Grenze International Journal of Engineering and Technology, June Issue

Intelligent Security Management in Cloud Computing using Machine Learning

Anand Vardhan Pandey[1], Radhika Garg[2], Ankit Kumar Maurya[3], Aman Raj[4], Arun Kumar Singh[5] and Arjun Singh[6]
[1-6]Greater Noida Institute of Technology, CSE, Greater Noida India
Email: Anandvardhanpandeyy@gamil.com, Amanraj97087@gmail.com, Radhikagarg604@gmail.com, Ankitji6565@gmail.com, arun.k.singh.iiit@gmail.com, innovativearjunsingh@gmail.com

***Abstract*— With the increase in the usage of cloud computing rapidly, it is the necessity to save the data from any target or attack. The emergence of the cloud computing raised Security issues for both industry and the consumer. Some of the companies are investing in this domain for their personal use and some for providing service in the same domain. Machine learning techniques is used in many ways to prevent and detect attacks on cloud server. As the growth of machine learning techniques learning based method for the software application is gaining high popularity in this era. In this paper, we provide a literature review on the use of machine learning in increasing cloud security and the application along with the ways to prevent the security of cloud computing. We will also evaluate the related studies and discuss their performance. This review and the key findings of this paper have the ability to contribute to more improvements in cloud computing and security issues with the machine-learning algorithm. It will help other researcher to give new ideas in this field so that new ideas can be executed which will help in finding the safe methods to access cloud computing based applications and avoid any security issue in the future.**

***Index Terms*— Cloud Computing, DDos Attack, Cyber Security, Machine Learning, Threats, Privacy, SVM.**

I. INTRODUCTION

Earlier, IT Companies used to follow traditional computing methods When comparing with the traditional IT security, cloud computing was responsible for multiple security issues. The security Issues starting from the cloud computing platform are: Firstly, the openness and distributed nature of the cloud expose it to the broader attack surface which significantly increase the risk of unauthorized access and data breaches [1,2]. Secondly the virtualization layer introduces more complexities in hiding and preventing individual Workload leading to compromise of multiple tenant environments. Finally, the decoupling of data ownership and management rights poses challenges in ensuring the traceability and accountability in the security incident leading to the challenges faced by cloud computing [3] The coexistence of multiple tenants on the cloud computing platform poses another significant challenge: ensuring the secure isolation of information resources across these tenants [4].
Cloud computing, as a novel service model, removing the connection of the ownership, management, and empowerment of resources. This decoupling means that users cede direct control over physical resources, exposing them to security vulnerabilities in their interactions with service providers [5,6].

Grenze ID: 01.GIJET.12.2.219_20

Even though the ways were safe still there was issue of the backups, capacity and cost [7]. In Recent Days, most of the communication between people is done through the internet. The internet is used in many of the fields in the world including medical, electronics, military, education, etc. Without it, the world would be not able to stay upright in the market. This is the reason that cloud computing recently become very famous due to the increasing demand to provide more efficient and secured ways of communication which will help the public to use these without worrying about security and storing big data in the network. Because of the increased computational cost, there is an increasing financial costs to the company which is caused due to storage and the analysis which is performed on data to analysis suspicious activity this is the main thing required to be there to make the relevant changes on the cloud computing to data [8].Cloud computing is a distributed computing platform that delivers a variety of services to the end-user over the internet. These services can be of three types (1) Software as a Service (SaaS), (2) Platform as a Service (PaaS), and (3) Infrastructure as a Service (IaaS).
Its main objective is to let users use and pay for what they want, promising on-demand services for their software or infrastructure needs [9]– [11].
Cloud platforms run through the internet protocols and they also use the virtualization technique which may be vulnerable to attack. Those attack might be coming from the traditional sources like address resolution protocol, IP spoofing, DoS etc. [12] [13]. They can also be from the other sources like Zero day attacks, for example, is the attack which is not known to the user and they are the main challenge as they are difficult to find out in the cyber security domain [14]. The earlier techniques were used for detection and prevention are not efficient enough to handle those attacks while also dealing with a large data flow. Machine learning methods are helpful in finding the type of attack, whether they are traditional or zero-day attack, it also includes the series of algorithm that can learn through the pattern of the attack and predict faster [15].

