JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Machine Learning Based IDS For Secure Cloud Environment

Mrs. P. Kamakshi Thai [1] Assistant Professor, Department of CSE (Artificial Intelligence & Machine Learning), ACE Engineering College, Ankushapur, Hyderabad
kamakshithai.panchagnula@aceec.ac.in (Corresponding Author)

Maruthi Thatikonda [2] Student of ACE Engineering College, Department of CSE (Artificial Intelligence &Machine Learning) maruthithatikonda04@gmail.com

Shashikanth Devarakonda [3] Student of ACE Engineering College, Department of CSE (Artificial Intelligence& Machine Learning) shashikanthdevarakonda@gmail.com

Harshit Sai Kamishetty [4] Student of ACE Engineering College, Department of CSE (Artificial Intelligence &Machine Learning)kamishetty.harshitsai@gmail.com

Abstract: In today's digital era, cloud computing platforms are widely used for data storage and online services, however, they are increasingly exposed to various cyberattacks. Traditional security mechanisms often fail to detect sophisticated or previously unseen intrusion patterns. This project proposes an optimized Intrusion Detection System (IDS) based on machine learning algorithms to enhance the security of cloud environments. The proposed system utilizes Random Forest for supervised classification of known and unknown attacks and Isolation Forest for unsupervised anomaly detection, and is evaluated using real-world network traffic datasets. The system is trained to effectively distinguish between normal and malicious network activities with high accuracy. The proposed solution automates intrusion detection, strengthens cloud security, and minimizes the risk of data breaches. Overall, the machine learning-based IDS provides a scalable, efficient, and intelligent approach to securing modern cloud infrastructures.

Keywords: Cloud Computing, Intrusion Detection System (IDS), Machine Learning, Network Traffic Analysis, Random Forest, Isolation Forest.

Introduction

In the modern digital landscape, cloud computing has become a key platform for data storage, application deployment, and online service delivery. Its benefits, including scalability, cost efficiency, and operational flexibility, have led to widespread adoption across various industries. However, the growing dependence on cloud infrastructures has also increased exposure to cyber threats, expanding the attack surface for malicious actors. As cloud platforms manage large volumes of sensitive and critical data, ensuring robust security has become a major challenge for organizations.

Conventional security mechanisms, particularly signature-based Intrusion Detection Systems (IDS), are increasingly inadequate in addressing sophisticated and evolving cyberattacks. These systems depend on predefined attack signatures and are ineffective against zero-day and previously unseen threats. Additionally, the distributed and dynamic nature of cloud environments makes real-time monitoring and intrusion detection more complex. This highlights the need for intelligent, adaptive, and scalable security solutions capable of analysing network behaviour and detecting malicious activities efficiently in cloud environments.

Existing System

Traditional intrusion detection systems (IDS) used in cloud environments mainly rely on signature-based or rule-based detection methods, where network traffic is compared against predefined attack patterns or manually defined security rules. While these systems are effective in detecting known threats, they fail to identify zero-day or previously unseen attacks and require frequent manual updates to remain effective. Even many existing machine learning–based IDS solutions depend only on supervised models trained on labelled datasets, which limits their ability to detect anomalous or unknown behaviours in dynamic cloud environments. Additionally, several systems operate offline without real-time monitoring, visualization, or alerting capabilities, leading to higher false positive rates, reduced adaptability, and limited scalability for large-scale cloud infrastructures.

Proposed Methodology

The system works by focuses on the design and evaluation of a machine learning–based Intrusion Detection System (IDS) to enhance security in cloud computing environments. The proposed system analyses network traffic data by combining supervised and unsupervised learning techniques to identify malicious activities. In this approach, Random Forest is employed to detect known attack patterns using labelled data, while Isolation Forest is utilized to identify anomalous behaviour, enabling the detection of zero-day and previously unseen attacks. This both combine detection strategy improves detection accuracy and reduces false positive rates when compared to traditional signature-based intrusion detection systems.

The system is trained and evaluated using the CICIDS2017 dataset, which represents realistic cloud network traffic containing both normal behaviour and various cyberattacks. The scope of this study is limited to intrusion detection and traffic analysis and does not include automated

prevention or response mechanisms. Experimental evaluation is conducted in a controlled environment to demonstrate the feasibility and effectiveness of the proposed IDS. The results provide a strong foundation for future enhancements, such as real-time deployment, improved scalability, and integration with advanced cloud security frameworks for proactive defence against evolving and zero-day cyber threats.

Literature Survey

[1] **Title:** A Survey of Intrusion Detection Systems in Cloud Computing.

