AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(1) (2026)
www.ajmimc.com

Improving Cloud Data Communication Security Through Intelligent Machine Learning Models

[1]P. Renuka,[2]Gaddam Kusumanjali,[3]Kedasu Vikitha,[4]Dhandagala Jansi,[5]M. Meenakshi,[6]Macha Bhargavi

[1]Assistant Professor, Department of Computer Science & Engineering, Princeton Institute of Engineering & Technology For Women

[2,3,4,5,6]B. Tech Students, Department of Computer Science & Engineering,Princeton Institute of Engineering & Technology For Women

ABSTRACT

Cloud computing has become an essential platform for data storage and communication due to its scalability, flexibility, and cost efficiency. However, the increasing volume of cloud-based data communication also raises significant security concerns, including unauthorized access, malicious attacks, and network intrusions. To address these challenges, this work proposes an intelligent machine learning–based framework for improving cloud data communication security. The proposed system analyzes network traffic attributes such as source IP, destination IP, protocol type, packet size, login time, country of origin, and risk score to detect potential attack patterns in cloud environments. Feature engineering techniques are applied to extract meaningful attributes from IP addresses, followed by preprocessing steps including label encoding and data normalization. Multiple machine learning algorithms, namely Random Forest, Gradient Boosting, and Extreme Gradient Boosting (XGBoost), are employed to classify and identify various types of cyber-attacks in cloud networks. The models are trained and evaluated using a cloud security dataset, and their performance is measured using metrics such as accuracy, classification report, and confusion matrix analysis. Among the implemented models, XGBoost demonstrates superior performance in predicting attack categories and identifying malicious activities. The proposed intelligent ML-based security framework enables early detection of suspicious network behavior and supports administrators in strengthening cloud communication security. This approach contributes to enhancing reliability, minimizing cyber threats, and improving the overall resilience of cloud computing environments.

Keywords: Cloud computing security, machine learning, data communication security, intrusion detection systems (IDS), anomaly detection, deep learning, network traffic analysis, cyber-threat detection, secure data transmission, artificial intelligence in cybersecurity, cloud data protection, threat intelligence, privacy-preserving learning, secure cloud architecture, predictive security analytics.

I. INTRODUCTION

Cloud computing has transformed the way organizations store, process, and transmit data by providing scalable, flexible, and cost-efficient computing resources over the internet. Many businesses, institutions, and individuals rely on cloud platforms for data communication and storage because they allow seamless access to services from anywhere. However, the rapid growth of cloud-based systems has also introduced significant security challenges. Cloud networks often face threats such as unauthorized access, malicious network traffic, distributed denial-of-service attacks, and other cyber intrusions that can compromise data integrity and system availability. Therefore, ensuring secure communication and early detection of malicious activities has become a critical requirement in cloud environments.

Traditional security mechanisms such as rule-based firewalls and signature-based

intrusion detection systems are often insufficient to detect new and evolving attack patterns in modern cloud infrastructures. These conventional approaches mainly depend on predefined signatures and may fail to identify unknown or sophisticated attacks. As a result, intelligent data-driven techniques are increasingly being adopted to enhance cloud security systems. Machine learning methods are particularly effective because they can analyze large volumes of network traffic data, identify hidden patterns, and classify potential threats with higher accuracy.

In this work, an intelligent machine learning framework is developed to improve cloud data communication security by analyzing network traffic features. The proposed system processes a cloud security dataset containing attributes such as source IP address, destination IP address, protocol type, packet size, login time, country of origin, and risk score. Feature engineering techniques are applied to extract subnet and host information from IP addresses to improve model learning capability. Data preprocessing methods including label encoding and feature scaling are used to prepare the dataset for training.

Multiple machine learning algorithms, including Random Forest, Gradient Boosting, and Extreme Gradient Boosting (XGBoost), are implemented and evaluated to classify different types of cyber attacks in cloud communication. The models are trained and tested using a stratified data split, and their performance is measured using metrics such as accuracy score, classification report, and confusion matrix analysis. Among these models, XGBoost is used for final prediction due to its strong classification performance.

The proposed system is implemented using Python and the Django web framework, which enables dataset visualization, model training, and real-time attack prediction through a user interface. By integrating intelligent machine learning techniques with cloud security analysis, the system helps identify suspicious activities in network traffic and supports administrators in strengthening the protection of cloud communication environments.