II. Literature Review

In this section, we will cover the detailed analysis and provide relevant studies on the security and threats of cloud computing. Recent studies have used Machine learning based approach to analysis the security issue in the cloud computing environment and provide solution for the threats.
Cloud computing itself is a very broad field, because it transmits and hosts its facilities on the Internet. It provides services to meet the needs of the clients and charges accordingly. This makes the Cloud crucial as people start to depend on it and organizations can now hire a Cloud service easily. Gaps in Cloud computing are defined as the trust issues between customers and Cloud providers, where customers fear policies that are hidden from them. On the other hand, Cloud providers are afraid that customers might take advantage and conduct attacks using their Cloud services.
Machine leaning with the help of patterns for cloud security. The rise of cloud security transitioned from basic defence parameter to more intelligent frameworks which are capable of managing the growing risks distributed environment. Research in adaptive control and optimizing the algorithms helped in managing the complex behaviours which are essential for maintaining the cloud infrastructure. As the cloud platforms increases the ability to host multi-tenant workload. The need for security becomes important. Recent Studies Proposes the system that uses game theory integrated with Deep Neural Networks to optimize network security more accurately in order to identify the intrusion in real time. These intelligent frameworks further enhanced by the integration of block chain technology which provided the decentralized and verifiable architecture to analyses the data and improve communication. These advancements are critical for professional management of hybrid cloud security where traditions parameters don't exist and ownership of data is decoupled. Detection mechanism have evolved to solve serious threads like distributive denial of service and common network attacks. Traditional methods will not able to handle large data flows whereas, machine learning models like support vector machines are more reliable researchers have found that combining SVM with other classification algorithm increases the accuracy of intrusion detection system(IDS).
To handle the constant flow of new data in cloud services specifically the incremental SVM method allow model to update without the need of programming providing training again. it helps in maintaining efficiency in the environment with heavy resource these proactive approaches are important for spotting zero – day attack or unknown attacks they work on finding the unusual behaviour detection to identify the deviation from regular uses that the system might miss. Beyond basic detection the literature focuses on need to manage security through fault tolerant software setup. Recent development like CC-COA method (cat boost integrated with the chameleon optimization algorithm demonstrate that adjusting the hyper parameter for log data based on category can greatly improve the accuracy.

TABLE I. COMPARISON OF EXISTING METHODS FOR CLOUD SECURITY

Paper Name	Problem Focus	Method Used	Result Summary	Key Limitation
Nassif et al. (2021)	Different security problems in cloud like DDoS and intrusion	Machine learning models like SVM and Random Forest	Most models give more than 90% accuracy	SVM works well, but results are mostly based on old data
A Comprehensive Review on Cloud Computing	Cloud system and its security issues	Review and study of cloud concepts	Clearly explains cloud security risks	No testing or result is shown
JETM Paper (83-JETM8685)	Intrusion detection in cloud systems	Machine learning classifiers	Better detection compared to traditional methods	Tested on limited data
APS-0250 Paper	Intelligent cloud security management	ML-based attack detection	Reduces false alarms and improves detection	Performance depends on quality of data

III. METHODOLOGY

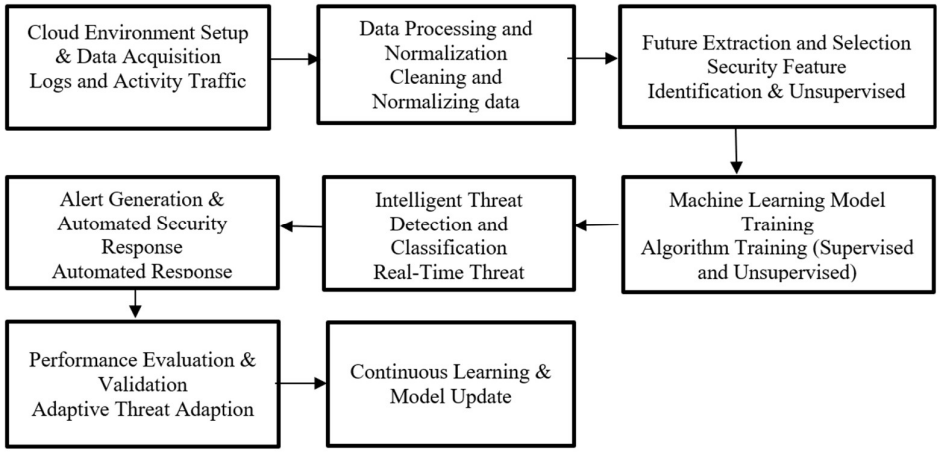

Figure 1. Proposed methodology for intelligent cloud security using machine learning

