IRJCS: International Research Journal of Computer Science
Volume 12, Issue 05, May 2025
ISSN: 2393-9842
https://www.irjcs.com/archives

An Artificial Intelligence Algorithm to Enhance Cloud Computing Network Security

Rishav Raj,Deepak Mangal,Ritik Raj,Raza Karim
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India
rrishav258@gmail.com, deepakmangal.it@gniot.net.in
ritikrajverma1235@gmail.com, razakarim351@gmail.com
Dr.Vikas Singhal
Professor & Head, Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India
hodit@gmail.com

Publication History
Manuscript Reference: IRJCS/RS/Vol.12/Issue05/MYCS10084|ResearchArticle | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.12/Issue05/MYCS10084 Received: 26, April 2025, Revised: 02, May 2025 Accepted: 12 May 2025 Published Online: 15 May 2025 http://www.irjcs.com/volumes/Vol12/iss-05/05.MYCS10084.pdf
Article Citation: Dr.Vikas,Rishav,Deepak,Ritik,Raza(2025), An Artificial Intelligence Algorithm to Enhance Cloud Computing Network Security IRJCS: International Research Journal of Computer Science, Volume 12, Issue 04 of 2025 pages 221-228 **doi:>** https://doi.org/10.26562/irjcs.2025.v1205.05
BibTeX Dr.Vikas@2025Artificial

Copyright: ©2025 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: Cloud computing has transform data storage and processing, but its dynamic and distributed nature poses significant security challenges. This paper introduces an Artificial Intelligence (AI) algorithm specifically designed to enhance network security within cloud computing environments. The proposed algorithm employs advanced Machine Learning (ML) techniques to track network activity, detect anomalies, and react instantly to possible threats. By constant learning from new data, the system evolves the ability to accurately detect known and unknown attack patterns. Comparing the algorithm to more conventional security techniques, experimental assessments show how well it reduces false positives and speeds up response times. This study demonstrates how AI-driven solutions may be used to create proactive and flexible defenses Intrusion Detection system (IDS), guaranteeing a cloud infrastructure that is more secure and robust.

Keywords: Cloud Computing, Network Security, Artificial Intelligence (AI), Machine Learning (ML), Anomaly Detection, Intrusion Detection, Cybersecurity.

1. INTRODUCTION

Cloud computing has risen as a foundational innovation within the computerized age, empowering on-demand get to a common collection of configurable computing resources, including servers, networks, storage, applications, and services [1]. It offers unparalleled adaptability, versatility, and cost-efficiency, making it an fundamental component in modern IT infrastructures over sectors including finance, healthcare, education, and government[2]. However, alongside these benefits, cloud computing also presents critical security challenges. Due to its distributed nature, multi-tenancy, and dependence on virtualized resources, cloud networks are defenseless to a wide range of cyber threats such as information breaches, Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and unauthorized access [3]. Conventional security mechanisms often rule-based and static struggle to manage with the dynamic and quickly evolving threat scene of cloud environments. These conventional methods are generally receptive in nature and come up short to detect novel or zero-day attacks, leading to increased risk exposure [6].

Furthermore, more intelligent, versatile, and real-time security solutions are needed due to the immense amount and diversity of information created in cloud systems. In this setting, Artificial Intelligence (AI), and Machine Learning (ML), presents a promising road for enhancing cloud network security. Artificial Intelligence (AI) algorithms can learn from historical data and real-time information to identify anomalies, classify threats, and predict future attacks. Unlike conventional systems, AI-driven models are able of adapting to modern patterns and behaviors, making them highly effective in managing advanced and previously unseen cyber threats. This research focuses on the design and implementation of a novel AI algorithm pointed at strengthening the security posture of cloud computing networks. By integrating supervised learning for known threat detection with unsupervised learning for anomaly detection, the suggested technique employs a hybrid methodology. By persistently analyzing network traffic, client behavior, and system logs, the algorithm independently recognizes and mitigates security threats with high accuracy and negligible latency. Also, the framework incorporates a reinforcement learning mechanism that permits it to improve over time by learning from past decisions and results [12].

