International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

An Intelligent Machine Learning Framework for Cloud Vulnerability Detection and Threat Prevention

Mrs. Ch.Sowjanya[1] , Kadari Jagadeeswara Veerraju[2], Yerra Pallavi Rani[3], Ganni Sameera[4], Bobbili Lakshmi[5] , Thumu Jayanth[6]

[1]Assistant Professor , [2,3,4,5,6] B.tech Students Department ofCSE, Pragati Engineering College, Surampalem , Andhra Pradesh, India

Abstract- — Cloud computing has transformed the way organizations store data, deploy applications, and manage digital infrastructure. Its scalability, flexibility, and cost efficiency have made it an essential technology for modern businesses. However, as cloud environments grow in size and complexity, they also become more vulnerable to various cybersecurity threats. Issues such as misconfigurations, insecure APIs, weak authentication mechanisms, and unauthorized access can expose cloud systems to serious security risks. Traditional security mechanisms such as firewalls and rule-based intrusion detection systems often struggle to detect new or evolving threats in dynamic cloud environments.To address these challenges, this work explores the use of machine learning techniques to improve cloud security by predicting and detecting vulnerabilities in distributed systems. The proposed approach analyses security-related data such as system logs, network traffic patterns, and vulnerability reports to identify abnormal behaviour and potential threats. Multiple machine learning algorithms, including Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest, are evaluated to determine their effectiveness in detecting security vulnerabilities.The experimental results indicate that ensemble models, particularly Random Forest, provide higher accuracy and better detection capability compared to other algorithms. Machine learning-based security systems can analyse large volumes of data in real time, identify suspicious patterns, and respond to potential threats more quickly than traditional security approaches.By integrating machine learning into cloud security frameworks, organizations can build more proactive and intelligent defence systems capable of adapting to evolving cyber threats. The proposed approach enhances vulnerability detection, reduces response time to security incidents, and supports the development of more resilient and secure cloud infrastructures.

Keywords :Cloud Security, Machine Learning, Vulnerability Detection, Distributed Systems, Anomaly Detection, Cybersecurity, Predictive Analytics, Threat Detection.

I. INTRODUCTION

Cloud computing has emerged as one of the most transformative technologies in modern information systems, enabling organizations to store data, deploy applications, and manage computing resources through remote servers rather than relying solely on local infrastructure. The advantages of cloud computing, including scalability, flexibility, cost efficiency, and accessibility, have encouraged businesses and institutions across multiple sectors such as finance, healthcare, education, and e-commerce to migrate their services and data to cloud platforms. As a result, cloud environments have become an essential component of modern digital infrastructures and enterprise information systems [1], [11].

Despite these advantages, the rapid adoption of cloud computing has introduced several significant security challenges. Cloud systems are typically distributed across multiple servers, networks, and geographical locations, making them complex to manage and protect. Security threats such as data breaches, unauthorized access, insecure application programming interfaces (APIs), configuration vulnerabilities, and distributed denial-of-service (DDoS) attacks can compromise the reliability, confidentiality, and availability of cloud services. Due to the dynamic and large-scale nature of cloud environments, traditional security mechanisms often struggle to detect and mitigate sophisticated cyber threats effectively [10], [13].

Conventional cloud security solutions generally rely on rule-based or signature-based detection mechanisms. Although these approaches are capable of identifying known attack patterns, they often fail to detect previously unseen threats or abnormal system behaviours within large-scale cloud infrastructures. Furthermore, the enormous volume of log data, network traffic information, and system activity generated in cloud environments makes manual monitoring and analysis extremely difficult for security administrators. Consequently, there is a growing demand for intelligent and automated security mechanisms capable of detecting vulnerabilities and responding to threats in real time [11], [12].

