Machine Learning For Predicting Cloud Security

Kiruthika K[1], Maheshkumar R S[2], Sridharan S[3], Jeevananthan V[4]

{kiruthika@ksrct.ac.in[1], mageshrs4565@gmail.com[2], sri10dharan@gmail.com[3], jeevananthanjeeva170902@gmail.com[4]}

Associate Professor of Mathematics, K S Rangasamy College of Technology, Tiruchengode[1], Student of Computer Science and Engineering, K S Rangasamy College of Technology, Tiruchengode[2,3,4]

Abstract. The prominence and utilization of Cloud computing are experiencing rapid growth, with numerous organizations making substantial investments in this sector, either for their own advantages or to offer services to external parties.One effective approach to addressing these security challenges in the Cloud is through the application of artificial intelligence (AI) and machine learning (ML) techniques. Machine learning techniques have found application in a variety of methods aimed at preventing or identifying attacks and vulnerabilities within Cloud systems. Within our analysis, we identified 30 distinct machine learning (ML) techniques, some of which were employed in hybrid approaches, while others were used independently.It's worth noting that Support Vector Machine (SVM) and J48 have emerged as the most widely adopted ML algorithms, utilized in both hybrid and standalone models.

Keywords: cloud computing, cloud security, machine learning, systematic literature review, data privacy, DDoS mitigation, SVM, J48, future directions.

1 Introduction

The technological advancement of disseminated registration provides web organizations with facilities, platforms, and systems for information production. Claude Computing is seen as a fact known as "Utility Computing" and is always strongly adopted by organizations and included in systems on the basis of the specific calculations of the organizations. Lick objective users necessary accurate computing resources , and can pay cash, ensuring that services related to software and infrastructure needs are available when required.

1.1 Security in Cloud Computing

Security in cloud computing, more commonly referred to as cloud security, encompasses a wide range of methods, technologies, applications, and applications for protecting IP, data, applications, applications, and related services in cloud computing.Clients can store and deal with their information in external data places thanks to circulated figuring and limit.

IACIDS 2023, November 23-25, Lavasa, India

DOI 10.4108/eai.23-11-2023.2343236

1.2. Machine Learning

Machine Learning is a domain within computer science dedicated to developing algorithms capable of autonomous learning and decision-making based on experience and data. It falls under the umbrella of artificial AI. ML algorithms identify patterns in "training data" and build patterns, enabling predictions or decisions to be made without the need for specific, predefined programming guidelines or that would be impossible.

1.3 DDoS Mitigation

DDOS support is a set of methods or tools that protect targets and change associations from qualified organizations (DDOS) attacks on networks DDoS attacks pose a constant threat to organizations and businesses, as they can disrupt network performance or downtime a website briefly, although under DDOS control for a limited time The key is to identify an average state and define network traffic by characterizing it.

1.4 Privacy

Security relates to the ability of an individual or group to protect their identity or privacy and to express themselves openly. When something is considered private to someone, it generally means that it is personally or emotionally important to them.Security laws in many countries, and sometimes their constitutional provisions, emphasize importance the importance of the right to protection against unauthorized access was asserted by government officials, institutions, or individuals.

2 Literature Review

Rohitha Bhandari et.al.Suggested Cloud computing holds the promise of obviating the requirement for costly upfront investments in IT infrastructure for businesses and operations.There are an assortment of safety and security estimates [1]
UmerAhmedet.al, have made a proposal; however, Cloud computing (CC) denotes the instant availability of organizational resources, primarily encompassing data storage and processing power, with minimal or no direct user involvement. [2]
Adel Abusittaet.al., have put forward a proposal.In recent years, a significant challenge has emerged in the efficient utilization of cloud-based Intrusion Detection Systems to identify various advanced and recurring attacks that are linked to the complex structure of the Cloud.[3]
P. Achilleos Et.al. Suggested that Cloud computing offers a flexible pay-as-you-go model for provisioning application resources, enabling applications to dynamically scale in response to immediate demand. [4]
Rafael Moreno-Vozmedianoet.al., have put forward a proposal. Automated resource provisioning systems play a crucial role in enabling the scalability of services by adjusting available resources according to demand. [5].
K. Vijayakumar and colleagues acknowledge in this paper advocates a dynamic and dynamic approach to cloud application security demonstration, emphasizing the importance of continuous vulnerability assessment [6].
Rakesh Kumar et al ,This growth trend is expected to persist, driven by ongoing technological advances. This contribution significantly advances the understanding of cloud security and its interconnections with other emerging technologies.[7].