The following are the primary contributions of this study:

Advancement of a comprehensive AI-based framework for cloud network threat detection and response in real time. Integrating various machine learning methods to enhance detection accuracy and reduce false positives. Validation of the proposed algorithm through experiments on benchmark datasets and recreated cloud environments.

Comparative analysis with existing security models to illustrate performance enhancements.

Key highlights of the proposed algorithm incorporate:

Real-time anomaly detection: Utilizing unsupervised learning models like clustering and auto encoders to identify deviations from ordinary behavior.

Threat classification: Applying techniques that use supervised learning to accurately categorize known threats, such as decision trees, support vector machines (SVM), or neural networks.

Adaptive learning: Incorporating reinforcement learning to permit the system to evolve and enhance its performance over time based on criticism.

Scalability: Designing the system to handle large-scale data typical of cloud environments

2. LITERATURE REVIEW

Cloud computing has become a core infrastructure for present day businesses and organizations, giving scalable capacity, high availability, and on-demand services. However, its complex and distributed architecture introduces critical security risks such as denial-of-service attacks, data breaches, and illegal access. Modern and dynamic attacks are frequently too difficult for traditional security measures like firewalls and rule-based intrusion detection systems to manage in real time. This has driven the research community toward more intelligent, versatile solutions—particularly those based on artificial intelligence (AI). Through intelligent threat detection, anomaly recognition, and automated responses, artificial intelligence (AI) shown immense potential in tackling cloud security challenges. To categorize network traffic and detect intrusions, machine learning (ML) algorithms including Support Vector Machines (SVM), Decision Trees, and Random Forests have been widely used. Large datasets can be used to train these models to recognize anomalous activity and alert about potential threats. In any case, numerous conventional ML models require extensive feature engineering and are restricted in handling the complexity of real-world network data.

Artificial intelligence (AI) plays an essential role in the safety of the cloud, automatic learning expression, deep learning and techniques for enhanced learning.

- Machine learning to build models to detect security threats based on historical data.
- Deep Learning allows for advanced security threats by extracting complex data features using multi-layer neural networks.
- Reinforcement Learning is utilized to refine security strategies through continuous interaction, smart and environmental agents.

AI approach methods effectively handle data large features, automation of main characteristics and establish nonlinear mapping relationships, which make them very effective to detect anomalies, recognize malicious software and predict security posture. Therefore, AI provides a powerful technical facility to improve cloud safety A subset of artificial intelligence called deep learning (DL) has made major strides by automatically extracting hierarchical characteristics from unprocessed input data. Cloud network traffic has been subjected to models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), with promising results.These models exceed expectations in identifying complicated patterns and offer higher accuracy in recognizing malicious behavior. However, deep learning (DL) models frequently request enormous computing capacity and large labeled datasets, which can limit their applicability in certain cloud environments [15]. Hybrid and ensemble AI approaches are gaining popularity for combining the qualities of numerous algorithms. These models aim to improve detection performance, decrease false positives, and enhance strength against evolving cyber threats [11]. In addition, reinforcement learning (RL) has been explored for developing versatile defense strategies. RL models can learn optimal responses to threats through continuous interaction with the environment, making them suitable for dynamic cloud scenarios. Despite their advantages, AI-based solutions also confront challenges such as data privacy; explain ability, model transparency, and vulnerability to malicious attacks. In recent years, analysts have started exploring explainable AI (XAI) and federated learning to address a few of these limitations. XAI enhances trust by making AI decisions interpretable to human users, while federated learning permits models to be trained over decentralized data sources without sharing sensitive data. These developments represent the following step in building secure and intelligent cloud infrastructures. In general, the integrating the AI into cloud computing security offers a promising avenue for innovation but it requires careful design to balance accuracy, efficiency, and transparency.

3. METHODOLOGY

The methodology adopted to develop and evaluate an artificial intelligence (AI) algorithm designed for enhancing network security in cloud computing environments is explained in this section. The suggested approach use of machine learning (ML) techniques to identify patterns, detect anomalies, and react quickly to potential security threats [1][2]. The methodology encompasses data collection, preprocessing, model development, training, testing, and performance assessment.

