International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

A Robust Machine Learning Approach for Real-Time Cloud Vulnerability Detection and Threat Mitigation

Miss. Pemmanaboyina Durga Devi[1], Miss. Savarapu Suhasini[2]
[1]MTech in department of computer Science and Engineering,
[2]HOD of Computer science and Engineering In Lenora college of engineering, rampachodavaram , alluri seetharama raju district , Andhra Pradesh, India.

Abstract — Cloud computing has become the foundation of modern digital services by providing scalable, flexible, and cost-effective computing resources for organizations across various domains. Despite its widespread adoption, the increasing complexity of cloud infrastructures has introduced numerous security challenges, including unauthorized access, insecure configurations, application vulnerabilities, distributed denial-of-service (DDoS) attacks, and abnormal network activities. Conventional cloud security mechanisms primarily rely on rule-based detection techniques, which often struggle to identify sophisticated and previously unknown cyber threats in dynamic cloud environments. To overcome these limitations, this paper proposes an intelligent machine learning-based framework for cloud vulnerability detection and threat prevention. The proposed framework analyzes security-related information collected from system logs, network traffic records, cloud service activities, and vulnerability reports to identify malicious behavior and potential security risks. Comprehensive data preprocessing and feature engineering techniques are employed to improve data quality before training multiple machine learning models, including Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest. The effectiveness of these algorithms is evaluated using performance metrics such as accuracy, precision, recall, F1-score, confusion matrix, and ROC-AUC analysis. Experimental results demonstrate that the Random Forest model achieves superior detection performance by accurately identifying cloud vulnerabilities while maintaining a low false alarm rate. The proposed framework enables real-time threat monitoring, intelligent anomaly detection, and adaptive security analysis, thereby improving the resilience, reliability, and overall protection of distributed cloud infrastructures against evolving cyber threats.

Keywords— Cloud Security, Machine Learning, Vulnerability Detection, Threat Prevention, Cybersecurity, Anomaly Detection, Random Forest, Distributed Cloud Systems, Predictive Security Analytics.

I. INTRODUCTION

Cloud computing has revolutionized modern information technology by enabling organizations to access computing resources, storage, and software services through scalable and on-demand cloud platforms. Its flexibility, cost-effectiveness, and rapid deployment capabilities have accelerated the adoption of cloud technologies across diverse sectors, including healthcare, finance, education, manufacturing, government services, and e-commerce. As enterprises increasingly migrate critical applications and sensitive data to cloud environments, ensuring the security and reliability of distributed cloud infrastructures has become a fundamental requirement for maintaining business continuity and protecting digital assets [1], [11].

Despite the numerous advantages offered by cloud computing, the distributed and dynamic nature of cloud infrastructures introduces significant cybersecurity challenges. Cloud environments continuously generate massive volumes of system logs, network traffic records, authentication events, application activity, and virtual machine interactions, making security monitoring increasingly complex. Attackers frequently exploit vulnerabilities such as insecure configurations, weak authentication mechanisms, misconfigured access controls, insecure APIs, privilege escalation, distributed denial-of-service (DDoS) attacks, and unauthorized access to compromise cloud services. These threats can lead to data breaches, service disruptions, financial losses, and violations of regulatory compliance requirements [10], [12].

Traditional cloud security solutions primarily rely on rule-based intrusion detection systems, firewalls, signature-based malware detection, and manual security analysis. Although these mechanisms provide protection against known attack patterns, they often struggle to detect sophisticated, zero-day, and continuously evolving cyber threats. Furthermore, manually analyzing the enormous volume of security events generated in distributed cloud environments is both time-consuming and computationally challenging, making real-time threat detection increasingly difficult for security administrators [11], [13].

Recent advances in machine learning have provided intelligent solutions for addressing these limitations by enabling automated analysis of large-scale cloud security data. Machine learning algorithms can identify hidden relationships within system logs, recognize abnormal behavioral patterns, and detect security anomalies without relying solely on predefined attack signatures. Unlike conventional security mechanisms, intelligent learning models continuously improve their predictive capability by learning from historical and newly generated security data, making them highly effective for protecting dynamic cloud infrastructures against emerging cyber threats [1], [4].