Machine learning has emerged as a promising approach for strengthening cloud security by enabling intelligent threat detection and predictive analysis. Machine learning algorithms can analyse large-scale datasets, identify hidden patterns, and detect anomalies that may indicate potential security breaches. Unlike traditional security systems, machine learning models can continuously learn from new data and adapt to evolving cyber threats. This adaptability makes machine learning particularly suitable for monitoring distributed cloud infrastructures where attacks may originate from multiple sources and evolve rapidly over time [1], [10].

Recent research has demonstrated the effectiveness of machine learning techniques in addressing cybersecurity challenges across various domains. Machine learning-based security systems have been applied to intrusion detection, vulnerability analysis, anomaly detection, and network traffic monitoring in cloud and IoT environments. These intelligent systems improve detection accuracy and enhance the overall resilience of cloud infrastructures against cyber threats [4], [9]. Additionally, advances in artificial intelligence and deep learning have enabled the development of sophisticated predictive models capable of improving threat detection and decision-making in complex computing environments [7], [8].

In this study, a machine learning-based cloud security framework is proposed to predict and detect vulnerabilities in distributed cloud systems. The proposed framework analyses various types of security-related data, including system logs, network traffic information, and vulnerability reports, to identify abnormal behaviour that may indicate potential security threats. Several machine learning algorithms, including Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest, are evaluated to determine their effectiveness in detecting cloud security vulnerabilities.

The main objective of this research is to develop an intelligent and automated cloud security approach that assists organizations in identifying potential threats at an early stage and reducing the risk of security breaches. By integrating machine learning techniques with cloud security mechanisms, the proposed system aims to enhance threat detection capabilities, reduce false alarms, and improve the overall protection of distributed cloud infrastructures.

The remainder of this paper is organized as follows. Section II reviews existing research related to machine learning applications in cloud security. Section III describes the system analysis and the proposed methodology for vulnerability detection. Section IV explains the implementation process and machine learning models used in the study. Section V presents the experimental results and performance evaluation of the proposed system. Finally, Section VI concludes the study and discusses possible future improvements in intelligent cloud security systems.

II. LITERATURESURVEY

With the rapid growth of cloud computing technologies, ensuring the security of distributed cloud environments has become a critical concern for both researchers and organizations. Cloud infrastructures host large volumes of sensitive data and critical applications, making them attractive targets for cyberattacks. Consequently, significant research efforts have been directed toward developing advanced security mechanisms capable of identifying vulnerabilities and preventing potential cyber threats. In recent years, machine learning techniques have emerged as powerful tools for enhancing cloud security systems due to their ability to analyse large datasets and detect abnormal patterns within complex computing environments [1], [11].

Several researchers have explored the application of machine learning algorithms for identifying security threats in cloud infrastructures. Alenezi et al. conducted a comprehensive survey on the use of machine learning techniques for improving cloud security. Their study highlighted that machine learning models can automatically analyse large-scale data generated by cloud infrastructures, enabling the detection of anomalies that may indicate potential security breaches. The authors concluded that machine learning-based security mechanisms can significantly improve the efficiency and automation of cloud security management systems [1].

Similarly, Zhang et al. investigated the use of machine learning approaches for vulnerability detection in distributed cloud systems. Their research demonstrated that supervised learning algorithms such as Decision Trees and Random Forest models can effectively analyse system activity data and identify potential security vulnerabilities before they cause system failures or data breaches. By analysing patterns in historical system logs and network traffic data, machine learning models can provide early warnings of possible threats within cloud infrastructures [10], [12].

Kumar et al. proposed a machine learning-based security analysis model for IoT and cloud ecosystems, emphasizing the importance of anomaly detection techniques for identifying unusual activities within distributed environments. Their research demonstrated that machine learning algorithms can analyse system behaviour and detect deviations from normal

operational patterns, thereby enabling the identification of suspicious activities that may indicate cyberattacks [4].

Unsupervised learning techniques have also been widely investigated for anomaly detection in cloud security systems. These techniques are particularly useful for identifying previously unknown attack patterns because they do not rely on predefined labels or training datasets. Liu and Wu evaluated several machine learning models for cloud security in hybrid computing environments and reported that unsupervised models can effectively detect anomalies within large-scale cloud infrastructures [12].