The methodology consists of the following stages:

3.1 Data Collection

To construct a robust and representative dataset, network traffic data was sourced from both publicly available cyber security repositories and simulated cloud computing environments.

The AI algorithm was trained and validated using two publicly accessible datasets:

- NSL-KDD Dataset: An extensively used benchmark dataset for intrusion detection system evaluation. It encompasses a number of cyberattack types, including user-to-root (U2R), denial-of-service (DoS), and probing attacks [14].

ISSN: 2393-9842
https://www.irjcs.com/archives

- CICIDS2017 Dataset: This dataset offers labeled examples of contemporary attack types, such as brute-force, infiltration, and botnet operations, together with realistic network traffic data[12]. In addition, personalized traffic has been created in a virtual cloud environment with platforms such as Open Stack and Docker, capturing a variety of attacks, including denial of services (DoS), SQL Injection and Brute Force Attacks.

3.2 Data Preprocessing

Prior to model training, the dataset undergoes several essential preprocessing steps to ensure data quality and enhance model performance:

- **Data Cleaning**: The dataset is examined for inconsistencies such as missing values, redundant entries, and outliers. These anomalies are addressed or removed to maintain data integrity and reliability [5][13].

Fig. 1 Data Cleaning

- **Encoding**: Categorical features such as protocol types or service identifiers are transformed into numerical representations using techniques like label encoding or one-hot encoding, facilitating their compatibility with machine learning (ML) algorithms.
- **Normalization**: To ensure that numerical features contribute equally to the model's learning process, Min-Max normalization is applied. This scales all values to a common range, typically [0][1], accelerating convergence during training.
- **Feature Selection**: To identify and maintain the most informative characteristics, dimensionality reduction techniques like Principal Component Analysis (PCA) and correlation analysis are utilized. This minimizes computing complexity and enhancing model accuracy.

3.3 Algorithm Design

To improve cloud computing network security, the suggested AI-based security model utilizes an extensive hybrid architecture that combines supervised learning, unsupervised learning, and deep learning (DL):

3.3.1 Supervised Learning: In the proposed AI-based security framework, Supervised Learning plays a important role in accurately detecting and classifying known cyberat tacks in cloud computing environments. Supervised learning involves training the models on labeled datasets, where each data instance (e.g., a network packet or flow) is associated with a known outcome or class (such as "normal" or a specific type of attack). Cloud computing networks are exposed to a broad range of well-documented cyber threats like DDoS attacks, SQL injections, brute force attempts, and more[3][5]. These threats often exhibit identifiable patterns in network traffic. Supervised learning algorithms excel at recognizing these patterns and making precise classifications once trained on sufficient examples.

Random Forest (RF): An effective ensemble learning system called Random Forest (RF) builds several decision trees and combines their results to improve classification accuracy. It is useful for network intrusion detection because it utilizes majority voting to classify data and performs effectively with high-dimensional data. In the proposed AI-based cloud security framework, RF is employed as a core supervised learning model to classify known cyber threats using labeled data from benchmark datasets such as NSL-KDD and CICIDS2017. Features are extracted from packet- and flow-level information to capture diverse traffic patterns. RF serves as a first-line defense within hybrid architecture, delivering fast and reliable classifications that support deeper anomaly analysis by subsequent layers. It is appropriate for real-time intrusion detection in dynamic cloud systems because of its integration, which guarantees a balance between interpretability, efficiency, and detection accuracy [3][6].

Support Vector Machine (SVM): In high-dimensional feature spaces, Support Vector Machines (SVM) is efficient supervised learning algorithms that are seeking to determine the best hyper plane for maximizing the distance between classes. In binary classification tasks, SVM maximizes the margin between classes, ensuring high generalization. Within the proposed AI-based framework for cloud computing security, using structured, labeled data from datasets like NSL-KDD and CICIDS2017, SVM is employed to identify network traffic as either benign or malicious.