Several supervised and unsupervised machine learning techniques have been successfully applied to cloud security applications, including intrusion detection, anomaly detection, malware classification, vulnerability assessment, and network traffic analysis. Algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Isolation Forest have demonstrated significant potential in improving detection accuracy while reducing false alarm rates. In particular, ensemble learning and anomaly detection techniques have shown remarkable performance in identifying both known attack patterns and previously unseen vulnerabilities within complex cloud environments [9], [10], [13].

Motivated by these advancements, this research proposes an intelligent machine learning-based framework for cloud vulnerability detection and threat prevention. The proposed framework integrates comprehensive data preprocessing, feature engineering, multiple machine learning models, anomaly detection, and real-time security monitoring to identify potential vulnerabilities within distributed cloud systems. Security-related information obtained from system logs, network traffic, cloud service activities, and vulnerability reports is analyzed to accurately distinguish normal operational behavior from malicious activities. By combining supervised classification with intelligent anomaly detection, the proposed framework enhances threat detection capability, improves response efficiency, and strengthens the overall security and resilience of cloud infrastructures against evolving cyber attacks [4], [10], [13].

The remainder of this paper is organized as follows. Section II presents a review of recent research on machine learning applications in cloud security and vulnerability detection. Section III discusses the existing security mechanisms and the proposed intelligent framework. Section IV describes the system architecture and implementation modules. Section V presents the experimental evaluation and comparative performance analysis of the implemented machine learning models. Finally, Section VI concludes the paper and outlines future research directions for intelligent cloud security systems.

II. LITERATURE SURVEY

The rapid adoption of cloud computing has significantly transformed modern computing infrastructures by providing scalable, flexible, and cost-efficient services for organizations worldwide. However, the increasing complexity of distributed cloud environments has also expanded the attack surface for cyber threats, making cloud security an active area of research. To address these challenges, researchers have explored various security mechanisms, including intrusion detection systems, anomaly detection techniques, vulnerability assessment frameworks, and intelligent machine learning models capable of identifying malicious activities within cloud infrastructures [1], [11].

Early cloud security solutions primarily relied on conventional protection mechanisms such as firewalls, encryption techniques, access control policies, authentication protocols, and signature-based intrusion detection systems. These approaches provide effective defense against known attack patterns by matching observed activities with predefined security rules. Although these techniques offer a basic level of protection, they often struggle to detect zero-day attacks, evolving malware, insider threats, and previously unseen vulnerabilities due to their dependence on static signatures and manually defined rules [10], [13].

Recent advancements in machine learning have introduced intelligent approaches for cloud vulnerability detection and cybersecurity monitoring. Supervised learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) have demonstrated strong capabilities in analyzing cloud system logs, network traffic, authentication records, and service activity data to classify normal and malicious behavior. These models automatically learn complex behavioral patterns from historical security datasets, enabling more accurate and efficient threat detection compared with traditional rule-based security systems [4], [10], [12].

Researchers have also investigated unsupervised learning techniques for detecting anomalies within distributed cloud environments. Algorithms such as Isolation Forest and clustering-based methods identify unusual system behavior without requiring labelled training data, making them highly effective for detecting previously unknown attacks and zero-day vulnerabilities. Anomaly detection has become an essential

component of modern cloud security frameworks because sophisticated cyber threats frequently evolve beyond predefined attack signatures [9], [12].

More recently, hybrid security frameworks integrating supervised learning, anomaly detection, optimization techniques, and ensemble machine learning have shown considerable improvements in cloud threat detection performance. Ensemble models combine the strengths of multiple classifiers to improve prediction accuracy, reduce false alarm rates, and enhance robustness when processing high-dimensional cloud security data. Several studies have reported that hybrid machine learning architectures outperform individual classifiers in identifying complex attack patterns while maintaining better scalability in large distributed cloud infrastructures [1], [9], [13].

Despite these significant advancements, several challenges continue to affect intelligent cloud security systems. Many existing models are trained using limited datasets that do not adequately represent the diversity and scale of real-world cloud environments. Furthermore, rapidly evolving cyber threats, increasing cloud service complexity, and the demand for real-time security analytics require adaptive learning models capable of continuously updating their knowledge from newly generated security data. Consequently, developing scalable, intelligent, and automated cloud vulnerability detection frameworks remains an important research direction for strengthening cybersecurity in next-generation distributed cloud systems [10], [11], [13].