In addition to anomaly detection, optimization-based and hybrid machine learning techniques have been explored to improve the effectiveness of cloud security mechanisms. Devi et al. proposed an optimization-based defence mechanism for detecting distributed denial-of-service (DDoS) attacks using artificial intelligence algorithms. Their approach integrates advanced optimization techniques with machine learning models to enhance the detection accuracy of intrusion detection systems in distributed computing environments [9].

Recent studies have also examined hybrid security frameworks that combine multiple machine learning algorithms to improve detection performance. Hybrid approaches integrate supervised and unsupervised learning models to analyse different types of security data and detect vulnerabilities more effectively. Such approaches have been shown to improve threat detection accuracy compared to single-model systems, particularly in complex distributed environments [13].

Furthermore, advances in deep learning have introduced new possibilities for improving security detection systems. Deep neural network architectures have demonstrated the ability to learn complex feature representations from large datasets, enabling more accurate detection of sophisticated cyber threats. Deep learning models have been successfully applied in various intelligent systems such as computer vision, medical image analysis, and pattern recognition, highlighting their potential for improving cybersecurity applications [7], [16], [19].

Despite these advancements, several challenges remain in applying machine learning to cloud security systems. Many existing approaches rely on limited datasets that may not fully represent the complexity of real-world cloud infrastructures. Additionally, cyber threats continue to evolve rapidly, requiring adaptive security systems capable of continuously learning and responding to new attack patterns. Therefore, there is a growing need for intelligent cloud security frameworks that integrate multiple machine learning techniques to improve vulnerability detection and threat prevention capabilities.

The present study addresses this challenge by evaluating different machine learning algorithms and integrating them into a cloud security framework designed to detect anomalies, predict vulnerabilities, and enhance overall protection for distributed cloud infrastructures. By combining multiple machine learning models and analysing various types of security-related data, the proposed system aims to improve threat detection accuracy and provide a more robust cloud security solution.

III.SYSTEM ANALYSIS

A. Existing System

Traditional cloud security systems primarily rely on rule-based security mechanisms such as firewalls, intrusion detection systems (IDS), and signature-based threat detection techniques. These approaches monitor system activity and compare it against predefined rules or known attack signatures in order to identify potential security threats. While such systems can effectively detect previously identified attacks, they often struggle to recognize new or previously unseen vulnerabilities within distributed cloud environments. The dynamic nature of cloud infrastructures makes it difficult for static security mechanisms to adapt to evolving cyber threats [10], [11].

In many cloud infrastructures, security monitoring is performed through manual analysis of system logs, network traffic data, and vulnerability reports. Security administrators analyse this information to identify suspicious behaviour and respond to potential threats. However, as cloud systems grow larger and more complex, the volume of security data generated by distributed infrastructures increases significantly. This large amount of data makes manual monitoring inefficient and increases the likelihood of delayed threat detection [1], [12].

To address these limitations, some existing studies have applied traditional machine learning models such as Decision Trees, Support Vector Machines (SVM), Random Forest, and K-Nearest Neighbors (KNN) for anomaly detection in cloud environments. These models analyse patterns within system logs and network activity to identify abnormal behaviours that may indicate potential security risks. Machine learning-based approaches have demonstrated improved detection capabilities compared to purely rule-based systems by enabling automated analysis of large-scale datasets [13].

However, many of these implementations rely on standalone machine learning models, which may not fully capture the complex relationships between multiple components of distributed cloud infrastructures. Cloud environments often involve interconnected services, virtual machines, network layers, and storage systems, making it difficult for single-model approaches to effectively analyse security risks across the entire system architecture [4].