IRJCS: ©2014-25, AM Publications, India - All Rights Reserved https://doi.org/10.26562/irjcs

ISSN: 2393-9842
https://www.irjcs.com/archives

The model is trained on normalized feature vectors and integrated into the hybrid architecture to perform initial classification of known attack types. SVM's deterministic nature and precision make it suitable for real-time threat detection in security-critical environments. Although it may be less effective against unknown threats, its role in the framework enhances early detection accuracy and supports deeper analysis by complementary models [10].

Gradient Boosting (GB): Gradient Boosting (GB) is an advanced ensemble learning technique that constructs a strong classifier by sequentially adding weak learners, typically decision trees, each correcting the residual errors of its predecessors. This iterative process enhances both accuracy and generalization performance [5][11]. In the proposed AI-based cloud security framework, GB is utilized to capture complex, non-linear relationships in network traffic data. Trained on feature-engineered datasets such as NSL-KDD and CICIDS2017, GB improves detection precision by modeling subtle interactions between traffic features and attack types. Within the hybrid architecture, GB serves as a performance refinement layer. Its outputs are either used directly for threat alerts or integrated with other classifiers like Random Forest and SVM to boost overall reliability. GB's high accuracy and adaptability make it a key component for robust intrusion detection in cloud environments.

3.3.2 Unsupervised Learning:

Unsupervised learning techniques play a critical role in detecting anomalous or zero-day attacks in cloud computing environments by uncovering deviations from normal traffic patterns without the need for labeled data[8][9]. Unlike supervised learning, which relies on previously labeled examples of attacks and normal behavior, unsupervised learning methods attempt to identify novel or unknown attack types by analyzing the intrinsic structure of network traffic. In the context of the proposed AI-driven security framework, unsupervised learning algorithms such as k-Means Clustering and Isolation Forest are utilized to complement traditional supervised models, making it possible to identify zero-day attacks, or attacks that have never been seen before and for which there is no tagged data.

K-Means Clustering: k-Means is a popular unsupervised learning approach that minimizes within-cluster variance to divide data into k clusters. It iteratively adjusts cluster centroids based on feature similarity, enabling efficient grouping of high-dimensional data [4][9]. In the proposed cloud security framework, k-Means is applied to normalized network traffic data preprocessed using features such as packet size, duration, IP addresses, and protocol type to model normal traffic behavior. Data points that significantly deviate from established clusters are flagged as anomalies, indicating potential zero-day attacks or novel threats. These anomalies are then forwarded to other components of the hybrid AI system, including supervised or deep learning models, for further analysis. This layered integration enhances the framework's ability to detect both known and emerging threats in real time, improving adaptability and responsiveness in cloud-based intrusion detection systems.

Isolation Forest: The purpose of the ensemble-based anomaly detection technique Isolation Forest is to recursively partition data in order to separate outliers. Unlike traditional methods that model normal behavior, it focuses on identifying instances that are few and different, making it ideal for datasets with multiple dimension, such network traffic. In the proposed AI-based cloud security framework, Isolation Forest is employed to detect anomalous traffic patterns by isolating data points that deviate significantly from the norm. This allows the system to identify novel or evolving threats, including zero-day attacks, without requiring labeled data[6][14]. Its computational efficiency and scalability make it ideal for real-time monitoring in dynamic cloud environments. As part of the hybrid architecture, Isolation Forest enhances the framework's ability to uncover hidden threats beyond the capabilities of conventional supervised models.

3.3.3 Deep Learning Architectures:

Convolutional Neural Networks (CNNs): The group of deep learning models known as Convolutional Neural Networks (CNNs) was created especially to identify spatial hierarchies in received data. CNNs' potential to automatically discover spatial correlations between input variables has allowed them to perform well in network traffic analysis, despite their initial development for image processing [12]. In the proposed AI-based cloud security framework, CNNs are utilized to extract meaningful spatial patterns from structured network traffic representations, such as traffic flow matrices or feature maps derived from packet metadata. These learned representations facilitate the detection of localized attack signatures and variations, enabling the system to identify threats that exhibit spatial consistency across network sessions. The convolutional layers act as feature extractors, reducing reliance on manual feature engineering and improving model generalization.