III. SYSTEM ANALYSIS

1. Existing System

Existing cloud security frameworks primarily depend on traditional cybersecurity mechanisms such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, encryption techniques, and signature-based threat detection methods to secure distributed cloud infrastructures. These security solutions continuously monitor cloud resources, user activities, network traffic, and system logs to identify malicious behavior based on predefined security rules and known attack signatures. While these approaches provide effective protection against previously identified cyber threats, they often struggle to detect sophisticated and rapidly evolving attacks within modern cloud environments [10], [11].

To improve security monitoring, several organizations employ centralized log analysis and vulnerability assessment tools that collect information from virtual machines, cloud applications, network devices, and storage systems. Security administrators manually analyze these logs to identify suspicious activities, detect system vulnerabilities, and investigate potential security incidents. However, the exponential growth of cloud-generated security data makes manual analysis increasingly difficult, resulting in delayed threat detection and slower incident response [1], [12].

Recent research has introduced machine learning algorithms such as Decision Tree, Support Vector Machine (SVM), Random Forest, and K-Nearest Neighbors (KNN) for automated cloud vulnerability detection. These models analyze system logs, network traffic, authentication records, and cloud service activities to classify normal and malicious behavior. Although these intelligent approaches improve detection accuracy compared to conventional rule-based systems, many existing implementations rely on individual machine learning models that may not effectively capture the complex relationships among distributed cloud resources, virtualized environments, and dynamic network activities [4], [13].

Furthermore, most existing cloud security systems are designed to detect either known attack signatures through supervised learning or abnormal behavior using standalone anomaly detection models. Such isolated approaches often reduce the ability of security frameworks to identify both previously known attacks and emerging zero-day threats simultaneously. Consequently, achieving accurate, scalable, and adaptive vulnerability detection remains a significant challenge in securing modern cloud infrastructures against continuously evolving cyber threats [9], [13].

Disadvantages of the Existing System

- Limited Detection of Unknown Threats: Traditional rule-based and signature-based security systems are effective only against known attack patterns and generally fail to detect zero-day vulnerabilities or newly emerging cyber threats [10], [13].
- High False Positive Rate: Conventional intrusion detection mechanisms often generate excessive false alarms, making it difficult for security analysts to accurately identify genuine security incidents.
- Dependence on Manual Security Analysis: Existing monitoring systems require continuous manual examination of system logs and network activities, increasing operational complexity and delaying threat response in large-scale cloud environments [1], [12].
- Poor Scalability: As cloud infrastructures expand across multiple virtual machines, containers, and distributed services, conventional security mechanisms struggle to

efficiently process the growing volume of security-related data.

- Limited Adaptability: Static security policies and predefined detection rules cannot quickly adapt to evolving attack techniques, reducing the effectiveness of traditional cloud protection mechanisms against sophisticated cyber attacks [11].
- Inadequate Detection Accuracy: Standalone machine learning models may experience reduced prediction performance when analyzing high-dimensional cloud security datasets containing complex behavioral relationships [4], [13].
- Lack of Continuous Learning: Many existing cloud security frameworks do not continuously update their learning models using newly generated security data, limiting their ability to respond effectively to changing threat landscapes and dynamic cloud environments [9], [10].

2. Proposed System

The proposed system introduces an intelligent machine learning-based framework for proactive cloud vulnerability detection and threat prevention in distributed cloud environments. The framework integrates data preprocessing, feature engineering, supervised and unsupervised machine learning algorithms, anomaly detection, and continuous security monitoring to identify potential cyber threats with high accuracy. By leveraging intelligent data analysis techniques, the proposed framework enhances cloud security, minimizes false alarms, and provides rapid identification of vulnerabilities before they can compromise critical cloud resources [1], [11].

The framework begins by collecting security-related information from multiple cloud infrastructure components, including system logs, network traffic records, authentication events, cloud service activities, virtual machine logs, and vulnerability databases. These heterogeneous data sources provide comprehensive visibility into cloud operations and enable the framework to monitor both network-level and application-level security events across distributed computing environments. Aggregating security information from multiple sources significantly improves the capability of detecting sophisticated attack patterns and hidden vulnerabilities [10], [12].

Following data acquisition, the collected information undergoes a comprehensive preprocessing stage involving missing value handling, duplicate record removal, noise filtering, feature normalization, categorical encoding, and data transformation. Feature engineering techniques are subsequently applied to extract meaningful security attributes such as abnormal login attempts, unusual network traffic behavior, privilege escalation events, unauthorized API access, configuration changes, and suspicious system activities. These preprocessing and feature optimization processes improve data quality while reducing computational complexity and enhancing machine learning performance [4], [13].

