Threat Behaviour Analytics for Cloud Security using Machine Learning

Deshmukh Jay Rajesh[1], Gangurde Pawan Rajaram[2], Raut Kartik Ganesh[3], Shankhpal Meghraj Vijay[4], Mr. Mahesh Dhande[5]

[5]Guide

[1,2,3,4,5]Department of Artificial Intelligence and Data Science Engineering, Matoshri College of Engineering and Research, Centre, Odhagaon Nashik-422105

Abstract:
Cloud computing has become an essential platform for storing and managing large volumes of sensitive data, making it a prime target for cyber-attacks. Traditional security mechanisms often fail to detect complex and evolving threats in real time. This paper presents an intelligent cloud security system based on threat behavior analytics using a hybrid machine learning approach. The proposed system analyzes cloud log data, including user activities, system events, and network transactions, to identify suspicious patterns and potential cyber-attacks. A hybrid model combining Random Forest and Support Vector Machine (SVM) is implemented to improve detection accuracy and reduce false alerts. The system also provides preventive suggestions and generates detailed reports to assist administrators in understanding and mitigating threats. A web-based interface is developed to enable easy interaction, allowing users to input data and monitor security status efficiently. The proposed solution aims to enhance cloud security by providing accurate, reliable, and real-time attack detection. Experimental results demonstrate that the system achieves high accuracy and efficiency, making it suitable for modern cloud environments.

Key Words: Cloud Security, Threat Detection, Machine Learning, Random Forest, Support Vector Machine (SVM), Hybrid Model, Cloud Log Analysis, Cyber Attack Detection, Anomaly Detection, Web-Based Security System.

INTRODUCTION

Cloud computing has become a widely adopted technology for storing, managing, and processing large amounts of data due to its scalability, flexibility, and cost-effectiveness. Organizations across various domains rely on cloud platforms to handle critical information and services. However, this rapid adoption has also made cloud environments a major target for cyber-attacks. Malicious activities such as unauthorized access, data breaches, Distributed Denial of Service (DDoS) attacks, and insider threats pose significant risks to cloud security. Traditional security mechanisms, including firewalls and rule-based intrusion detection systems, are often limited in their ability to detect complex and evolving attack patterns, especially in large-scale cloud environments.

To overcome these limitations, machine learning techniques have emerged as an effective solution for enhancing cloud security. Machine learning models can analyze large volumes of cloud log data, identify hidden patterns, and detect anomalies that indicate potential threats. However, relying on a single algorithm may not always provide optimal results in terms of accuracy and reliability. Therefore, hybrid approaches that combine multiple machine learning algorithms can significantly improve detection performance.

This work focuses on the development of a threat behavior analytics system for cloud security using a hybrid machine learning model. The proposed system analyzes cloud logs, including user activities, system events, and network transactions, to detect suspicious behavior and potential cyber-attacks. It combines Random Forest for feature analysis and Support Vector Machine (SVM) for precise classification, enhancing both accuracy and efficiency. Additionally, the system provides preventive suggestions and generates detailed reports to assist administrators in understanding and mitigating threats. A web-based interface is developed

to enable easy interaction, allowing users to input data and monitor security status in real time. The primary goal of this system is to provide an intelligent, reliable, and user-friendly solution for improving cloud security and preventing cyber-attacks.

LITERATURE SURVEY

The use of machine learning techniques for improving cloud security has gained significant attention in recent years. Researchers have explored various approaches to detect cyber-attacks and enhance the reliability of cloud environments.

Gupta (2025) proposed a machine learning-based approach using Decision Tree algorithms to predict and prevent vulnerabilities in distributed cloud systems. The study focused on integrating machine learning into real-time security pipelines and reducing false positives. However, the approach mainly relied on a single model, which may limit detection accuracy for complex attack patterns.

Joon (2024) investigated cloud security policies using machine learning techniques such as K-Nearest Neighbors (KNN) and Linear Regression. The study emphasized the use of data mining and clustering methods to improve classification accuracy. Although effective, the system lacked advanced anomaly detection capabilities for identifying unknown threats.

Singh (2021) discussed various machine learning techniques for enhancing cloud security through anomaly detection and automated response systems. The research highlighted the importance of intelligent systems in identifying cyber threats but also pointed out limitations in handling large-scale cloud data efficiently.

Patel (2020) introduced a predictive model using Gradient Boosting Decision Trees to forecast malware attacks in cloud environments. The model showed improved prediction accuracy but required high computational resources, making it less suitable for real-time applications.

Overall, existing research demonstrates that machine learning plays a crucial role in improving cloud security. However, many systems rely on single-model approaches, lack real-time performance, or do not provide preventive insights for future attacks. The proposed system addresses these limitations by implementing a hybrid Random Forest–SVM model, which improves detection accuracy, reduces false alerts, and provides actionable suggestions along with a user-friendly web-based interface for effective cloud security management.