- We collect different kinds of security data from the cloud, such as system logs, user activity, network traffic, and API requests. This data helps us understand normal behaviour and spot any suspicious activity.
- Cleaning and Organizing Data: The data collected from the cloud can be messy or incomplete. So, we clean it by removing unnecessary information, filling in missing values, standardizing numbers, and converting categories into a usable format. This makes the data ready for analysis and helps the machine learning models work better.
- Choosing Important Features: From the cleaned data, we pick out the important details that indicate security issues, like how often users log in, unusual IP addresses, request timing, resource usage, or access levels. We select only the most useful features to make the system faster and more accurate.
- Training the Machine Learning Model: Next, we use machine learning to train the system on historical security data. Algorithms like Decision Trees, Random Forests, or SVM help detect known attacks, while anomaly detection or deep learning methods can catch unknown threats. The system learns what normal cloud activity looks like.
- Detecting and Classifying Threats: Once trained, the model monitors cloud activity in real-time and classifies events as normal or suspicious. It can identify threats like unauthorized access, DDoS attacks, malware, insider threats, or data leaks by noticing unusual patterns.
- Alerts and Automatic Responses: If a threat is detected, the system sends alerts to the cloud administrator. It can also take automatic actions, such as blocking suspicious IPs, stopping harmful sessions, isolating infected machines, or restricting access to resources to prevent damage.
- Checking Performance: We test how well the system works using standard measures like accuracy, precision, recall, and F1-score. We also compare it with traditional security methods to show how machine learning improves cloud security.
- Continuous Learning: Finally, the system keeps learning from new attacks. This helps it stay effective against evolving threats and zero-day attacks, keeping the cloud environment safe over time.

III. CONCLUSIONS

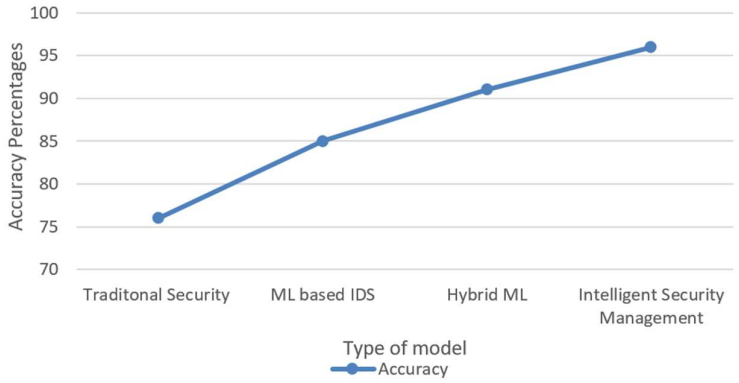

Figure 2: Line chart of comparison between previously present system and our proposed system

The above line chart shows the comparison between the previously present models and our proposed intelligent security management system.

At earlier there was traditional security management system that was used in cloud computing. They work on fixed rules that are once taught to the system and the fixed signature. Since they can't learn by them own so they were not able to handle new type of attack.

After traditional security management machine learning based security system came in action. These System are able to learn from their past data and are able to detect the attack better than the traditional type of security system. Although it was better then also it is unable to handle the real time cloud data and unknown types of cyber-attacks.

After that hybrid machine leaning model are came in action. The hybrid type of models is developed by using more than one machine learning algorithm. This model has better accuracy and the error are reduced from the previous type of model that were in use. It was good in all previously type of attack but it was not fully able to handle the new threats.

Now, our proposed intelligent security management system had shown the highest accuracy then previously present models. Our system handles the threats more efficiently because it continuously monitors cloud activity that are happening their it also learns from new data set and it is capable to auto respond to the attacks that are on cloud computing. It is able to detect the known and unknown types of attack in real time.

ACKNOWLEDGMENT

We would like to sincerely thank Mr. Arjun Singh, our project coordinator, and all of the professors for their counsel, inspiration, and unwavering support over the course of our project work. Without their assistance and insightful recommendations, our task would not have been feasible. We are deeply grateful to our esteemed Department Head, CSE Dr. S.P.S Chauhan for his counsel and assistance when needed.