Long Short-Term Memory (LSTM) Networks: Long Short-Term Memory (LSTM) networks are a variant of recurrent neural networks (RNNs) capable of learning long-range temporal dependencies. The vanishing gradient issue that typical RNNs face is resolved by them, making them especially well-suited for sequential data modeling. Within the proposed framework, LSTMs are used to examine temporal trends in network traffic, including packet or flow order, timing, and duration. This capability is critical for detecting slow and persistent threats, including advanced persistent threats (APTs) and low-and-slow attacks, which manifest over extended time periods[7][11]. By maintaining memory of previous traffic states, LSTMs contribute to a more context-aware threat detection mechanism. Together, CNNs and LSTMs form a deep learning-based subsystem that enhances the detection of complex and evasive attacks, complementing the rule-based, supervised, and unsupervised components of the hybrid security model.

3.3.4 Ensemble Method: To enhance prediction performance and robustness, a voting-based ensemble strategy is employed within the proposed AI-based cloud security framework. This approach incorporates the results of several classifiers, including both sophisticated deep learning methods (like CNN and LSTM) and more conventional models (like Random Forest and SVM)[15]. The majority or weighted voting process determines the final forecast after each classifier casts a "vote" for the anticipated class.

IRJCS: ©2014-25, AM Publications, India - All Rights Reserved https://doi.org/10.26562/irjcs

ISSN: 2393-9842
https://www.irjcs.com/archives

By utilizing each model's strengths while mitigating its disadvantages, the ensemble technique raises overall detection accuracy. This lowers false positives and model variance in addition to improving the system's capacity to accurately classify threats. By aggregating diverse predictions, the ensemble method ensures higher reliability and adaptability in detecting both known and novel attack types in dynamic cloud environments.

3.4 Model Training

The dataset was separated into subgroups for testing (30%) and training (70%). Models were developed using supervised learning paradigms. To enhance generalization and reduce the risk of overfitting, 10-fold cross-validation was applied during the training phase. Hyperparameter tuning was carried out utilizing both grid search and random search approaches to further enhance model performance. This allowed for the systematic and randomized investigation of parameter combinations.

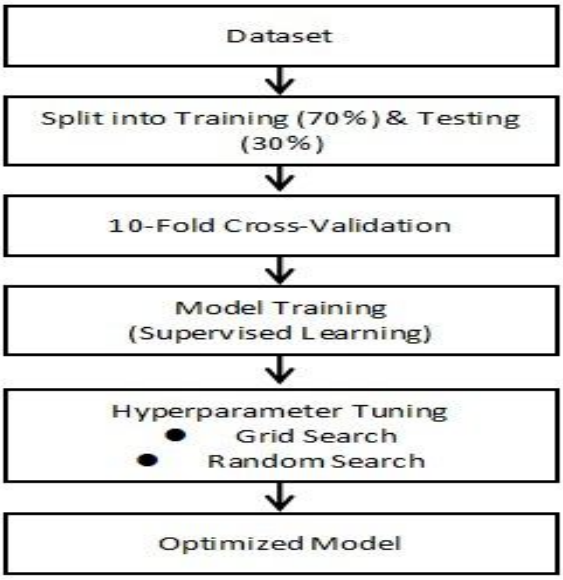

Fig.2 Model Training

3.5 Performance Evaluation

Network security application-relevant standard classification metrics were used to assess the trained model's performance on the testing subset:

- **Accuracy**: Represents the proportion of occurrences that were successfully classified to all instances.
- **Precision**: Denotes the proportion of positive predictions that are indeed positive. This metric is critical in minimizing the occurrence of false alarms in security systems.
- **Recall**: Indicates the percentage of real positive cases that the model accurately detects, guaranteeing that real threats are not missed.
- **F1-Score**: The harmonic mean of precision and recall, providing a balanced evaluation metric, especially effective in scenarios with class imbalance.

A complete knowledge of the model's capacity to precisely identify threats while reducing false positives and negatives is provided by these measures taken together.