Authors: Prashanth Kumar., et al

This study presents the evolution of intrusion detection systems (IDS) in cloud computing environments and highlights the limitations of traditional signature-based and rule-based approaches in handling modern cyber threats. The study emphasize that the dynamic and scalable nature of cloud infrastructures requires intelligent IDS solutions capable of detecting both known and unknown attacks efficiently. The study identifies machine learning techniques such as Support Vector Machines, Decision Trees, and clustering methods as effective tools for improving intrusion detection accuracy through automated analysis of network traffic.

The paper further discusses hybrid IDS approaches that combine misuse-based and anomaly-based detection techniques to reduce false alarms and enhance detection performance. It concludes that machine learning-based hybrid IDS frameworks provide a scalable and reliable foundation for securing cloud environments, motivating further research in intelligent cloud security solutions

[2] **Title:** Enhancing Cloud Security through Machine Learning Based Intrusion Detection. **Authors:** Pradeep Reddy., et al.

This study examines the application of machine learning techniques to enhance intrusion detection in cloud computing environments, with a focus on improving accuracy, scalability, and of the responsiveness. It introduces a cloud-based intrusion detection system (IDS) that employs ensemble machine learning models to identify and mitigate cyber threats such as Distributed Denial-of-Service and insider attacks. The research highlights the increasing complexity of cloud workloads and the need for IDS frameworks capable of efficiently processing large volumes of

data in dynamic cloud settings. The proposed system integrates Random Forest and Gradient Boosting algorithms to analyse network traffic and distinguish between normal and malicious activities with high precision. By combining multiple machine learning models, the framework achieves greater detection accuracy

and robustness compared to traditional methods, while maintaining computational efficiency. The study concludes that ensemble-based IDS designs are well-suited for cloud environments due to their adaptability and scalability. It also suggests that future research should focus on enhancing real-time detection, minimizing latency, and improving model interpretability to ensure more effective and transparent cloud security management.

[3] **Title:** Cloud Intrusion Detection Using Optimized Deep Neural Networks.
Authors: Hao Li, Qiang Chen., et al.

The proposed system presents an optimized deep neural network framework for real-time intrusion detection in cloud computing environments. The model applies advanced deep learning techniques to improve detection accuracy, adaptability, and processing efficiency compared to traditional security systems. By using adaptive learning rates, the framework achieves faster convergence and responds effectively to changing network conditions, enabling the detection of both known and unknown cyber threats while efficiently utilizing system resources.

To further enhance performance, the framework incorporates optimization techniques such as dropout regularization to prevent overfitting and improve generalization across diverse attack scenarios. These optimizations allow the model to handle high data flow and complex traffic patterns commonly found in cloud environments. The system balances accuracy, scalability, and efficiency, making it suitable for large-scale and multi-tenant cloud infrastructures. Future enhancements may focus on improving real-time deployment, model interpretability, and reducing reliance on large labelled datasets for broader cloud security applications.

[4] **Title:** An Improved Design for a Cloud Intrusion Detection System Using Hybrid Features Selection Approach with ML Classifier
Authors: Mohamad Bakro, Rakesh Ranjan Kumar., et al.

The proposed system demonstrates the effectiveness of machine learning–based intrusion detection in managing the complexity and high data flow of modern cloud environments. By leveraging a Random Forest classifier with optimized feature selection, the framework enhances detection accuracy while maintaining computational efficiency. This makes it well suited for dynamic, multi-tenant cloud infrastructures that require continuous analysis of large-scale network traffic.

Additionally, the framework achieves a balanced design by addressing accuracy, scalability, and efficiency, supporting practical real-world deployment. The results show lower false alarm rates and better adaptability than traditional intrusion detection systems. Future work may focus on real-time implementation, minimizing dependence on large labelled datasets, and improving model interpretability to enable more transparent cloud security solutions.

[5] **Title:** Machine Learning-Based Intrusion Detection for Cloud Computing: A Review
Authors: Patel, D. & Thakkar, A. et al.

The proposed system presents an optimized machine learning–based intrusion detection framework for real-time security in cloud computing environments. It utilizes algorithms such as Random Forest and Support Vector Machine (SVM) along with feature selection and hyperparameter tuning to improve detection accuracy, reduce false positives, and enhance processing efficiency. By eliminating redundant features and optimizing model performance, the system effectively handles high-volume and dynamic cloud traffic while detecting both known and unknown cyber threats. Designed for scalability and resource efficiency, the framework provides a practical and robust solution for securing large-scale cloud infrastructures, with future improvements aimed at enhancing real-time deployment and adaptability to evolving attack patterns.