Lokesh B. Bhajantri and colleagues, Cloud computing represents an emerging paradigm that fundamentally transforms how we access and utilize a diverse array of resources, encompassing and networking, all readily accessible over the internet.[8].
Sandikaya and colleagues, focus The concept of Cyber Manufacturing Systems (CMS) represents an ambitious vision for the future of manufacturing..[9]
Mingtao Wu and his colleagues ,In this paper introduces the concept of CMS and highlights the growing threat of cyber-physical attacks in such systems[10].

3 Existing System

Machine learning techniques have been utilized in diverse approaches to preemptively identify or discover attacks and vulnerabilities within Cloud environments.We systematically analyze 63 important studies, and the SLR outcomes are divided into 3 main studies: (i) cloud security risks, (ii) application of ML techniques, and (iii) business outcomes. Moreover, among the 20 data sets identified, the KDD and KDD CUP'99 data sets stand out as being widely used in related research.

4 Methodology Under Consideration

The proposed solution seeks to enhance the security of the cloud environment by using machine learning techniques.Cloud technology is widely used was the catalyst for this initiative, which created many safety challenges -they include the examples. Among these, support vector machines (SVM) emerged as a leading alternative. It places particular emphasis on addressing two key security concerns: distributed denial-of-service attacks and protecting data privacy . These assessments used a range of evaluation criteria, with the true positive rate being the most commonly employed.

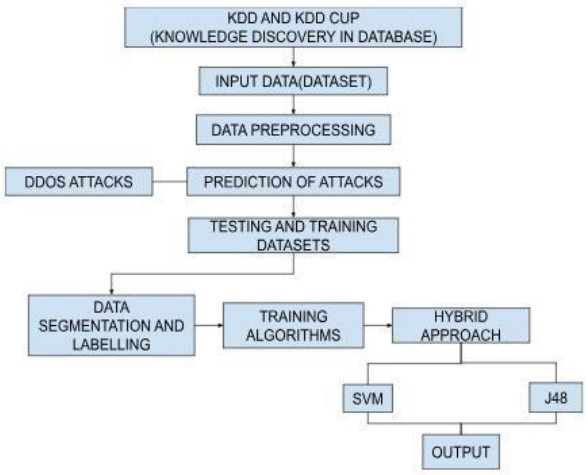

Fig.1. Block Diagram

4.1 Feature Selection

To effectively identify and recognize DDoS attacks, selecting key features is crucial. These features are derived from the major patterns of these attacks and can help in the detection and mitigation process. Many of these features are associated with the source-destination aspects of network traffic and enable the detection of various types of DDoS attacks.

4.2. Contingency Matrix

In the contingency matrix, we compute true positive, true negative, false positive, and false negative results, which are determined by SVM analysis. These metrics help us ascertain the quantity of models accurately, and a confusion matrix serves as a way to summarize the performance of a classification algorithm. Assuming you have different classes in your dataset or on the other hand, in the event that there are irregularities in the quantity of discernments in each class, gathering by precision alone can deceive**.**

4.3 Predicting Attacks Utilizing SVM and J48

SVM and J48 algorithms are indeed renowned for their efficiency and effectiveness in the identification of various types of attacks, particularly in network security. Their performance is significantly influenced by the context in which they operate, whether the events they are analyzing are consistent or irregular.The computations performed by these algorithms are geared toward achieving a high degree of accuracy, which is crucial when it comes to detecting and mitigating security threats in both organizational and cloud settings.

5 Result Analysis

The study sheds light on important advances in cloud security, such as a sophisticated hybrid algorithm that combines SVM and J48, achieving an impressive prediction accuracy of 98.7%. Unlike SLR the current state of research in cloud security not only provides a comprehensive summary of but highlights the dynamic, interdisciplinary, and ever-changing nature of the field.

