performance Metrics Analysis between Existing and Proposed Hybrid Model.

7. Result and discussion

Cloud Computing (CC) represents an innovative technology that facilitates on-demand access to network and computing resources, including storage and data management services. However, it faces numerous security challenges, such as issues related to availability, data confidentiality, integrity, and access control. Traditional security systems are inadequate for safeguarding cloud services against various threats. Consequently, a range of intrusion detection strategies have been proposed and implemented to identify and mitigate undesirable activities in real time.

The cloud computing environment necessitates the deployment of intrusion detection systems (IDSs) to protect each machine from potential attacks. Typically, an intrusion detection system operates in a predetermined manner, regardless of the chosen implementation mechanism. A limited number of studies have addressed the intrusion detection challenge by framing it as a time series problem, which requires time series modeling techniques. In the proposed study aimed at detecting intrusions in cloud environments, various machine learning-based supervised learning algorithms, including Naïve Bayes, Decision Tree, k-nearest neighbor, and Linear Regression, have been applied to the dataset to classify users as either Anomalous or Normal. The analysis utilized a Kaggle dataset containing 17,634 records. The testing and evaluation process consisted of three distinct phases: Individual Evaluation Phase analysis, Individual Testing Phase analysis, and Hybrid Phase analysis.

During the Individual Evaluation phase, the classifiers DT, KNN, and LR achieved accuracies of 100%, 99.37%, and 95.46%, respectively. In the Individual Testing phase, the accuracies for DT, KNN, and LR were recorded at 99.47%, 99.16%, and 95.55%, respectively. The hybrid phase yielded an accuracy of 96.87% with the NB+DT classifiers. When conducting the performance analysis using various metrics, the DT classifier, KNN classifier, and LR classifier demonstrated accuracies of 99.47%, 99.17%, and 95.55% in the individual testing phase. In the hybrid phase, the NB+DT classifier achieved an accuracy of 99.71%. Limitation of this research is that the selected supervised machine learning algorithms only used to analysed the models efficiency and Deep learning algorithms, Unsupervised algorithms and Reinforcement algorithms like dimensionality reduction, association rule, model based method, model free method has not used in this research. Future research should explore additional combinations of hybrid models like RF, CNN, RNN, ANN, LSTM, DBSCAN, Markov model to enhance efficiency across all metrics.

References

[1] Gulshan Kumar, Krishan Kumar, Monika Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: a review", Artif Intell Rev, pp: 1-20, 2010. https://doi.org/10.1007/s10462-010-9179-5.

[2] Nabil Ali Alrajeh and J. Lloret, "Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, pp: 1-6, 2013. https://doi.org/10.1155/2013/351047.

[3] Omar Achbarou, My Ahmed El kiram, and Salim El Bouanani, "Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems", International Journal of Interactive Multimedia and Artificial Intelligence, Vol. 4, No3, pp: 61-64, 2017. https://doi.org/10.9781/ijimai.2017.439.

[4] Kanimozhi, Prem Jacob, "Artifcial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing", ICT Express, 5, pp: 211-214, 2019. https://doi.org/10.1016/j.icte.2019.03.003.

[5] Avinash Appasha Chormale, Arjun Ghatule, "Cloud Intrusion Detection System Using Fuzzy Clustering and Artificial Neural Network", International Conference on Future of Engineering Systems and Technologies & Journal of Physics: Conference Series, 1478, pp: 1-14, 2020, https://doi.org/10.1088/1742-6596/1478/1/012030.

[6] Suryanarayana, Jagadeesh, Vanamala Kumar, Musala Venkateswara Rao, "Artificial Intelligence Based Intrusion Detection Analysis Using Cloud Computing", Journal of Critical Reviews, Vol. 7, No.18, pp: 32-36, 2020.

[7] Abdel-Rahman Al-Ghuwairi, Yousef Sharrab, Dimah Al-Fraihat, Majed AlElaimat, Ayoub Alsarhan and Abdulmohsen Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning", Journal of Cloud Computing, pp:12-17, 2023. https://doi.org/10.1186/s13677-023-00491-x.