We are also appreciative of Dr. Dhiraj Gupta -, our director, for providing the resources we needed to complete our project job effectively.

We would like to express our gratitude to all of our friends for their support and helpful advice throughout this effort. Finally, we have no words to express our sincere gratitude to our parents who have shown us this world and for everything they have given to us.

REFERENCES

[1] N. Basil, H.M. Marhoon, Correction to: selection and evaluation of FOPID criteria for the X-15 adaptive flight control system (AFCS) via Lyapunov candidates: optimizing trade-offs and critical values using optimization algorithms, in: e Prime Adv. Electr. Eng. Electron. Energy, 8, 2024 100589.

[2] N. Basil, H.M. Marhoon, A.F. Mohammed, Evaluation of a 3-DOF helicopter dynamic control model using FOPID controller-based three optimization algorithms, Int. J. Inf. Technol. (2024) 1–10.

[3] E. Balamurugan, A. Mehbodniya, E. Kariri, K. Yadav, A. Kumar, M. Anul Haq, Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN), Pattern Recognit. Lett. 156 (2022) 142–151.

[4] H.M. Marhoon, N. Basil, A. Ma'arif, Exploring blockchain data analysis and its communications architecture: achievements, challenges, and future directions: a review article, Int. J. Robot. Control Syst. 3 (3) (2023) 609–626.
[5] N. Indrason, G. Saha, Exploring Blockchain-driven security in SDN-based IoT networks, J. Netw. Comput. Appl. 224 (2024) 103838.
[6] R. Iqbal, R. Hussain, S. Arif, N.M. Ansari, T.A. Shaikh, Data analysis of network parameters for secure implementations of SDN-based firewall, Comput. Mater. Contin. 77 (2) (2023) 1575–1598.
[7] Velde, V., Mandala, S. K., Vurukonda, N., & Ramesh, D. (2021). WITHDRAWN: Enterprise based data deployment inference methods in cloud infrastructure.
[8] A. Gordon, The hybrid cloud security professional. IEEE Cloud Comput. 3(1), 82–86 (2016). https://doi.org/10.1109/MCC.2016.21
[9] R. Kumar, S. P. Lal, and A. Sharma, ''Detecting denial of service attacks in the cloud,'' in Proc. IEEE 14th Int. Conf. Dependable, Autonomic Secure Comput., 14th Int. Conf. Pervas. Intell. Comput., 2nd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), Aug. 2016, doi: 10.1109/DASC PICom-DataCom-CyberSciTec.2016.70.
[10] T. Halabi and M. Bellaiche, ''A broker-based framework for standardization and management of cloud security-SLAs,'' Comput. Secur., vol. 75, pp. 59–71, Jun. 2018, doi: 10.1016/j.cose.2018.01.019.
[11] M. R. Chinnaiah and N. Niranjan, ''Fault tolerant software systems using software configurations for cloud computing,'' J. Cloud Comput., vol. 7, p. 3, Jan. 2018, doi: 10.1186/s13677-018-0104-9.
[12] B.Xu,S.Chen,H.Zhang,andT.Wu,''Incremental k-NN SVMmethodin intrusion detection,'' in Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS), Nov. 2017, pp. 712–717, doi: 10.1109/ICSESS.2017.8343013.
[13] R. Moreno-Vozmediano, R. S. Montero, E. Huedo, and I. M. Llorente, ''Efficient resource provisioning for elastic cloud services based on machine learning techniques,'' J. Cloud Comput., vol. 8, no. 1, p. 5, Dec. 2019, doi: 10.1186/s13677-019-0128-9.
[14] A. AlEroud and G. Karabatis, ''A contextual anomaly detection approach to discover zero-day attacks,'' in Proc. Int. Conf. Cyber Secur., Dec. 2012, pp. 40–45, doi: 10.1109/CyberSecurity.2012.12.
[15] N. Chand, P. Mishra, C. R. Krishna, E. S. Pilli, and M. C. Govil, ''A comparative analysis of SVM and its stacking with other classifica tion algorithm for intrusion detection,'' in Proc. Int. Conf. Adv. Com put., Commun., Autom. (ICACCA) (Spring), Apr. 2016, pp. '1–6, doi: 10.1109/ICACCA.2016.7578859.