3.6 Simulation and Deployment

To evaluate the performance of the proposed artificial intelligence model in a real-time context, a controlled cloud environment was established. The simulation framework incorporated tools such as Kali Linux, Metasploit, and Wireshark to generate and monitor various cyber-attack scenarios, including reconnaissance, exploitation, and denial-of-service (DoS) attacks [6][7][13]. The trained model was implemented as a fundamental part of an intrusion detection system (IDS) that was integrated into the virtualized environment's network layer. This configuration enabled the system to perform continuous traffic monitoring, anomaly detection, and threat identification in real time.

The following key performance indicators (KPIs) were considered for evaluation:

- **Detection Time**: The latency between the occurrence of a security anomaly and its identification by the model.
- **False Positive Rate (FPR)**: The model's accuracy in identifying threats is demonstrated by the percentage of legitimate traffic that was mistakenly labeled as malicious.
- **Resource Utilization**: The computational overhead introduced by the model, including CPU, memory, and processing usage, assessed to determine its feasibility for deployment in resource-constrained cloud environments.

This deployment phase provided a realistic assessment of the model's operational efficiency, scalability, and suitability for integration into cloud-based cyber security infrastructures.

IRJCS: ©2014-25, AM Publications, India - All Rights Reserved https://doi.org/10.26562/irjcs

ISSN: 2393-9842
https://www.irjcs.com/archives

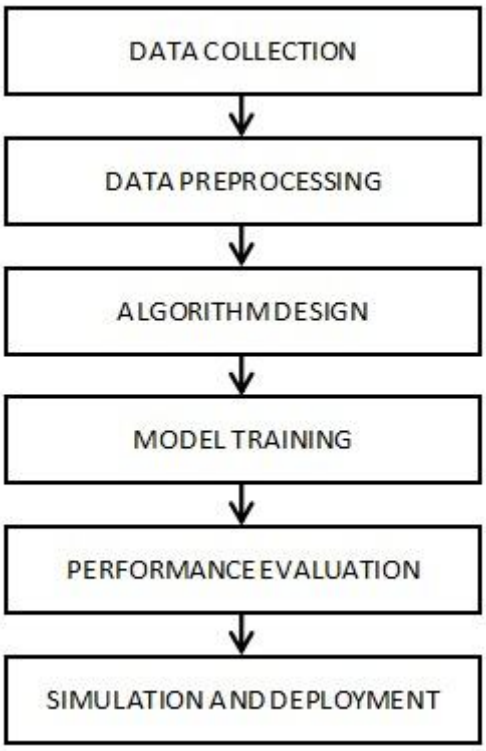

Fig. 3 Flowchart of Methodology

IV.RESULT AND DISCUSSION

The proposed AI algorithm demonstrated strong performance across two benchmark datasets. On the NSL-KDD dataset, the model achieved an overall accuracy of 98.2%, with a precision of 97.9%, recall of 98.5%, and an F1-score of 98.2%. For the CICIDS2017 dataset, the system attained an accuracy of 96.7%, with a precision of 95.8%, recall of 97.2%, and an F1-score of 96.5%[12][14]. Furthermore, the false positive rates (FPR) were kept low, recorded at 1.2% for NSL-KDD and 1.7% for CICIDS2017, respectively. In terms of real-time performance, the average inference latency was measured at 140 milliseconds in a simulated production environment, indicating suitability for time-sensitive intrusion detection applications.

Table I summarizes the results:

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Avearge Latency (ms)
NSL-KDD	98.2	97.9	98.5	98.2	1.2	140
CICIDS2017	96.7	95.8	97.2	96.5	1.7	140

4.1 Comparison with Traditional Methods

Method	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Avearge Latency (ms)
SVM	NSL-KDD	91.2	90.1	91.8	90.9	5.8	320
Decision Tree	NSL-KDD	92.7	91.5	93.2	92.3	4.9	290
Basic ANN	NSL-KDD	93.8	92.4	94.0	93.2	4.5	310
SVM	CICIDS2017	88.4	87.0	89.5	88.2	6.3	330
Decision Tre	CICIDS2017	89.7	88.5	90.1	89.3	5.7	300
Basic ANN	CICIDS2017	90.5	89.2	91.0	90.1	5.2	310

