Semiconductor Optoelectronics
ISSN: 1001-5868

MACHINE LEARNING PERSPECTIVE FOR CLOUDCOMPUTING SECURITY: A REVIEW

Kushwaha Akhilesh[1], Dr. Warish Patel[2], Dr. Swapnil Parikh[3], Prof. Ankit Chauhan[4]

[1] Computer science and Engineering Department, Parul institute of Engineering and Technology,

Vadodara Gujarat, India; akhilesh.kushwaha0705@gmail.com

[2] Computer science and Engineering Department, Parul institute of Engineering and Technology,

Vadodara Gujarat, India; warishkumar.patel@paruluniversity.ac.in

[3] Computer science and Engineering Department, Parul institute of Engineering ,Vadodara Gujarat, India; swapnil.parikh17761@paruluniversity.ac.in

[4] Computer science and Engineering Department, Parul institute of Engineering and Technology,

Vadodara Gujarat, India; ankit.chauhan@paruluniversity.ac.in

Abstract— *Due to the blooming of digitalization of industries cloud computing become interest point for all the organization to run their businesses because it offers inexpensive infrastructure and can be operate remotely anywhere. With the ongoing improvement in cloud the services come the duty to uphold the confidentiality of cloud data and find defenses against potential threats. This paper identifies various security issues, attacks, and threats that individuals or organizations might encounter when accessing a cloud services or other distributed computing architecture, as well as how these issues might be reduced by utilizing tools like machine learning. By implementing machine learning technique like supervised, Unsupervised Learning, Semi-supervised Learning and Reinforcement Learning techniques we can tackle the Threats like confidentiality, Integrity, availability, and provide the solutions to threats in Cloud Model such as Platform as a Service, Infrastructure as a Service and Software as a Service by implementing ML techniques like Support Vector Machine, K-Means Algorithm, Artificial-Neural-Network Algorithm (ANN), K-nearest Neighbours (KNN), Decision Tree, Naive-Bays Algorithm, and Decision Tree. Based on each approach's traits, advantages, and drawbacks, we assessed its effectiveness and made comparisons. We also suggest potential directions for future research to protect cloud frameworks.*

Keywords—: *Cloud computing, Machine Learning, Cloud Threats, Cloud Threat Solutions, defend, Secure, Vulnerability.*

INTRODUCTION

With the emergence of a pandemic, the digitization every basic need has also contributed to the use of cloud computing and the growth of the cloud sector. Cloud based services has extended its

claws in all practicable ways and has expand over important domains and institutions. In recent years, the basic services for delivering over the Internet, known as "cloud computing", cloud has undergone tremendous transformation.

Despite the many advantages and simplicity of use that cloud computing provides. The continued existence of security issues prevents the speedy adoption of computing technologies. Gaining consumer trust is more difficult because of the data's sensitivity to cyberattacks.

Integrity, availability, and confidentiality are three categories under which the major security flaws in cloud technology are often categorized. For increased scalability and better usability, cloud computing enables users, including different businesses, individuals, to serve their computer needs (software, hardware, storage, etc.) control over their data and computer resources [1].

In order to maintain their user base and competition, cloud service providers must ensure the security of both their user programmes and data. Today's businesses want to expand their on-premises infrastructure and offer cloud computing options, but many of them are unsure of how to secure their applications and data. 263 IT executives and their line-of-business counterparts were polled by the International Data Corporation to assess their preferences and the utilisation of IT cloud services by their organizations. One of the cloud computing industry's top concerns was security [2].

Literature Survey

A. Cloud Services

Software-as-a-Service, platform-as-a-Service, and Infrastructure-as-a-Service are the three primary categories of cloud computing services [3].

1. Infrastructure-as-a-service

IaaS manages computer hardware as a service, enabling infrastructure scalability and resource provisioning issues without requiring a substantial outlay of cash and time. Computer tools includes network storage capacity, virtual servers or computers, data centres, processors, and memory. IaaS also emphasises firewall, intrusion detection, monitoring virtual machines, and other Computer securities related to this topic. PaaS is a type of service providing model that offers cloud services in the form of IDEs, applications, Framework and development tools. Relationships with other businesses, lifecycle design, and infrastructure security are just a few of the difficulties that faces PAAS [6,8].

2. Platform-as-a-service

Customers are provided with operating system access, enabling them to upload their software and other software to the cloud. PaaS refers to providing IaaS in addition to running a server programme [6,8].

3. Software-as-a-service

SaaS is "On-Demand Software." A cloud service provider hosts the services in this style of software distribution. End consumers don't need to install any software on their devices to access these services because they are accessible to them over the internet [6,8].

