Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

Risk Recognition in Cloud Computing using Different Types of Machine Learning Technologies : A Review

Jayati Mitra
Dept. of Computer science and Technology
The Institute of Leadership, Entrepreneurship, and Development (iLEAD)
Kolkata, India

Riya Biswas
Dept. of Computer science and Technology
The Institute of Leadership, Entrepreneurship, and Development (iLEAD)
Kolkata, India

***Abstract*- Cloud computing has transformed the IT sector by delivering adaptable and scalable solutions for managing data storage and computational tasks. Nevertheless, the widespread adoption of cloud technologies has brought about notable security and operational concerns, including unauthorized intrusions, information leaks, and system slowdowns. Machine learning (ML) has surfaced as an effective means to confront these issues, offering capabilities such as forecasting, abnormal behavior identification, and intelligent threat management. This review explores recent developments in leveraging ML for risk identification in cloud environments. It classifies ML methods, assesses their suitability for various cloud-related threats, and discusses major obstacles and potential avenues for future research.**

***Keywords*— Cloud computing, Machine Learning, IDS, SVM, Introduction**

I. INTRODUCTION

Cloud computing enables on-demand access to a shared pool of customizable computing resources, fostering innovation and lowering IT expenditures. Despite its benefits, the transition to cloud-based systems has brought about numerous challenges, including information leakage, cyber threats, and service outages. Traditional risk management techniques often fall short due to the vast scale, intricate architecture, and dynamic nature of cloud platforms. Machine learning presents a powerful alternative by utilizing data-centric methods to detect and respond to risks in real time. We analyze current methodologies, evaluate their advantages and drawbacks, and explore evolving trends within this area of research.

II. LITERATURE REVIEW

Qazi Omair Ahmed et al [1] With the rapid expansion of cloud computing, concerns regarding security have become increasingly prominent. This paper presents a comparative analysis of various machine learning (ML) techniques employed for intrusion detection within cloud computing environments. It explores and evaluates multiple ML algorithms—including decision trees, support vector machines, k-nearest neighbors, and neural networks—based on their effectiveness in identifying and mitigating a range of cyber-attacks.

Rajashekhargouda C. Patil et .al., [2] This research proposes a novel methodology for identifying data leakage within cloud computing environments by utilizing data classification powered by deep learning frameworks. The input, acquired in the form of network traffic, is subjected to a series of preprocessing techniques, including noise reduction and signal smoothing. Subsequently, classification is executed using a Generative Regression Kernel-based Support Vector Machine (SVM), enhancing the precision of anomaly detection.

Amira Abdallah , Aysha Alkaabi et al., [3] This research endeavors to address existing gaps in anomaly detection across cloud network environments, presenting viable solutions for precisely identifying irregularities. The central objective is to deliver valuable insights and practical methodologies aimed at enhancing the security and reliability of cloud infrastructures through the application of machine learning (ML) and deep learning (DL) techniques. The study outlines specific ML/DL methodologies, emphasizing their respective advantages, constraints, and implementation strategies. Additionally, it offers a comparative evaluation of various ML and DL models in the context of anomaly detection.

R. Gupta , Deepika Saxena, Ashutosh Kumar Singh et. al., [4] this paper presents a comprehensive discussion on the cloud computing environment, highlighting its advantages, inherent challenges, and emerging research trends centered on the secure processing and sharing of data.

Ayesha Sarosh et.al [5] This paper proposes a machine learning (ML)-based hybrid intrusion detection system specifically designed for virtualized environments within cloud computing. The system employs a composite algorithm that integrates Support Vector Machine (SVM) with K-means clustering to improve the precision of anomaly revealing. For performance evaluation, the UNSW-NB15 dataset is utilized, and the results are benchmarked against existing methodologies. Key performance indicators, such as average detection time, are analyzed to assess the system's efficiency, with conclusion indicating that the proposed approach outperforms earlier techniques in terms of detection accurateness.

Prisca I. Okochi et al. [6] This research aims to detect and mitigate both intentional and unintended data breaches by incorporating dynamic password or key-based mechanisms within data decryption security frameworks. The Object-Oriented Analysis and Design Methodology (OOADM) was utilized to guide the system's expansion process. The system was implemented using ASP.NET MVC, with Microsoft SQL Server Management Studio serving as the backend. An integrated Audit Trail and Transaction Log feature enables comprehensive tracking of user and system activities, recording each action with corresponding date and time stamps. As a result, the system demonstrates strong flexibility across various computing environments, offering a dependable solution for both the prevention and detection of data leakage.

Gupta, I., Mittal, S., et .al., [7] This paper utilizes a semantic-based approach to classify data through the execution of a statistical Data Leakage Prevention (DLP) model. Statistical analysis techniques are employed to detect sensitive information and strengthen security measures within data leakage-prone environments. The Term Frequency-Inverse Document Frequency (TF-IDF) algorithm is leveraged as the core information retrieval mechanism, enabling the categorization of documents based on thematic relevance. Experimental results express that the projected statistical DLP framework is capable of accurately classifying documents, even in scenarios involving substantial modifications or content rearrangement.