The optimized dataset is then used to train multiple machine learning algorithms, including Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest. Supervised learning models classify known attack patterns using historical security data, while the Isolation Forest algorithm performs anomaly detection by identifying abnormal behaviors that may represent previously unknown cyber threats or zero-day vulnerabilities. The integration of supervised classification and unsupervised anomaly detection enables the framework to provide comprehensive protection against both known and emerging security attacks [9], [13].

To further improve prediction reliability, hyperparameter optimization and cross-validation techniques are incorporated during model training. These optimization methods enhance model generalization, reduce overfitting, and ensure consistent detection performance when analyzing unseen cloud security data. Comparative performance evaluation is conducted using accuracy, precision, recall, F1-score, confusion matrix analysis, and Receiver Operating Characteristic (ROC) curve analysis to identify the most effective machine learning model for cloud vulnerability detection [1], [10].

The proposed framework also incorporates a real-time security monitoring and intelligent alert generation mechanism that continuously analyzes incoming cloud security events. Whenever suspicious behavior or potential vulnerabilities are detected, the system immediately generates security alerts to support rapid incident response and mitigation. Furthermore, the framework supports continuous learning by periodically retraining machine learning models with newly generated security data, enabling adaptive protection against evolving cyber threats. This intelligent, scalable, and automated approach significantly strengthens the security, resilience, and reliability of distributed cloud infrastructures while supporting proactive cybersecurity management in modern cloud computing environments [4], [11], [13].

IV. SYSTEM DESIGN

1. System Architecture

Below diagram depicts the whole system architecture.

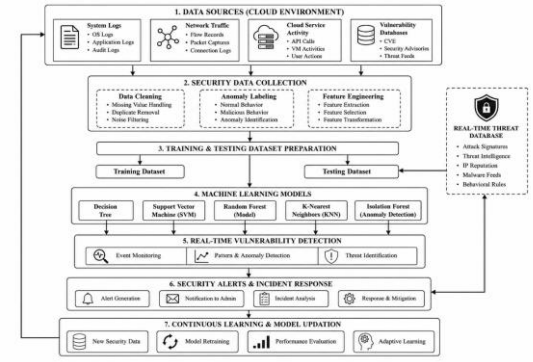

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

1. Modules

Security Data Acquisition and Preprocessing Module

The first module is responsible for collecting security-related information from various components of the cloud infrastructure. Data is acquired from system logs, network traffic records, cloud service activities, authentication logs, virtual machine events, and vulnerability databases. Before model development, the collected data undergoes preprocessing operations including missing value handling, duplicate removal, noise filtering, normalization, and categorical feature encoding. These preprocessing techniques improve data consistency, eliminate redundant information, and prepare the dataset for effective machine learning analysis. High-quality preprocessing significantly enhances the reliability and accuracy of cloud vulnerability detection models [1], [12].

Feature Engineering and Security Analytics Module

After preprocessing, the framework extracts meaningful security features that accurately represent cloud system behavior. Important attributes such as abnormal login attempts, API request frequency, network communication patterns, privilege escalation events, resource utilization, and suspicious configuration changes are identified and analyzed. Feature selection techniques are applied to eliminate irrelevant variables while preserving the most informative security indicators. This process reduces computational complexity, improves model interpretability, and enhances the capability of detecting sophisticated cyber threats within distributed cloud environments [4], [10].

Machine Learning Model Development Module

The optimized dataset is utilized to train multiple machine learning algorithms capable of identifying vulnerabilities and malicious activities within cloud infrastructures. The implemented models include Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest. Supervised learning algorithms classify known attack patterns using historical security data, while the Isolation Forest algorithm detects anomalous behavior associated with previously unknown threats. Hyperparameter tuning and cross-validation techniques are employed to optimize model performance, improve generalization capability, and minimize overfitting [9], [13].

Intelligent Threat Detection and Alert Generation Module

Once the models are trained, they are integrated into the cloud security framework for continuous monitoring of incoming security events. The system analyzes real-time cloud activities, including network traffic, authentication requests, service logs, and virtual machine operations, to identify suspicious behavior and potential vulnerabilities. Whenever malicious activity or abnormal system behavior is detected, the framework immediately generates security alerts and notifies administrators for rapid investigation and mitigation. This intelligent detection mechanism enables proactive defense against both known cyber attacks and emerging security threats [10], [11].