METHODOLOGY

The proposed system follows a structured methodology to detect and prevent cyber-attacks in cloud environments using machine learning techniques. The overall workflow consists of data collection, preprocessing, feature extraction, hybrid model-based classification, and result generation through a web-based interface.

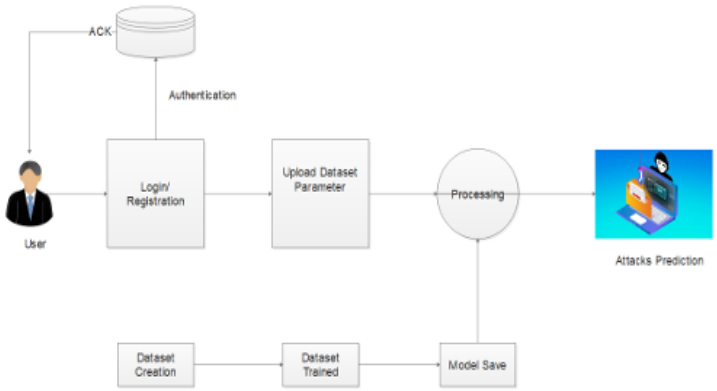
Initially, cloud log data is collected, which includes user activities, system events, and network transactions. This data may contain noise, missing values, or irrelevant information; therefore, preprocessing is performed to clean and organize the dataset. The preprocessing steps include data cleaning, normalization, and formatting to ensure consistency and improve model performance.

After preprocessing, feature extraction is carried out using the Random Forest algorithm. Random Forest helps in identifying important features and patterns from the cloud data, reducing noise and improving the quality of input for the next stage. These extracted features are then passed to the Support Vector Machine (SVM) classifier, forming a hybrid machine learning model. The SVM is responsible for classifying the input data as normal behavior or potential cyber-attack based on learned patterns.

Once the classification is completed, the system generates the output in the form of attack detection results along with preventive suggestions. To enhance usability, a web-based interface is developed where an admin can log in, input data, and monitor the system in real time. The system also generates detailed reports that include information about detected threats, attack patterns, and recommended actions.

This structured approach ensures accurate detection of both known and unknown threats, reduces false alerts, and provides an efficient and user-friendly solution for improving cloud security.

BLOCK DIAGRAM



OBJECTIVE

1. To analyze cloud log data, including user activities, system events, and network transactions, for detecting suspicious behavior.
2. To develop a hybrid machine learning model using Random Forest and Support Vector Machine (SVM) for accurate threat detection.
3. To identify and classify different types of cyber-attacks in cloud environments efficiently.
4. To provide preventive suggestions to help administrators avoid future security threats.
5. To design a web-based interface that allows easy monitoring, data input, and real-time threat detection.
6. To generate detailed reports summarizing detected threats, attack patterns, and recommended security measures.

PROBLEM DEFINATIONS

Cloud computing environments are highly vulnerable to cyber-attacks due to the large volume of sensitive data and complex network interactions. Traditional security systems rely on predefined rules and are unable to detect new or evolving threats effectively. This creates a need for an intelligent system that can automatically analyze cloud data, detect suspicious activities, and provide accurate and timely threat detection to improve overall cloud security.

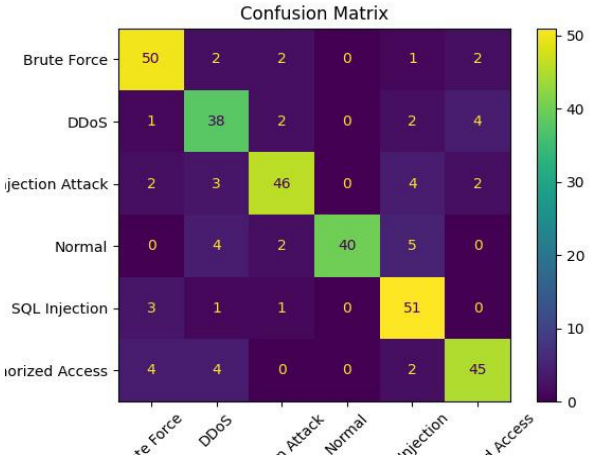
FUCTIONAL REQUIREMENTS

1. The system shall allow secure admin login and access.
2. The system shall accept and process cloud log data as input.
3. The system shall preprocess data before analysis.
4. The system shall detect and classify cyber-attacks using the hybrid ML model.
5. The system shall generate reports with detected threats and preventive suggestions.