II. LITERATURE SURVEY

1. Title: Machine Learning-Based Intrusion Detection System for Cloud Computing

Author: S. M. Milajerdi, A. Eshete, R. Sekar

Abstract—
This study presents a machine learning-based intrusion detection system designed to improve security in cloud computing environments. The proposed system analyzes network traffic patterns and identifies malicious activities using supervised learning techniques. Various algorithms such as Random Forest and Support Vector Machines are evaluated to classify normal and abnormal traffic. The results show that machine learning methods significantly improve detection accuracy compared to traditional signature-based security systems. The study highlights the importance of intelligent models in identifying evolving cyber threats in cloud infrastructures.

2. Title: An Intelligent Intrusion Detection Framework Using Machine Learning Techniques

Author: M. Tavallaee, E. Bagheri, W. Lu, A. Ghorbani

Abstract—
This research proposes an intelligent intrusion detection framework that utilizes machine learning algorithms to detect cyber

attacks in network environments. The framework uses data preprocessing and feature selection techniques to improve detection performance. Multiple classifiers are applied to analyze network traffic and categorize different attack types. Experimental results demonstrate that ensemble learning methods provide better classification performance and reduce false positive rates in intrusion detection systems.

3. Title: Network Intrusion Detection Using Random Forest Classification

Author: Y. Xin, L. Kong, Z. Liu

Abstract—
This work focuses on the application of Random Forest classification for detecting malicious activities in network traffic. The proposed model analyzes various network features and builds multiple decision trees to classify attack patterns. The experimental analysis shows that Random Forest provides high detection accuracy and robustness when compared to traditional classification techniques. The research confirms that ensemble learning algorithms are effective for improving network security and intrusion detection.

4. Title: A Machine Learning Approach for Detecting Cyber Attacks in Cloud Networks

Author: A. S. Ashoor and S. Gore

Abstract—
The authors propose a machine learning-based model for detecting cyber attacks in cloud network environments. The system uses network traffic attributes and applies classification algorithms to identify malicious activities. Data preprocessing and feature extraction techniques are used to enhance model performance. The results demonstrate that machine learning models can efficiently detect multiple types of attacks and provide improved security for cloud communication systems.

5. Title: Extreme Gradient Boosting for Cyber Attack Detection

Author: T. Chen and C. Guestrin

Abstract—
This study introduces Extreme Gradient Boosting (XGBoost), a scalable machine learning algorithm designed for efficient classification and prediction tasks. The algorithm combines gradient boosting techniques with optimized computation to achieve high accuracy and speed. XGBoost has been widely used in cybersecurity applications for detecting anomalies and classifying attack types in network traffic data. Experimental evaluations show that XGBoost outperforms many traditional machine learning algorithms in classification performance.

III. EXISTING SYSTEM

In traditional cloud computing environments, security mechanisms mainly rely on rule-based firewalls, signature-based intrusion detection systems (IDS), and manual monitoring techniques to identify malicious activities. These systems analyze network traffic using predefined rules or known attack signatures to detect potential threats. When suspicious traffic patterns match stored signatures, the system generates alerts for administrators. Although these approaches provide basic protection for cloud communication networks, they are mainly designed to detect previously known attacks. With the rapid growth of cloud infrastructure and the increasing complexity of cyber threats, traditional security systems often struggle to process large volumes of network data and identify sophisticated or newly emerging attack patterns. As a result, these conventional approaches may not provide efficient or real-time detection of

malicious activities in modern cloud environments.

IV. PROPOSED SYSTEM

The proposed system introduces an intelligent machine learning–based framework to enhance the security of cloud data communication by detecting and classifying potential cyber attacks in network traffic. The system utilizes a cloud security dataset containing network attributes such as source IP address, destination IP address, protocol type, packet size, login time, country, and risk score. Feature engineering techniques are applied to extract subnet and host information from IP addresses, which helps improve the model's ability to analyze communication patterns. Data preprocessing methods such as label encoding and feature scaling are performed to prepare the dataset for effective model training. Multiple machine learning algorithms, including Random Forest, Gradient Boosting, and XGBoost, are implemented to identify different types of attacks in cloud communication. The models are trained and evaluated using performance metrics such as accuracy score, classification report, and confusion matrix. The system is integrated with a Django-based web application that allows administrators or users to view the dataset, train the models, and predict potential attack types by providing network communication details. By applying intelligent learning techniques, the proposed system improves the accuracy and efficiency of detecting malicious activities in cloud environments.