Performance Evaluation and Continuous Learning Module

The final module evaluates the effectiveness of the proposed framework using standard performance metrics such as accuracy, precision, recall, F1-score, confusion matrix analysis, and Receiver Operating Characteristic (ROC) curve analysis. Comparative evaluation identifies the most effective machine learning model for cloud vulnerability detection. The framework also supports continuous learning by periodically retraining models with newly generated security data collected from cloud environments. This adaptive learning capability enables the system to respond to evolving attack techniques, maintain high detection accuracy, and improve long-term security performance in dynamic cloud infrastructures [1], [9], [13].

VI. RESULTS AND DISCUSSION

This section presents the experimental evaluation of the proposed machine learning-based cloud vulnerability detection framework. The experiments were conducted using a cloud security dataset consisting of system logs, network traffic records, authentication events, cloud service activities, and vulnerability reports collected from distributed cloud environments. Prior to model development, the dataset underwent preprocessing through data cleaning, normalization, feature engineering, and anomaly labeling to improve data quality and model performance. Multiple machine learning

algorithms were trained and evaluated to determine their effectiveness in detecting cloud vulnerabilities and identifying malicious activities. The performance of each model was assessed using standard evaluation metrics, including accuracy, precision, recall, F1-score, confusion matrix analysis, and Receiver Operating Characteristic (ROC) analysis [1], [10].

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

Several machine learning algorithms were implemented to classify normal cloud activities and potential security threats. The evaluated models include Decision Tree, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbors (KNN), and Isolation Forest. Each classifier was trained using security-related attributes extracted from cloud infrastructure data, including system logs, network traffic behavior, authentication records, service activities, and vulnerability information.

The classification performance of each model was evaluated using commonly accepted performance metrics.

Table 1. Performance Comparison of Machine Learning Models for Cloud Vulnerability 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

The experimental results demonstrate that the Random Forest classifier achieved the highest prediction accuracy of 93.4%, outperforming all other machine learning models. Its ensemble learning strategy effectively combines multiple decision trees to capture complex security patterns, resulting in improved detection accuracy, reduced false alarms, and enhanced generalization capability. These findings indicate that Random Forest provides a reliable solution for identifying cloud vulnerabilities and cyber threats in distributed cloud environments [1], [10], [13].

2. ROC Curve Analysis

Receiver Operating Characteristic (ROC) analysis was performed to evaluate the capability of the implemented models to distinguish normal cloud operations from malicious activities. The ROC curve illustrates the relationship between the True Positive Rate (TPR) and the False Positive Rate (FPR) across different classification thresholds.

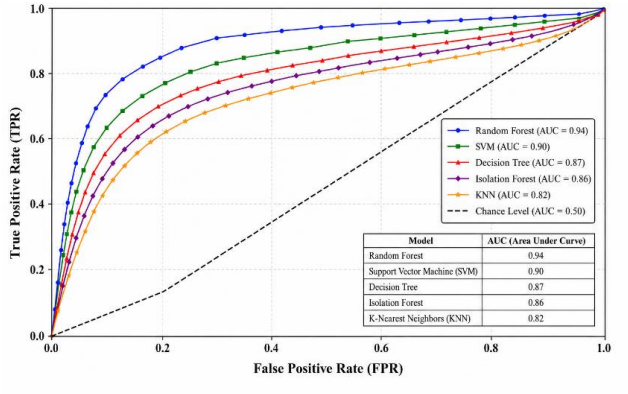

Fig. 2. ROC Curve for Machine Learning-Based Cloud Security Detection

The Random Forest model achieved an Area Under the Curve (AUC) value of approximately 0.94, indicating excellent classification performance and strong discrimination capability. The high ROC-AUC score demonstrates that the proposed framework accurately identifies cloud security threats while maintaining a low false positive rate. This confirms the effectiveness of the proposed machine learning framework for real-time cloud security monitoring and intelligent threat detection [10], [12].