NON FUCTIONAL REQUIREMENTS

1. Performance: The system should provide fast and efficient threat detection.
2. Accuracy: The model should deliver high accuracy with minimal false alerts.
3. Usability: The interface should be simple and user-friendly.
4. Scalability: The system should handle large volumes of cloud data.
5. Security: The system must ensure secure data handling and access control.

RESULTS



Training and Validation Performance Analysis

The confusion matrix illustrates the performance of the proposed hybrid Random Forest–SVM model in classifying different types of cyber-attacks. The diagonal elements represent correct predictions, and most classes show high values, such as Brute Force (50), SQL Injection (51), Injection Attack (46), and Normal (40), indicating strong classification accuracy.

The off-diagonal elements represent misclassifications, which are relatively low across all categories. Minor confusion is observed between similar attack types such as DDoS and Injection Attack, and between Unauthorized Access and Brute Force. However, these errors are limited and do not significantly affect overall performance.

Overall, the results demonstrate that the model achieves high accuracy with minimal false predictions, effectively distinguishing between normal activities and various cyber-attacks. This confirms the reliability and efficiency of the proposed system for cloud security applications.

IMPLEMENTAION

Fig: Home Page

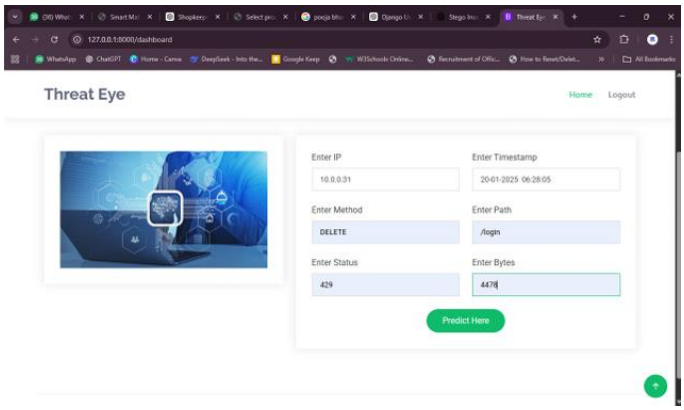


Fig: Dashboard

CONCLUSION

The proposed system provides an effective solution for enhancing cloud security using a hybrid machine learning approach. By combining Random Forest and Support Vector Machine (SVM), the system is able to accurately detect and classify different types of cyber-attacks. It analyzes cloud log data efficiently, identifies suspicious activities, and provides preventive suggestions to reduce future risks. The results demonstrate high accuracy with minimal false alerts, making the system reliable for real-world applications. The web-based interface further improves usability by allowing easy monitoring and real-time threat detection. Overall, the system offers a scalable, efficient, and intelligent approach to securing cloud environments against evolving cyber threats.

REFERENCES:

[1] S. K. Singh, P. Bhambu, A. Sandhu, A. Kumar, D. Sharma, and A. Pandey, "Achieving Cloud Security Solutions based on Machine Learning and Past Information," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 29, 2021.

[2] A. R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, and M. AlElaimat, "Intrusion Detection in Cloud Computing Based on Time Series Anomalies Utilizing Machine Learning," *IEEE Access*, vol. 11, pp. 102345–102358, 2023.

[3] H. Attou, A. Gueroui, and A. Bounceur, "Cloud-Based Intrusion Detection Approach Using Machine Learning," in *Proc. IEEE Int. Conf. Smart Computing (SMARTCOMP)*, 2023.

[4] N. Jagan Mohan, S. R. Dubey, and S. Chaudhuri, "Machine Learning-Based Intrusion Detection System for Cloud Security," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1456–1468, 2023.

[5] M. Tălu, "Exploring Machine Learning Algorithms to Enhance Cloud Computing Security," in *Proc. IEEE Int. Conf. Digital Technologies and Applications (DTA)*, 2025.

[6] H. Gupta and A. P. Sundareswaran, "Optimizing Cloud Security with Machine Learning: Predicting and Preventing Vulnerabilities in Distributed Systems," in *Proc. IEEE Int. Conf. Networks and Cryptology (NETCRYPT)*, 2025.

[7] V. Joon, "Study and Investigation of Cloud-Based Security Policies Using Machine Learning Techniques," in *Proc. IEEE Int. Conf. Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, 2024.

[8] W. Nazih, A. El Moutaouakil, and M. Ezziyyani, "Machine Learning Techniques for Cloud Intrusion Detection Systems: A Comparative Study," *IEEE Access*, vol. 12, pp. 55678–55690, 2024.

[9] A. Alharbi and M. Alshammari, "Hybrid Machine Learning Approach for Detecting Cyber Threats in Cloud Environments," in *Proc. IEEE Int. Conf. Artificial Intelligence and Data Analytics (CAIDA)*, 2022.