[6] **Title:** Deep Learning Approaches for Intrusion Detection in Cloud Environments
Authors: Zhang, L., & Wang, Y. et al.

This system presents a deep learning–based intrusion detection framework for cloud environments that uses CNN and LSTM models to automatically learn complex spatial and temporal patterns from network traffic data. By applying optimization techniques such as adaptive learning rates and regularization methods, the system improves detection accuracy and reduces false positives. It effectively detects both known and unknown cyber threats while handling high-volume and dynamic cloud traffic. The framework is designed for scalability and enhanced performance, making it suitable for real-time security in large-scale cloud infrastructures.

[7] **Title:** Optimized Feature Selection for Intrusion Detection Using Metaheuristic Algorithms
Authors: Ahmed, M. & Khan, S. et al.

The proposed system introduces an optimized feature selection–based intrusion detection framework for cloud environments that utilizes metaheuristic algorithms such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) to identify the most relevant network traffic features. By eliminating redundant and irrelevant attributes, the system reduces computational complexity and enhances detection speed without compromising accuracy. The optimized feature set improves model performance, lowers false positive rates, and ensures efficient processing of high-volume cloud data. Designed for scalability and resource efficiency, the framework provides a practical solution for real-time intrusion detection in large-scale cloud infrastructures.

[8] Title: A Comparative Study of Intrusion Detection Systems Using Machine Learning Techniques.
Authors: Singh, A., & Kaur, J. et al.

This system compares multiple machine learning classifiers, including KNN, Naïve Bayes, SVM, and ANN, for intrusion detection using the UNSW-NB15 dataset. The results show that ensemble methods achieve higher accuracy and lower false positive rates than individual classifiers. The study also highlights the importance of dataset quality and effective feature engineering in improving the overall performance of machine learning–based intrusion detection systems.