Furthermore, several existing cloud security solutions focus exclusively on either supervised learning techniques or anomaly detection models. This limited approach may reduce the system's ability to respond to rapidly evolving cyber threats. As attackers continuously develop new techniques to exploit vulnerabilities in cloud infrastructure, traditional security systems may fail to detect sophisticated attacks, including zero-day vulnerabilities and advanced persistent threats [9].

Disadvantages Of The Existing System

Limited ability to detect unknown threats:
Traditional security systems rely heavily on predefined rules or signatures, which makes them ineffective in identifying new and previously unseen cyberattacks [10].
High false alarm rates:
Rule-based intrusion detection systems may generate a large number of false positives, making it difficult for security administrators to accurately identify real security threats.
Manual monitoring challenges:
Security analysts must manually analyse large volumes of system logs and network data, which is time-consuming and inefficient in large-scale cloud environments [1].
Scalability issues:
As cloud infrastructures expand, traditional monitoring systems often struggle to process the increasing volume of security-related data generated by distributed systems [12].
Slow response to evolving threats:
Static security rules cannot easily adapt to new attack patterns, reducing the overall effectiveness of traditional cloud security mechanisms [11].
Complex system environments:
Cloud infrastructures consist of multiple interconnected services and platforms, making it difficult for traditional tools to analyse security risks across the entire distributed system architecture [4].

B. Proposed System

To address the limitations of traditional cloud security mechanisms, this study proposes a machine learning-based cloud security framework designed to detect vulnerabilities in distributed cloud environments. The proposed framework utilizes intelligent data analysis techniques to continuously monitor cloud infrastructures and identify abnormal activities that may indicate potential security threats. Machine learning approaches have demonstrated strong capabilities in analysing large-scale datasets and improving threat detection in cloud systems [1], [11].

The process begins with collecting security-related data from multiple sources within the cloud environment. These sources include system logs, network traffic records, vulnerability databases, and cloud service activity logs. Such data provide valuable insights into system behaviour and potential security risks. Data collection from multiple sources allows the proposed framework to analyse both network-level and application-level security events within the cloud infrastructure [10], [12].

After the data collection stage, data preprocessing techniques are applied to improve the quality and usability of the dataset. This process includes cleaning the data, removing missing or inconsistent values, and transforming raw security data into structured formats suitable for machine learning algorithms. Data preprocessing is an essential step in security analytics because it ensures that the machine learning models can accurately identify patterns and anomalies within the dataset [4].
Once the dataset is prepared, several machine learning models are trained to analyse patterns within the data and detect potential vulnerabilities. The algorithms used in this study include Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest. These models are widely used in cybersecurity applications because they can analyse large datasets and identify abnormal system behaviour that may indicate cyber threats or security vulnerabilities [13].

To enhance the effectiveness of the proposed framework, model optimization techniques such as hyperparameter tuning and cross-validation are applied during the training process. These optimization methods help improve the generalization capability of the models and prevent overfitting, thereby ensuring reliable performance when analysing previously unseen security data.

Furthermore, the proposed system integrates both supervised and unsupervised learning techniques to improve threat detection capabilities. Supervised learning models are used to classify known vulnerabilities and attack patterns based on labelled datasets, while unsupervised anomaly detection models such as Isolation Forest are applied to detect unusual

system behaviours that may indicate previously unknown or emerging cyber threats. Combining multiple machine learning techniques enables the system to identify both known and unknown attack patterns within distributed cloud infrastructures [9].

By integrating multiple machine learning algorithms within a unified framework, the proposed system enables real-time threat detection, automated vulnerability analysis, and continuous learning from new security data. This intelligent approach allows cloud security systems to adapt to evolving cyber threats and provides a proactive defence mechanism for distributed cloud environments. The proposed machine learning-based framework therefore improves the efficiency, accuracy, and adaptability of cloud security monitoring systems [1], [10].

IV. SYSTEM DESIGN

System Architecture

Below diagram depicts the whole system architecture.