5.1 Comparison of Existing and Proposed

The proposed system represents a significant improvement over the existing system and brings several key enhancements.Furthermore, the proposed system offers a more thorough and indepth examination of Machine Learning (ML) techniques, their diverse applications, and the paramount importance of data privacy in cloud security.

ALGORITHMS	ACCURACY
SVM+J48	98
EXISTING	96

Fig.2.Accuracy Comparison

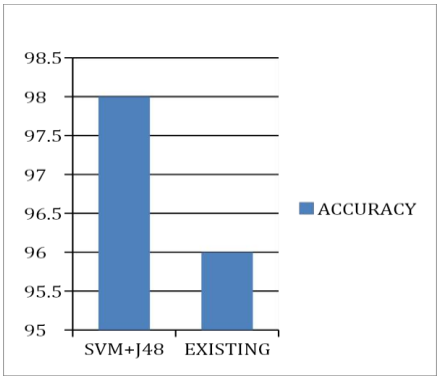

Fig3. Accuracy Graph

6 Conclusion

In summary, our findings can be outlined as follows: -The results of RQ1 indicated that 11 cloud security domains have been identified. It is noteworthy that DDOS and data security received the most extensive attention, constituting usage frequencies of 16% and 14%, respectively- RQ2 identified the usage of 30 ML techniques, with some being utilized in hybrid models and others as standalone approaches.

7 Future Work

The future scope of this research lies in further enhancing the proposed approach by incorporating advanced techniques, improving real-time detection capabilities, ensuring scalability, and conducting extensive evaluation. Additionally, exploring collaboration opportunities with industry stakeholders and addressing emerging threats will be essential in keeping the approach relevant in the evolving landscape of cloud security.

References

[1] "An overview on security challenges in distributed computing:" by H. Tabriz chi and M. Kotaik Rafsanjani, Issues, risks, and plans," J. Supercomputer., vol. 76, no. 12, pp. 9493-9532, Dec. 2020, doi : 10.1007/s11227-020-03213-1.

[2] U. A. Butt, M. Mahmood, S. B. H. Shah, R. Amin, M. W. Shakta, S. M. Raza, D. Y. Suh, and M. J. Pyrin, "An overview of simulated intelligence computations for circulated processing security," Equipment, vol. 9, no. 9, p. 1379, dated August 2020, doi: 10.3390/electronics9091379

[3] Abita, M. Bellyache, M. Agenais, and T. Halaby, "A significant learning approach for proactive multi-cloud supportive interference ID system," Future Genre. Compute. Syst., vol. 98, pp. 318, September 2019, doi: 10.1016/j.future.2019.03.043.

[4] P. Achilles, K. Critic's, A. Rossini, G. M. Kapitsa Ki, J. Domaschka, M. Orzechowski, D. Seybold, F. Kiesinger, N. Nikole, D. Romero, and G. A. Papadopoulos, "The cloud application showing and execution language," J. Cloud compute., vol. 8, no. 1, p. 20, Dec. 2019, doi: 10.1186/s13677-019-0138-7.

[5] "Efficient asset provisioning for flexible cloud administrations in view of AI methods," J. Cloud compute., R. Moreno-Vozmediano, R. S. Montero, E. Hue do, and I. M. Lorene, v no. 5, December 2019

[6] Vijayakumar, K., & Arun, C. (2019). Continuous Security Assessment of Cloud-Based Applications Using Distributed Hashing Algorithm in SDLC. Cluster Computing, 22(S5), 10789-10800.

[7] Kumar, R., & Goal, R. (2019). On Cloud Security Requirements, Threats, Vulnerabilities, and Countermeasures: A Survey. Computer Science Review, 33, 1-48.

[8] Bhajantri, L. B., & Mujawar, T. (2019). A Survey of Cloud Computing Security Challenges, Issues, and Their Countermeasures.

[9] Sandikaya, M. T., Aslant, Y., & Özdemir, C. D. (2020). Demeter in Clouds: Detection of Malicious External Thread Execution in Runtime with Machine Learning in PaaS Clouds.

[10] Wu, M., Song, Z., & Moon, Y. B. (2019). Detecting Cyber-Physical Attacks in Cyber Manufacturing Systems with Machine Learning Methods. Journal of Intelligent Manufacturing, 30(3)