Xiquan Wang, Zhen Pan, et. al., [8] this paper introduces a data anomaly detection and response framework. Utilizing the LOF (Local Outlier Factor) anomaly detection algorithm, the framework incorporates traceability mechanisms and adaptive theory to enhance its performance, resulting in the progress of the adaptive DR-LOF algorithm (Dimensional Reasoning Local Outlier Factor) for real-time, dynamic anomaly detection. moreover, the Analytic Hierarchy Process (AHP) algorithm is employed to raise an anomaly response hierarchy model, ensuring the stability and integrity of the cloud computing platform. The uncovering rate of the LOF algorithm increased from 10% to 70% after the improvements, while the false alarm rate decreased from 40% to 20%. Simulation results reveal that the %inset/s dimension index exhibits the lowest LOF value during virtual machine migration without abnormal attacks, while the rcpck/s dimension index shows the lowest LOF value when abnormal attacks are present. Furthermore , the change in K value has nominal impact on the anomaly detection presentation of the adaptive DR-LOF algorithm. These findings hold significant value and potential in the field of detecting and responding to cloud computing security incidents.

Gavini Sreelatha, et. a,.l [9] This survey presents a comprehensive analysis of security challenges in cloud computing, exploring both conventional security approaches and advanced machine learning (ML)-based solutions. It begins by methodically identifying key vulnerabilities inborn in cloud infrastructures and proceeds to highlight state-of-the-art techniques for mitigating threats, addressing system weaknesses, and countering malicious attacks. Furthermore, the survey evaluates a range of security mechanisms developed using machine learning and deep learning (DL) methodologies, purposely tailored to enhance the resilience and integrity of cloud environments.

Ashish Singh, Kakali Chatterjee et. al.,[10] This paper investigates the core aspects of cloud computing, with a particular emphasis on security concerns, potential threats, and their corresponding lessening strategies. It provides a inclusive overview of essential topics, including the cloud architecture framework, service and deployment models, primary cloud technologies, and key cloud security principles. Various types of security threats and attack vectors are discussed in detail. Moreover, the paper highlights several open research challenges that continue in the area of cloud security, emphasizing the need for continued innovation and investigation in this critical area.

III. OBJECTIVE

The rapid advancement of cloud computing has transformed how businesses and individuals manage data, applications, and infrastructure. While the cloud offers unmatched scalability, flexibility, and cost-efficiency, it also introduces a broad range of reliability concerns and security threats. These challenges arise from the multi-tenant nature of cloud environments, the complex interdependencies among services, and the constantly evolving tactics of malicious actors. Risks such as data breaches, denial-of-service attacks, and unauthorized access can significantly compromise the confidentiality, integrity, and availability of critical information—posing serious threats to both cloud providers and their clients.

The specific objectives of this paper are as follows:

i. To Review Machine Learning Techniques for Risk Detection: This paper aims to explore various machine learning techniques, including supervised, unsupervised, and reinforcement learning, and their applications in detecting security risks and anomalies in cloud environments.

ii. To Categorize and Analyze Risk Detection Methods: The paper will categorize distinct risk observation methods based on the category of risk they address (e.g., data breaches, denial of service, unauthorized access, etc.) and evaluate their effectiveness in different cloud environments (private, public, and hybrid clouds).

iii. To Identify Challenges in Risk Detection: A crucial objective is to highlight the challenges associated with applying machine learning techniques to risk detection in cloud computing, such as data privacy concerns, scalability issues, and the progress nature of cyber threats.

iv. To Discuss the Integration of ML Models with Existing Security Frameworks: The paper will inspect how machine learning models can be united with traditional security approaches like firewalls, intrusion spotting systems, and encryption to create a more robust security ecosystem in the cloud.

IV. EXISTING METHODS OF MACHINE LEARNING IN RISK DETECTION

A. INTRUSION DETECTION SYSTEMS (IDS)

Cloud computing environments face increasing threats due to their dynamic, distributed, and multi-tenant nature. To effectively identify and mitigate these risks, automated systems leveraging machine learning (ML) have become essential. A risk detection system in cloud computing typically involves a structured methodology that includes data collection, preprocessing, feature selection, model training, risk detection, and response.

This methodology allows for the real-time identification of threats such as data breaches, unauthorized access, or denial-of-service attacks, and enables proactive mitigation strategies. The integration of ML enhances the system's ability to adapt to new attack patterns and evolving risks, reducing false positives and improving overall security.