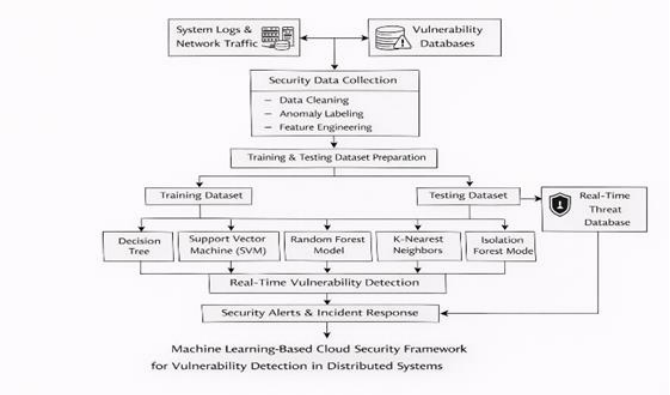

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

Modules

1. Data Collection and Preprocessing

The first stage of the proposed system focuses on collecting relevant security-related data from distributed cloud environments. These data sources include system logs, network traffic records, vulnerability databases, and cloud service activity logs. Such information provides valuable insights into system behaviour and enables the identification of patterns associated with potential security threats and vulnerabilities in cloud infrastructures. Collecting data from multiple sources allows the framework to perform a comprehensive analysis of both network-level and application-level security events [10], [12].

After data collection, data preprocessing techniques are applied to improve the quality and usability of the dataset. This stage includes removing incomplete or corrupted records, handling missing values, and normalizing feature values to ensure compatibility with machine learning algorithms. Feature engineering techniques are also applied to extract meaningful attributes such as unusual login attempts, abnormal network traffic behaviour, or repeated configuration changes that may indicate potential security risks. Proper preprocessing of security datasets plays a crucial role in improving the accuracy and reliability of machine learning-based security detection systems [4].

2. Feature Selection and Data Analysis

Once preprocessing is completed, the dataset is analysed to identify the most relevant features for detecting vulnerabilities and abnormal behaviour within cloud systems. Feature selection techniques help reduce unnecessary data dimensions and improve the efficiency of machine learning models by focusing only on the most significant attributes.

Statistical analysis and correlation methods are applied to identify relationships among different variables within the dataset. These techniques help uncover patterns associated with security threats and improve the ability of machine learning models to accurately identify vulnerabilities. Feature analysis is particularly important in cloud security systems because distributed infrastructures generate large volumes of heterogeneous data [1].

3. Training Machine Learning Models

In this stage, several machine learning algorithms are trained using the prepared dataset. The models used in this study include Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest. These algorithms are widely used in cybersecurity applications due to their ability to analyse large datasets and detect abnormal system behaviours.

During the training phase, the models learn patterns associated with both normal and abnormal system activity. Historical

security data is used to enable the models to recognize potential vulnerabilities and cyber threats within cloud infrastructures. Additionally, hyperparameter tuning techniques are applied to optimize the performance of the models and ensure accurate predictions when analysing new security data [13].

4. Real-Time Threat Detection

After the machine learning models are trained, they are integrated into the cloud security framework to enable real-time monitoring of system activities. Incoming data from system logs, network traffic records, and service activity logs are continuously analysed by the trained models to detect anomalies or suspicious activities.

If unusual behaviour is detected, the system identifies it as a potential vulnerability or cyber threat and generates an alert for further investigation. This real-time monitoring capability enables faster detection of cyberattacks and reduces the risk of damage to cloud infrastructures. Machine learning-based detection systems are particularly effective for identifying previously unknown threats and abnormal patterns in distributed computing environments [9].

5. Model Evaluation and Continuous Learning

The effectiveness of the machine learning models is evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, and AUC–ROC. These evaluation metrics provide detailed insights into how effectively the models detect vulnerabilities and distinguish between normal and abnormal system behaviour.