VII. CONCLUSION AND FUTURE WORK

This paper presented an intelligent machine learning-based framework for cloud vulnerability detection and threat prevention in distributed cloud environments. The proposed framework integrates security data collection, comprehensive preprocessing, feature engineering, supervised and unsupervised machine learning techniques, and real-time threat monitoring to strengthen cloud security. By analyzing system logs, network traffic records, authentication events, cloud service activities, and vulnerability information, the framework accurately identifies malicious behavior and potential security risks while improving the efficiency of cloud security management [1], [11].

Experimental evaluation demonstrated that machine learning algorithms significantly enhance the detection of cloud vulnerabilities compared with conventional rule-based security mechanisms. Among the evaluated classifiers, the Random Forest model achieved the highest performance in terms of

accuracy, precision, recall, and F1-score, demonstrating superior capability in identifying both known attack patterns and abnormal system behavior. The integration of anomaly detection techniques further improved the framework's ability to recognize previously unseen cyber threats while maintaining a low false positive rate. These results confirm that intelligent machine learning approaches provide a reliable and scalable solution for protecting modern cloud infrastructures against continuously evolving cybersecurity threats [4], [10], [13].

The proposed framework offers an adaptive security solution capable of supporting proactive vulnerability assessment, automated threat detection, and rapid incident response within dynamic cloud environments. By reducing manual security analysis and enabling continuous monitoring, the framework improves operational efficiency, strengthens cloud resilience, and assists organizations in safeguarding critical digital assets and cloud-based services [1], [12].

Future research can focus on integrating advanced deep learning architectures such as Long Short-Term Memory (LSTM) networks, Graph Neural Networks (GNNs), Transformer-based security models, and federated learning techniques to further improve vulnerability prediction and threat detection accuracy. The incorporation of Explainable Artificial Intelligence (XAI) can enhance the transparency and interpretability of security decisions, enabling administrators to better understand model predictions. Additionally, integrating blockchain-based security mechanisms, edge computing, and Security Information and Event Management (SIEM) platforms can strengthen secure data sharing, real-time incident response, and distributed threat intelligence. Evaluating the proposed framework using large-scale multi-cloud environments and real-world enterprise security datasets will further validate its effectiveness and support the development of intelligent, scalable, and resilient cloud security systems capable of defending against next-generation cyber threats [9], [10], [13], [18].

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.

AUTHOR DETAIL

Miss. Pemmanaboyina Durga Devi is currently pursuing M.Tech in Computer Science and Engineering at Lenora College of Engineering, Rampachodavaram, Alluri Sitarama Raju District, Andhra Pradesh, India. She possesses a strong academic foundation in Machine Learning, Cloud Computing, Cybersecurity, Java Programming, Web Technologies, and Database Management Systems. Her practical experience includes developing intelligent security systems for cloud environments involving data preprocessing, feature engineering, model training, vulnerability analysis, and threat prediction using machine learning techniques. Her work focuses on implementing robust predictive models for real-time cloud vulnerability detection and automated threat mitigation to enhance the security and reliability of cloud infrastructures. She is also experienced in software system design using Unified Modelling Language (UML), including use case, class, sequence, activity, and data flow diagrams. Her research interests include Machine Learning, Cloud Security, Cybersecurity, Data Processing Pipelines, Predictive Analytics, and Intelligent Threat Detection Systems. She is committed to advancing academic research and developing innovative AI-driven solutions for secure cloud computing and intelligent cyber defence systems.

Miss. SAVARAPU SUHASINI is the Head of the Department of Computer Science and Engineering at Lenora College of Engineering, Rampachodavaram, Alluri Sitarama Raju District, Andhra Pradesh, India. She possesses extensive academic and research expertise in Machine Learning, Artificial Intelligence, Natural Language Processing (NLP), Data Science, Computer Vision, Web Technologies, and Database Management Systems. She has guided numerous postgraduate research projects in emerging domains of intelligent computing, with a strong emphasis on the design, development, and evaluation of AI-driven solutions for real-world applications. Her research interests encompass Machine Learning, Deep Learning, Natural Language Processing, Explainable Artificial Intelligence (XAI), Intelligent Data Analytics, Computer Vision, and Predictive Modelling. She has significant experience in software engineering methodologies, system

analysis, and Unified Modelling Language (UML)-based software design, including use case, class, sequence, activity, and data flow diagrams. As an academic mentor and researcher, she is committed to promoting excellence in teaching, fostering innovative research, and developing intelligent computational frameworks that address contemporary challenges in artificial intelligence and data-driven technologies.