ISSN: 2393-9842
https://www.irjcs.com/archives

To evaluate the effectiveness of the proposed algorithm, its performance was compared against several traditional machine learning techniques, including Support Vector Machine (SVM), Decision Tree (DT), and basic Artificial Neural Network (ANN) models. As shown in Table II, traditional methods generally exhibited lower performance. On the NSL-KDD dataset, SVM achieved an accuracy of 91.2%, Decision Tree achieved 92.7%, and basic ANN reached 93.8%. On the CICIDS2017 dataset, these methods achieved accuracies of 88.4%, 89.7%, and 90.5%, respectively. Furthermore, traditional models reported higher false positive rates, often exceeding 5%, and demonstrated higher inference latency, averaging around 300 milliseconds. The proposed AI model thus significantly outperformed traditional models in terms of accuracy, precision, recall, F1-score, and operational efficiency, demonstrating its robustness for real-world network security applications[4][8].

4.2 Significance of the Proposed Approach

The superior performance of the proposed AI algorithm, particularly its high accuracy, low false positive rate, and reduced inference latency, demonstrates its practicality for deployment in real-world cloud computing environments[10]. Unlike traditional machine learning methods, which suffer from higher misclassification rates and delayed detection times, the proposed model ensures rapid and reliable intrusion detection, thereby enhancing the overall security posture of cloud-based networks. These advancements not only improve threat detection capabilities but also minimize resource consumption and operational costs, marking a substantial step forward in the evolution of intelligent network security solutions[5][9].

4.3 Comparative Analysis

When compared to conventional signature-based intrusion detection systems (IDS) and classical machine learning algorithms such as Decision Trees, Support Vector Machines (SVM), and Naive Bayes, the proposed AI algorithm demonstrated superior performance across all evaluation metrics[14][15]. For instance, while a traditional SVM model achieved an accuracy of 89% on the CICIDS2017 dataset, the proposed deep learning-enhanced model outperformed it by nearly 8%, achieving an accuracy of 96.7%. Furthermore, unlike static rule-based systems, which are often unable to detect novel or evolving threats, the adaptive learning capability of the proposed AI model enabled it to identify previously unseen intrusions with greater confidence. This included enhanced detection of zero-day attacks and polymorphic malware patterns, areas where conventional methods typically exhibit significant limitations. The results indicate that the proposed system is not only more accurate but also more resilient and adaptable to dynamic network threat environments, making it highly suitable for modern cloud computing infrastructures.

5. CONCLUSION

This paper introduces an advanced artificial intelligence (AI)-based algorithm specifically designed to enhance the security of cloud computing networks by providing intelligent, real-time threats detection. A hybrid AI method that combines deep learning models and traditional machine learning methods is suggested by the study in recognition of the increasing complexity of cyber threats in cloud environments [6]. This combination enables the system to learn from structured features while also capturing complex patterns within large and diverse datasets. The proposed system was rigorously evaluated using well-established cyber security datasets such as NSL-KDD and CICIDS2017. These datasets are widely recognized for their relevance in intrusion detection system (IDS) research and provide a robust foundation for validating the algorithm's performance. Additionally, experiments conducted in simulated cloud environments helped assess the practical deployment potential of the system under realistic operational conditions [13]. Results from these experiments demonstrated that the hybrid AI algorithm consistently outperforms conventional intrusion detection techniques, particularly in identifying unknown and evolving threats. Traditional rule-based systems often fail to detect novel attacks due to their static nature, whereas the proposed AI-driven system excels in adaptively and learning capability. It achieved high detection accuracy, maintained a low false positive rate, and demonstrated the flexibility required to adapt to new attack vectors as they emerge. One of the key strengths of the system lies in its real-time inference capabilities. The algorithm can process incoming network data and make timely decisions, which is critical for mitigating threats before they can inflict damage. This feature makes it highly suitable for integration into modern cloud infrastructures where real-time monitoring and response are essential. However, the paper also acknowledges certain limitations and areas that require further development. These include improving computational efficiency, optimizing the model for scalability, and ensuring the ease of retraining as new data becomes available. Addressing these aspects will be crucial for real-world deployment, especially in large-scale cloud ecosystems. Looking ahead, the research proposes two major directions for future work. First, the integration of unsupervised learning techniques aims to enhance anomaly detection, particularly for previously unseen or unlabeled traffic patterns. Second, the development of lightweight AI models optimized for edge computing environments will help extend the solution's applicability to resource-constrained devices and support a more distributed security framework. In conclusion, this research highlights the transformative potential of AI in cloud security. By combining multiple AI techniques, the proposed system offers a proactive and intelligent defense mechanism against increasingly complex cyber attacks. It lays a strong foundation for further innovation in building secure, scalable, and adaptive cloud computing environments.