Furthermore, the proposed framework supports continuous learning, allowing models to be updated and retrained as new security data becomes available. Continuous learning enables the system to adapt to evolving cyber threats and improve detection accuracy over time. Adaptive machine learning systems are essential for maintaining robust security in dynamic cloud environments where attack patterns frequently change [1],

VI. RESULTS AND DISCUSSION

To evaluate the performance of the proposed machine learning-based cloud security framework, several machine learning algorithms were implemented and tested using the prepared security dataset. The dataset included system logs, network traffic records, and vulnerability-related information collected from cloud environments. Each model was evaluated using commonly used performance metrics such as accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). These metrics provide a comprehensive assessment of the effectiveness of machine learning models in detecting vulnerabilities and identifying abnormal behaviour within cloud infrastructures [1], [12].

Several machine learning algorithms were evaluated in this study, including Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest. These models were trained using the pre-processed dataset and tested to determine their ability to classify normal system behaviour and potential security threats. Machine learning-based detection systems have been widely used in cloud security research due to their capability to analyse large-scale datasets and identify complex patterns associated with cyber threats [10], [13].

Table 1
Performance Comparison of Machine Learning Models for Cloud Security Detection

Model	Accuracy (%)	Precision	Recall	F1-Score	AUC
Decision Tree	87.3	0.86	0.85	0.85	0.88
Support Vector Machine	89.1	0.88	0.87	0.87	0.90
Random Forest	93.4	0.92	0.91	0.91	0.94
K-Nearest Neighbors	85.6	0.84	0.83	0.83	0.86
Isolation Forest	88.2	0.87	0.88	0.87	0.89

As shown in Table 1, the Random Forest algorithm achieved the best overall performance, providing the highest accuracy, precision, recall, and F1-score among the evaluated models. The ensemble structure of Random Forest allows it to analyse complex patterns within large datasets by combining the outputs of multiple decision trees. This capability enables the model to effectively detect security vulnerabilities and abnormal system behaviour in cloud infrastructures [1].

The Decision Tree and Support Vector Machine (SVM) models also demonstrated strong performance in identifying security

threats. These models were able to detect patterns associated with abnormal system behaviour; however, they occasionally produced slightly lower accuracy compared to Random Forest due to limitations in handling highly complex and high-dimensional datasets.

The K-Nearest Neighbors (KNN) algorithm achieved moderate performance. While KNN can effectively classify data based on similarity measures, it requires higher computational resources when processing large-scale datasets commonly found in distributed cloud environments.

The Isolation Forest algorithm, which is specifically designed for anomaly detection, demonstrated promising results in identifying unusual patterns within unlabelled data. This model is particularly useful for detecting previously unknown threats because it isolates anomalous data points without requiring labelled training datasets.

ROC Curve Analysis
To further analyse model performance, a Receiver Operating Characteristic (ROC) curve was generated for the evaluated models. The ROC curve illustrates the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) at different classification thresholds.

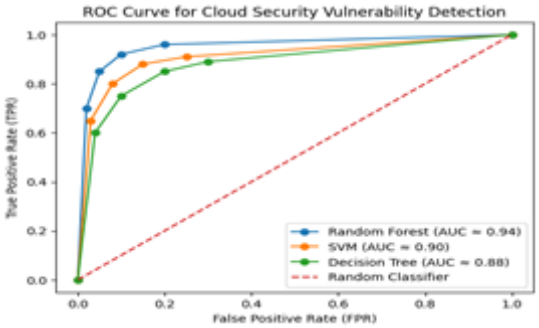

Fig. 2. ROC Curve for Machine Learning-Based Cloud Security Detection

The ROC analysis indicates that the Random Forest model achieved the highest AUC value of approximately 0.94, demonstrating strong capability in distinguishing between normal system behaviour and potential security threats. A higher AUC value indicates better classification performance and improved detection accuracy.

Overall, the experimental results demonstrate that machine learning techniques significantly improve the detection of vulnerabilities and security threats in cloud environments. By combining supervised learning models with anomaly detection algorithms, the proposed framework provides a comprehensive cloud security solution capable of identifying both known and previously unknown threats. Machine learning-based approaches therefore offer a promising direction for enhancing security monitoring and threat detection in distributed cloud infrastructures [4], [9].