[8] Hanaa Attou, Azidine Guezzaz, Said Benkirane, Mourade Azrour, and Yousef Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques", Big Data Mining and Analytics, Vol.6, No.3, pp: 311-320, September 2023. https://doi.org/10.26599/BDMA.2022.9020038.

[9] Mohsin Ali, Abdul Razaque, Damelya Yeskendirova, Talgat Nurlybayev, Nessibeli Askarbekova and Zarina Kashaganova, "Enhancing Cloud Computing Security through AIBased Intelligent Intrusion Detection Leveraging Neural Networks and Artificial Bee Colony Optimization", Proceedings of the 8th International Conference on Digital Technologies in Education, Science and Industry, pp: 1-13, 2023.

[10] Anupam Rathore, Tripti Sahu, "AI-Based Intrusion Detection System in Cloud Computing", International Journal of Innovative Research in Computer Science & Technology, Vol. 12, Special Issue. 1, pp: 45-51, March-2024. https://doi.org/10.55524/CSISTW.2024.12.1.8.

[11] Chaimae Saadi, Imane Daha Belghiti, Souad Atbib, Tarek Radah, "Contribution to Threat Management through the use of AI based IDS", RGSA– Revista de Gestão Social e Ambiental, Vol.18, No.10, pp:1-20, 2024. https://doi.org/10.24857/rgsa.v18n10-096.

[12] Kalpana Verma, "AI-Based Intrusion Detection System in Cloud Computing", Journal of Emerging Technologies and Innovative Research, Vol. 11, No. 4, pp: 254-259, 2024.

[13] Muhammad Sajid, Kaleem Razzaq Malik, Ahmad Almogren, Tauqeer Safdar Malik, Ali Haider Khan, Jawad Tanveer and Ateeq Ur Rehman, "Enhancing intrusion detection: a hybrid machine and deep learning approach", Journal of Cloud Computing: Advances, Systems and Applications, Vol. 13, No.123, pp: 1-24, 2024. https://doi.org/10.1186/s13677-024-00685-x.

[14] Nishtha Singh, "Artificial Intelligence Based Intrusion Detection System for Cloud Computing", International Journal for Research in Applied Science & Engineering Technology, Vol. 12, No. 3, PP: 1- 11, March 2024. https://doi.org/10.22214/ijraset.2024.58920.

[15] Salman Muneer, Umer Farooq, Atifa Athar, Muhammad Ahsan Raza, Taher Ghazal, Shadman Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis", Journal of Engineering, pp: 1-16, 2024. https://doi.org/10.1155/2024/3909173.

[16] Vadetay Saraswathi Bai, Sudha, "Deep Learning Inspired Intelligent Framework to Ensure Effective Intrusion Detection in Cloud", International Journal of Intelligent Systems and Applications in Engineering, Vol. 12, No. 14s, pp: 441–456, 2024.

[17] Zhiyan Chen, Murat Simsek, Burak Kantarci, Mehran Bagheri, Petar Djukic, "Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier", Computer Networks, 250, pp: 1-15, 2024. https://doi.org/10.1016/j.comnet.2024.110576.

[18] Anuja Beatrice, Aasheka , "AI-Powered Intrusion Detection Systems for Secure Network Communication", International Research Journal of Education and Technology, Vol. 7, No. 3, pp: 1945-1950, 2025. https://doi.org/10.34218/IJAIML_04_01_011.

[19] Tirumala Ashish Kumar Manne, "Artificial Intelligence in Hybrid Cloud Security: Enhancing Threat Detection and Response", International Journal of Artificial Intelligence & Machine Learning, Vol. 4, No. 1, January-June 2025, pp. 144-157, https://doi.org/10.1038/s41598-025-85866-7.

[20] UsamaAhmed, Mohammad Nazir, Amna Sarwar, TariqAli, El-Hadi M.Aggoune, Tariq Shahzad & Muhammad Adnan Khan, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering", Scientific Reports, 15,1726, pp:1-33, 2025. https://doi.org/10.1038/s41598-025-85866-7.