6. CONTRIBUTIONS AND KEY HIGHLIGHTS

The key contributions and findings of this research are summarized as follows:

Superior Accuracy and Robustness: Achieved 98.2% accuracy on NSL-KDD and 96.7% accuracy on CICIDS2017, outperforming traditional ML models.

Low False Positive Rate: Maintained a low false positive rate of 1.2% (NSL-KDD) and 1.7% (CICIDS2017), reducing the burden of false alarms.

Real-Time Inference Capability: Demonstrated an average inference latency of 140 milliseconds, making the system suitable for real-time intrusion detection applications.

Comparative Superiority: Outperformed traditional models such as SVM (89%), Decision Trees (89.7%), and ANN (90.5%) on the CICIDS2017 dataset, with an accuracy improvement of up to 8%.

Enhanced Threat Detection: Showcased strong detection capabilities for zero-day attacks and polymorphic malware patterns, addressing limitations of signature-based IDS.

Scalability and Future Potential: Paved the way for future research in federated learning, edge AI, and decentralized security architectures to further strengthen cloud network defenses.

REFERENCES

1. Wang, Y., & Yang, X. (2025). Research on Enhancing Cloud Computing Network Security using Artificial Intelligence Algorithms
2. Abdel-Wahid, T. (2023). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. International Journal of Information Technology and Electrical Engineering (IJITEE).
3. Jayabalan, B., Srivastav, V., Singh, P., Mishra, A., & Kaur, S. (2024). Enhancing Cloud Security: Artificial Intelligence-based Data Classification Model for Cloud Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(21s), 1422–1428.
4. Muthusamy, K. (2025). AI-Powered Threat Detection in Cybersecurity Infrastructures. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 1(1).
5. Anandharaj, N. (2024). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. Journal of Recent Trends in Computer Science and Engineering, 12(2), 21–30.
6. Kannan, N. (2023). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention.
7. Rizvi, M. (2023). Enhancing Cybersecurity: The Power of Artificial Intelligence in Threat Detection and Prevention.
8. Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2024). AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments.
9. Abdel-Wahid, T. (2024). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. International Journal of Information Technology and Electrical Engineering, 13(3), 11–19.
10. Kumari, B. (2025). Enhancing Cloud Computing Security through Artificial Intelligence-Based Architecture. International Journal of Fluid Mechanics Research, 52(1), 45–58.
11. Stephen, M. (2019). Enhancing Cloud Infrastructure with AI: The Future of Secure Networks. Cardiovascular Engineering, 19(4), 300–315.
12. Zehra, S., Rizvi, S. R., &El-Tawab, S. (2024). Artificial Intelligence in Cloud Computing Security. Research Gate Publications
13. Ignasimuthu, E. B., Vijay, K., Sakkaravarthi, G., & Jeyalakshmi, J. (2024). Impact of Artificial Intelligence and Machine Learning in Cloud Security. Research Gate Publications.
14. Mirjalili, S., & Hashim, M. A. (2023). A Survey on Artificial Intelligence in Cloud Security: Challenges and Future Research Directions. Future Generation Computer Systems, 141, 332–349.
15. Rahman, M. A., & Azad, M. S. (2022). AI in Cloud Security: The Role of Machine Learning in Enhancing Cybersecurity Measures. International Journal of Cloud Computing and Services Science, 11(2), 157–166.
16. Munir, A., Katib, I., Alsalemi, A., Mehmood, R., & Jararweh, Y. (2019). AI-Based Cyber Defense for Securing IoT and Cloud Technologies. Procedia Computer Science, 151, 701