VII. CONCLUSION AND FUTURE WORK

This study presented a machine learning-based framework for enhancing cloud security by predicting and detecting vulnerabilities in distributed cloud environments. The proposed system integrates multiple machine learning algorithms to analyse cloud security data, including system logs, network traffic records, and vulnerability reports, in order to identify potential threats within complex cloud infrastructures. Machine learning techniques have demonstrated strong potential in improving cloud security systems by enabling automated analysis of large-scale datasets and detecting abnormal patterns associated with cyber threats [1], [11].

The experimental results demonstrate that machine learning models can effectively detect vulnerabilities and abnormal activities within cloud environments. Among the evaluated algorithms, theRandom Forest model achieved the highest accuracy and overall performance, indicating its effectiveness in identifying potential security risks in distributed cloud infrastructures. Ensemble learning methods such as Random Forest are particularly effective for security analysis because they combine multiple decision trees to capture complex patterns and improve detection accuracy [10], [13].

By integrating machine learning techniques into cloud security frameworks, organizations can significantly enhance their ability to monitor large-scale cloud environments and respond rapidly to emerging cyber threats. The proposed framework enables automated vulnerability detection, anomaly identification, and intelligent analysis of security events, thereby reducing false alarms and improving the reliability of security monitoring systems. Machine learning-based security mechanisms can therefore play a critical role in strengthening the protection of cloud infrastructures against evolving cyberattacks [4], [12].

For future work, the proposed framework can be extended by incorporating advanced deep learning techniques and larger security datasets to further improve detection accuracy and system scalability. Deep learning models have demonstrated strong capabilities in analysing complex patterns in large

datasets and may enhance the detection of sophisticated cyber threats in distributed computing environments [7], [16], [19].

In addition, integrating the framework with real-time cloud monitoring platforms and automated responsemechanismscan further enhance the capability of the system to detect and mitigate cyber threats in modern cloud infrastructures. Future research may also explore hybrid machine learning approaches and optimization techniques to improve threat detection performance and support adaptive cloud security systems capable of responding dynamically to evolving attack patterns [9], [18].

Overall, the integration of machine learning with cloud security mechanisms represents a promising approach for developing intelligent and adaptive security systems capable of protecting distributed cloud infrastructures against increasingly sophisticated cyber threats.

REFERENCES :