System Architecture

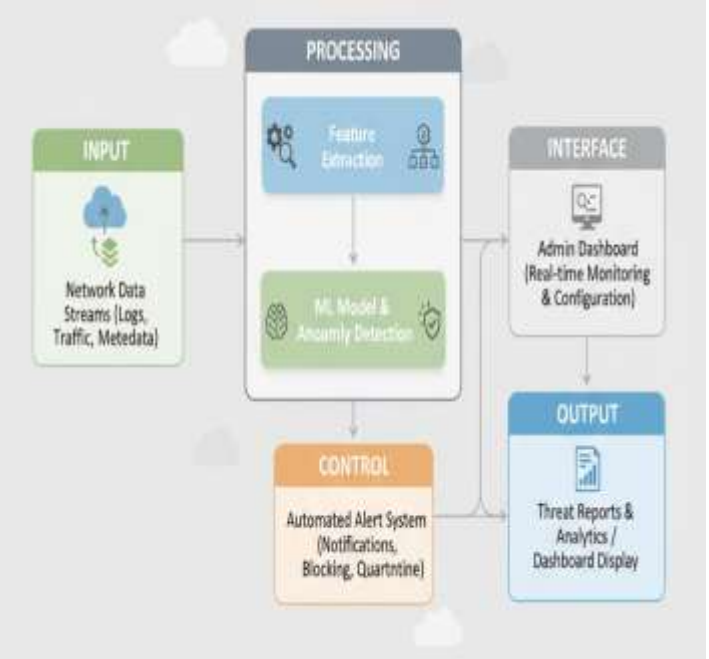

Fig: System Architecture of ML based cloud IDS

Comparison Table of Title& Authors, Methodology and Key Contributions

SNO	Title & Authors	Methodology/ Approach	Key Contributions / Findings
1	A Survey of Intrusion Detection Systems in Cloud Computing. Prashanth Kumar., et al	Conducted a detailed review of existing IDS techniques used in cloud systems. Analyzed strengths and weaknesses of traditional vs. ML-based IDS models.	Found that traditional IDS cannot adapt to new cloud threats. Recommended using machine learning for better accuracy and adaptability.
2	Enhancing Cloud Security through Machine Learning Based Intrusion Detection. Pradeep Reddy., et al.	Proposed an ensemble ML model combining Random Forest and Gradient Boosting for better detection of complex cloud attacks. .	Achieved high accuracy and scalability. Effectively detected DDoS and insider attacks with fewer false positives.
3	Cloud Intrusion Detection Using Optimized Deep Neural Networks. Hao Li, Qiang Chen., et al.	Developed an optimized Neural Network model using adaptive learning and dropout regularization for intrusion detection.	Improved real-time detection efficiency and reduced resource usage while maintaining strong accuracy.
4	An Improved Design for a Cloud Intrusion Detection System Using Hybrid Features Selection Approach with ML Classifier Mohamad Bakro, Rakesh Ranjan Kumar., et al.	Designed an ensemble-style IDS that integrates supervised and unsupervised machine learning techniques to improve cloud attack detection accuracy.	Improved real-time intrusion detection efficiency while reducing of computational overhead and resource usage.
5	Machine Learning-Based Intrusion Detection for Cloud Computing: A Review Patel, D. & Thakkar, A. et al	Uses optimized machine learning algorithms such as Random Forest and SVM with feature selection and hyperparameter tuning for efficient cloud intrusion detection.	Improves detection accuracy, reduces false positives, and enhances scalability and efficiency for real-time cloud security.
6	Deep Learning Approaches for Intrusion Detection in Cloud Environments Zhang, L., & Wang, Y. et al.	Applies CNN and LSTM models with optimization techniques to learn complex patterns from cloud network traffic.	The model effectively detects accuracy and unknown attacks while maintaining stable performance in high-volume cloud environments.

7	Optimized Feature Selection for Intrusion Detection Using Metaheuristic Algorithms Ahmed, M. & Khan, S. et al.	Applies Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) to select relevant features, reducing data size and computational complexity for efficient intrusion detection.	The optimized feature set improves detection speed and accuracy while lowering false positive rates. The system ensures efficient and scalable real-time intrusion detection in cloud environments.
8	A Comparative Study of Intrusion Detection Systems Using Machine Learning Techniques. Singh, A., & Kaur, J. et al.	Evaluates multiple machine learning classifiers such as KNN, Naïve Bayes, SVM, and ANN using the UNSW-NB15 dataset to compare their intrusion detection performance.	Ensemble methods outperform individual classifiers in terms of accuracy and false positive reduction, highlighting the importance of proper dataset selection and feature engineering for effective IDS performance.

Conclusion:

The Machine Learning–Based Cloud Intrusion Detection System (IDS) delivers an intelligent security solution by combining machine learning algorithms, rule-based detection, and real-time network monitoring to accurately classify network traffic as benign or malicious using models trained on the CICIDS2017 dataset. By integrating TCP control rules and SYN flood detection with ML-based classification, it enhances accuracy while reducing false positives. Built on a Flask architecture with Socket IO, the system enables real-time monitoring, dashboard visualization, database logging, Geo IP mapping, and automated email alerts, ensuring continuous, efficient cloud protection without performance delays or manual inspection.

References:

[1] Prashanth Kumar, & Ravi Kumar. (2021). A Survey of Intrusion Detection Systems in Cloud Computing.

[2] Reddy, P., Sharma, A., & Kumar, S. (2022). Enhancing Cloud Security through Machine Learning-Based Intrusion Detection.

[3] Li, H., & Chen, Q. (2020). Cloud Intrusion Detection Using Optimized Deep Neural Networks.

[4] Zhang, L., & Wang, Y. (2019). Deep Learning Approaches for Intrusion Detection in Cloud Environment.

[5] Alshamrani, A., Alismaeel, Z., & Alabdulatif, A. (2023). An Efficient Machine Learning Based Intrusion Detection System for Cloud Computing Environments.

[6] Kumar, R., Sharma, T., & Singh, P. (2024). Lightweight Deep Learning Framework for RealTime Intrusion Detection in Cloud Networks.

[7] Bakro, M., Kumar, R. R., Alabrah, A., Ashraf, Z., Ahmed, M. N., Shameem, M., & Abdelsalam, A. (2024). An Improved Design for a Cloud Intrusion Detection System Using Hybrid Features Selection Approach with ML Classifier.

[8] Patel, D., & Thakkar, A. (2021). Machine Learning-Based Intrusion Detection for Cloud Computing: A Review.

[9] Ahmed, M., & Khan, S. (2023). Optimized Feature Selection for Intrusion Detection Using Metaheuristic Algorithms.

[10] Singh, A., & Kaur, J. (2020). A Comparative Study of Intrusion Detection Systems Using Machine Learning Techniques.

[11] Sharma, S., & Gupta, V. (2022). An Efficient Intrusion Detection System Using Hybrid Machine Learning Algorithms.

[12] Mousavi, S. S., & Shams, R. (2024). Enhanced Cloud Intrusion Detection Using Hybrid Machine Learning and Feature Optimization.

[13] Zhou, T., & Li, X. (2025). Real-Time Machine Learning–Based Intrusion Detection for Cloud IoT Environments.