V. SYSTEM ARCHITECTURE

The presented diagram illustrates the system architecture for improving cloud data communication security using intelligent machine learning models. The system begins with two main components: the cloud network and the user interface. The cloud network represents the infrastructure where data is transmitted and stored, while the user interface allows users or administrators to interact with the system. During communication between these components, network traffic data is generated. This traffic contains important information about the data packets, communication patterns, and system behavior. The collected traffic data is then stored in a cloud security dataset, which acts as the foundation for further analysis and machine learning processing.

After collecting the dataset, the next stage is data preprocessing, which prepares the raw network traffic data for machine learning algorithms. In this phase, feature engineering is performed to extract meaningful attributes from the dataset, such as packet size, protocol type, or connection duration. These features help the model understand patterns in network activity. Additionally, label encoding and scaling are applied to convert categorical data into numerical form and normalize feature values. This step improves the efficiency and accuracy of the machine learning models by ensuring that the data is structured and consistent.

Once preprocessing is completed, the processed data is fed into multiple machine learning classifiers, including Random Forest, Gradient Boosting, and XGBoost. These algorithms are ensemble learning methods known for their high performance in classification tasks. Each model analyzes the processed network data to detect patterns associated with normal or malicious communication behavior. By applying multiple classifiers, the system can improve prediction accuracy and robustness in identifying different types of cyber threats within cloud environments.

The outputs of these classifiers are then used for attack prediction and classification. In this stage, the system determines whether the network traffic represents legitimate

activity or a potential security attack, such as intrusion attempts or abnormal data transmission. Based on the model predictions, the system generates alerts and displays results to administrators through the interface, enabling quick response to security threats. Additionally, a confusion matrix and performance reports are produced to evaluate the accuracy, precision, recall, and overall effectiveness of the machine learning models. This evaluation helps in understanding the reliability of the system and in improving future model performance for enhanced cloud communication security.

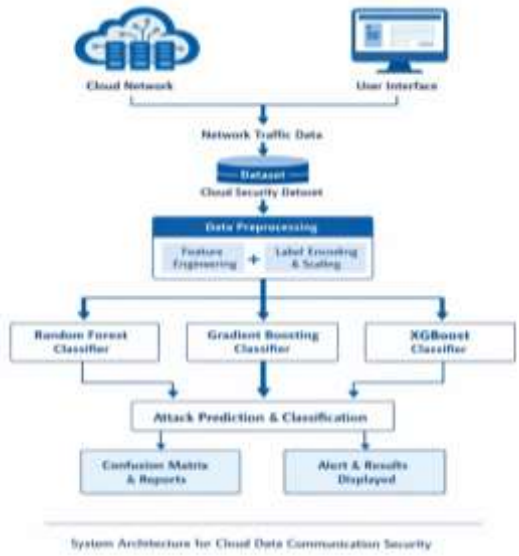

Fig 5.1: System Architecture Of Proposed System

VI. IMPLEMENTATION

Fig 6.1: Admin Home

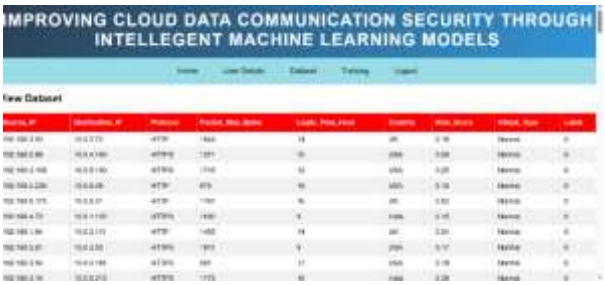

Fig 6.2: Load Dataset

Fig 6.3: Model Training

Fig 6.4: Prediction Page

Fig 6.5: Result Page

VII. CONCLUSION

This project presents an intelligent machine learning–based framework for improving

cloud data communication security by detecting and classifying potential cyber attacks in network traffic. The system analyzes various network communication features such as source IP address, destination IP address, protocol type, packet size, login time, country, and risk score to identify suspicious activities in cloud environments. Feature engineering techniques are applied to extract subnet and host information from IP addresses, and data preprocessing methods such as label encoding and feature scaling are used to prepare the dataset for effective model training.

Multiple machine learning algorithms, including Random Forest, Gradient Boosting, and XGBoost, are implemented and evaluated to identify attack patterns in the cloud security dataset. The models are trained and tested using appropriate evaluation metrics such as accuracy score, classification report, and confusion matrix. Among the implemented models, the XGBoost classifier demonstrates better performance in predicting attack types and detecting malicious network behavior.