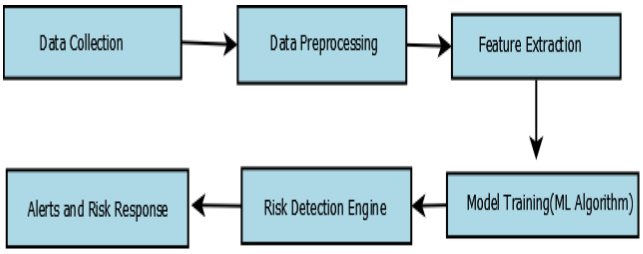

Fig 1: Work flow of Instruction Detection System

B. DECISION TREE-BASED RISK PREDICTION (DTRP)

Decision Tree algorithms are a powerful machine learning method used for categorization and prediction tasks. In the context of cloud computing, the DTRP methodology helps predict potential risks such as unauthorized access, service failures, or malicious activity by analyzing historical and real-time data.

This approach uses a tree-like structure where decisions are made based on feature conditions (e.g., IP behavior, access frequency, request anomalies). The outcome is a prediction of whether an activity is regular or dicey.

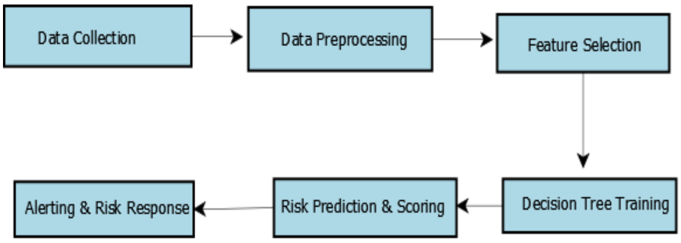

Fig 2: Work flow of Decision Tree Based Risk Detection

C. FRAUD DETECTION BY SUPPORT VECTOR MACHINE

Support Vector Machine (SVM) is a powerful supervised machine learning algorithm used for classification tasks, especially effective in high-dimensional and imbalanced datasets—common in fraud detection. The core idea is to find an optimal hyperplane that best separates the classes (fraudulent vs. legitimate transactions) with maximum margin.

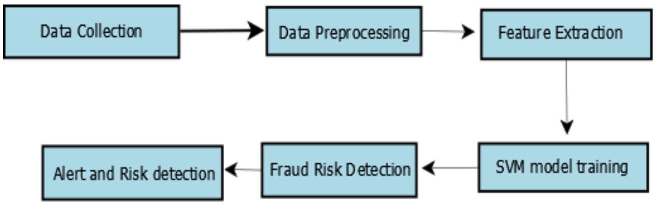

Fig3: Work diagram of SVM

V. CONCLUSION

Machine learning has demonstrated significant potential in enhancing risk detection in cloud computing. By automating the analysis of complex data and enabling Real-time decision-making, ML techniques are transforming the way risks are managed in cloud environments. However, challenges related to scalability, interprettability, and integration persist. Future research should focus on addressing these challenges while exploring emerging paradigms like federated learning and edge computing.

REFERENCES

1. Qazi Omair AhmedMachine.(2024). Learning for Intrusion Detection in Cloud Environments: A Comparative Study. ISSN: 3006- 4023, DOI: 10.60087.
2. Rajashekhargouda C. Patil, A. K. Data, Narmadha T, M. Suganthi, Akula VS Siva Rama Rao, Rajesh A.(2022). Leakage Detection in Cloud Computing Environment Using Classification Based on Deep Learning Architectures. VOl. 10 No.2s(2022).
3. Amira Abdallah , Aysha Alkaabi , Ghaya Alameri , Saida Hafsa Rafique , Nura Shifa Musa ,and Thangavel Murugan.(2024). Cloud Network
Anomaly Detection Using Machine and Deep Learning Techniques - Recent Research Advancements. IEEE Access PP(99):1-1 DOI:10.1109/ACCESS.2024.3390844
4. R. Gupta , Deepika Saxena, Ashutosh Kumar Singh(2021),DATA SECURITY & PRIVACY IN CLOUD COMPUTING: CONCEPTS AND EMERGING TRENDS 29(3), 89-101.
5. Ayesha Sarosh,(2021) Machine Learning Based Hybrid Intrusion Detection For Virtua Lized Infrastructures in Cloud Computing. 2089(2021)012072, doi:10.1088/1742-6596/2089/1/012072.
6. Prisca I. Okochi , Stanley A. Okolie and Juliet N. Odii,(2021). An improved data leakage detection system in a cloud computing Environment.11(02),321–328, https://doi.org/10.30574/wjarr.2021.11.2.0385.
7. Gupta, I., Mittal, S., Tiwari, A., Agarwal, P., & Singh, A. K. (2022). TIDF-DLPM: Term and Inverse Document Frequency based Data Leakage Prevention Model. arXiv preprint arXiv:2203.05367.
8. Xiquan Wang, Zhen Pan, uan Zhang & Jiao Huang(2021), Detection and elimination of project engineering security risks from the perspective of cloud computing.
9. Gavini Sreelatha, A. Vinaya Babu, Divya Midhunchakkarvarthy (2020), A Survey on Cloud Attack Detection using Machine Learning Techniques.International Journal of Computer Applications (0975 – 8887) ,Volume 175 – No. 34.
10. Ashish Singh, Kakali Chatterjee (2016), Cloud security issues and challenges: A survey.DOI:10.1016/j.jnca.2016.11.027.