1. M. Alenezi, F. Alhaidari, and F. Alsaadi, "Machine learning for cloud security: A survey," Journal of Cloud Computing: Advances, Systems and Applications, vol. 10, no. 1, pp. 1–18, 2021.
2. S. Mukhopadhyay, A. Kumar, J. Gupta, A. Bhatnagar, M. P. Kantipudi, and M. Singh, "A review and analysis of IoT enabled smart transportation using machine learning techniques," International Journal of Transport Development and Integration, vol. 8, no. 1, pp. 61–77, Mar. 2024, doi:10.18280/ijtdi.080106.
3. V. Agrawal, J. Jagtap, and M. P. Kantipudi, "An overview of hand-drawn diagram recognition methods and applications," IEEE Access, vol. 12, pp. 19739–19751, 2024, doi:10.1109/ACCESS.2024.3357398.
4. P. Kumar N. S., P. N., S. S., R. Aluvalu, and J. Jagtap, "A security analysis model for IoT ecosystem using machine learning approach," Recent Advances in Computer Science and Communications, vol. 17, no. 6, 2024, doi:10.2174/0126662558286885240223093414.
5. V. Agrawal and J. Jagtap, "Exploration of advancements in handwritten document recognition techniques," Intelligent Systems with Applications, vol. 22, p. 200358, 2024, doi:10.1016/j.iswa.2024.200358.
6. V. Kumar, C. Sen, A. Jain, A. Jain, and A. Sharma, "Analysis of business intelligence in healthcare using machine learning," in Optimized Predictive Models in Healthcare Using Machine Learning, 2024, pp. 329–339.
7. S. Kumar, D. Ghai, A. Jain, S. L. Tripathi, and S. Rani, Multimodal Biometric and Machine Learning Technologies: Applications for Computer Vision. Hoboken, NJ, USA: John Wiley & Sons, 2023.
8. K. B. Rao, Y. Bhardwaj, G. E. Rao, J. Gurrala, A. Jain, and K. Gupta, "Early lung cancer prediction by AI-inspired algorithm," in Proc. IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2023, pp. 1466–1469.
9. S. Devi, Y. K. Sharma, S. Athithan, S. Sachi, A. K. Singh, and A. Jain, "Implementation of ABC & WOA-based security defense mechanism for distributed denial-of-service attacks," in Proc. International Conference on Contemporary Computing and Informatics (IC3I), IEEE, 2023, pp. 546–551.
10. Y. Zhang, W. Li, and L. Jiang, "Cloud security: A machine learning perspective on vulnerability detection and prevention," Journal of Cyber Security, vol. 17, no. 2, pp. 124–136, 2019.
11. S. Radha and M. Reddy, "Machine learning applications in cloud computing for security management," International Journal of Cloud Computing and Services Science, vol. 8, no. 2, pp. 89–101, 2019.
12. J. Liu and J. Wu, "Evaluating machine learning models for cloud security in hybrid environments," International Journal of Cloud Applications and Computing, vol. 10, no. 4, pp. 15–28, 2020.
13. S. Ali and A. Ahmed, "Cloud security using supervised machine learning techniques," Journal of Cloud Computing, vol. 7, no. 1, pp. 1–10, 2018.
14. S. Kumar, A. Jain, S. Rani, D. Ghai, S. Achampeta, and P. Raja, "Enhanced SBIR based re-ranking and relevance feedback," in Proc. International Conference on System Modeling& Advancement in Research Trends (SMART), 2021, pp. 7–12.
15. K. Lakhwani and S. Kumar, "Knowledge vector representation of three-dimensional convex polyhedrons and reconstruction of medical images using knowledge vector," Multimedia Tools and Applications, vol. 82, no. 23, pp. 36449–36477, 2023.
16. S. Rani, D. Ghai, M. P. Kantipudi, A. H. Alharbi, and M. A. Ullah, "Efficient 3D AlexNet architecture for object recognition using syntactic patterns from medical images," Computational Intelligence and Neuroscience, vol. 2022, 2022.
17. K. Lakhwani and S. Kumar, "Three dimensional objects recognition and pattern recognition technique: Related challenges—A review," Multimedia Tools and Applications, vol. 81, no. 12, pp. 17303–17346, 2022.
18. H. Atri, A. Sharma, T. Mehrotra, and S. Saxena, "Optimization of network mapping for screening and intrusion sensing devices," in Proc. International

Conference on Cryptology & Network Security with Machine Learning, Springer, Singapore, 2023, pp. 1–19.
19. K. Kaushik, A. Bhardwaj, X. Cheng, S. Dahiya, A. Shankar, M. Kumar, and T. Mehrotra, "Residual network-based deep learning framework for diabetic retinopathy detection," Journal of Database Management, vol. 36, no. 1, pp. 1–21, 2025.
20. L. Sachan, P. Katiyar, Y. Kumbhawat, G. K. Rajput, and T. Mehrotra, "Comparative analysis on violence detection using YOLO and ResNet," in Proc. International Conference on System Modeling& Advancement in Research Trends (SMART), IEEE, 2023, pp. 89–92.
21. S. Vats et al., "Iterative enhancement fusion-based cascaded model for detection and localization of multiple diseases from CXR images," Expert Systems with Applications, Jun. 2024, doi:10.1016/j.eswa.2024.124464.