The system is integrated with a Django-based web application that provides functionalities such as user registration, login, dataset viewing, model training, and real-time attack prediction. By combining machine learning techniques with a web-based interface, the proposed system enables efficient monitoring and detection of security threats in cloud communication. Overall, the system contributes to enhancing the reliability, security, and protection of cloud computing environments by providing an intelligent approach for early detection of cyber attacks.

VIII. FUTURE SCOPE

The proposed system can be further enhanced in several ways to improve the effectiveness and applicability of cloud communication security. One potential improvement is the integration of real-time network traffic monitoring, which would allow the system to analyze live cloud communication data and detect attacks instantly. The system can also be extended by incorporating deep learning techniques, such as Convolutional Neural Networks (CNN) or Long Short-Term Memory (LSTM) networks, to capture more complex patterns in network traffic and further improve prediction accuracy.

Another possible enhancement is the development of a mobile or cloud-based monitoring dashboard that allows administrators to track security alerts and attack predictions from anywhere. The system can also be expanded to support larger and more diverse cloud security datasets, which would improve the robustness and generalization of the machine learning models. Additionally, implementing explainable artificial intelligence (XAI) techniques could help provide insights into why a particular attack is predicted, making the system more transparent and trustworthy for administrators.

Future versions of the system may also integrate automated response mechanisms, where detected threats trigger immediate defensive actions such as blocking suspicious IP addresses or generating alerts for system administrators. By incorporating these improvements, the system can evolve into a more advanced and intelligent cloud security solution capable of handling complex and emerging cyber threats in modern cloud environments.

IX. REFERENCES

[1] H. Attou, A. Guezzaz, S. Benkirane, and M. Azrour, “Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques,” *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311–320, 2023. doi: 10.26599/BDMA.2022.9020038.

[2] T. Sowmya and E. A. M. Anita, "A Comprehensive Review of AI-Based Intrusion Detection Systems," *Measurement: Sensors*, 2023. doi: 10.1016/j.measen.2023.100827.

[3] A. Pinto et al., "A Survey on Intrusion Detection Systems Using Machine Learning," *Sensors*, vol. 23, no. 5, p. 2415, 2023. doi: 10.3390/s23052415.

[4] S. Neupane et al., "Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities," *IEEE Access*, vol. 10, pp. 112392–112415, 2022. doi: 10.1109/ACCESS.2022.3216617.

[5] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," *IEEE Access*, 2023. doi: 10.1109/ACCESS.2023.3296444.

[6] M. Mayuranathan et al., "An Efficient Optimal Security System for Intrusion Detection in Cloud Computing Using Hybrid Deep Learning," *Information Processing & Management*, 2022. doi: 10.1016/j.ipm.2022.102839.

[7] W. H. Aljuaid et al., "A Deep Learning Approach for Intrusion Detection Systems in Cloud Environments," *Applied Sciences*, vol. 14, no. 13, 2024. doi: 10.3390/app14135381.

[8] B. C. Preethi, R. Vasanthi, G. Sugitha, and S. A. Lakshmi, "Multiscale Deep Bidirectional GRU for Intrusion Detection in Cloud Systems," *Expert Systems with Applications*, 2024. doi: 10.1016/j.eswa.2024.124428.

[9] S. S. Nasim, P. Pranav, and S. Dutta, "A Systematic Literature Review on Intrusion Detection Techniques in Cloud Computing," *Discover Computing*, 2025. doi: 10.1007/s10791-025-09641-y.

[10] L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computer Network Security," *Computers*, vol. 14, no. 3, 2025. doi: 10.3390/computers14030087.

[11] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, "Intrusion Detection System and Intrusion Learning: Bridging the Gap Between Hype and Reality," in *Proc. Int. Conf. Advanced Computing and Emerging Technologies (ACET)*, IEEE, 2024. doi: 10.1109/ACET61898.2024.10730334.

[12] A. Hozouri et al., "A Comprehensive Survey on Intrusion Detection Systems and Machine Learning Approaches," 2025. doi: 10.1007/s44163-025-00578-1.

[13] S. A. Ahmed et al., "Comparative Analysis of RNN, CNN and LSTM Models for Cloud Security," *Engineering, Technology & Applied Science Research*, 2025. doi: 10.48084/etasr.9445.

[14] S. K. Mandal et al., "Machine Learning-Driven Intrusion Detection System for Network Security," *Expert Systems with Applications*, 2025. doi: 10.1016/j.eswa.2025.122407.

[15] Q. O. Ahmed, "Machine Learning for Intrusion Detection in Cloud Environments: A Comparative Study," *Journal of Artificial Intelligence and General Science*, 2024. doi: 10.60087/jaigs.v6i1.287.