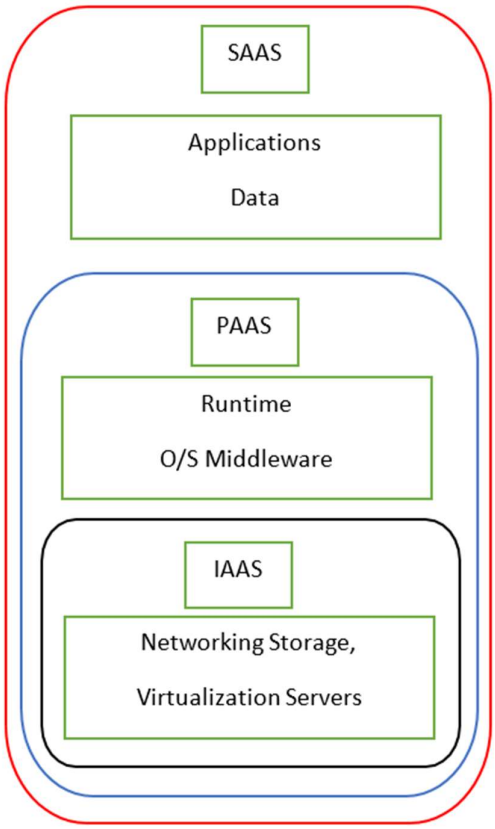

Fig 1 Cloud Models

B. How machine learning approach for security concern?

In order identify insider threats to improve malware detection in encrypted traffic., forecast where "badneighbourhoods" are online to keep users safe while browsing, or safeguard data in the cloud by spotting suspicious user behaviour, machine learning constantly learns by analyzing data to find patterns. The foundation of machine learning is the algorithms that are used to train the models. Depending on the nature of the problem to be solved, a machine learning algorithm is selected. The process of using machine learning to address a problem begins with the collecting of data, which is followed by the tasks of datapreparation, data analysis, model training, model testing, and ultimately model deployment for real usage [10].

C. Types of machine Learning

Machine learning allows computers to learn automatically from historical data. Machine learning uses different algorithms to construct models and make predictions based on historical data or information. It is currently used for a variety of tasks including image recognition, security analyzing, recommendation systems, and many others.

A. Supervised Machine learning

In order to predict future results, supervised ML algorithms are trained on datasets that have

been tagged and mapped with the relevant output target values. The main responsibility of the supervised machine learning algorithm is to observe theincoming data and assign the proper class to it. Onlyby getting trained earlier using a large volume of correctly labelled dataset with well-defined classes can this class allocation be performed.

Classification and regression problems can be solved using supervised machine learning algorithms. Supervised machine learning algorithms are used to solve problems where the goal variable is categorical (yes/no), whereas Regression ML techniques are used to solve problems where the target variable is continuous rather than categorical [11].

B. Unsupervised Machine Learning

Unsupervised ML methods use datasets without labels or classification to train ML models. Unsupervised ML algorithm discovers and learns all the data insights, such as data patterns, classes, and categories, on its own by analyzing the vast dataset. Unsupervised machine learning falls into two categories: clustering andassociation. An algorithm based on clustering creates groups of related data that have common traits. The relationship between the data that can be put together is discovered by association-based algorithms, though[11].

C. Reinforcement Learning

reinforcement provides idea about how intelligent agents should behave in any situation to maximize theidea. One of the three fundamental of machine learning together with supervised learning and unsupervisedlearning it makes reinforcement learning better.

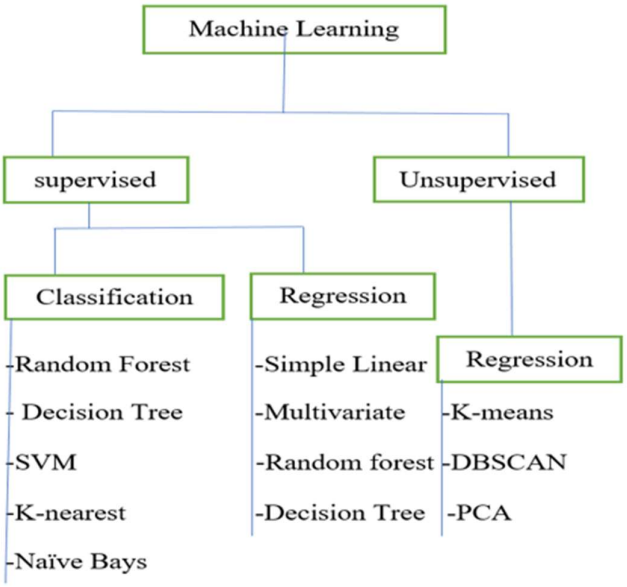

Fig 2 Classification of Machine LearningAlgorithm

D. Cloud Security Threats

Security issues can occur in system due to misconfiguration, faults, attacks, vulnerability, or loopholes. The various features of cloud computing contribute to cloud security issues is Data issue, Data privacy issues, Data integrity issue and data confidentiality issues are among them.

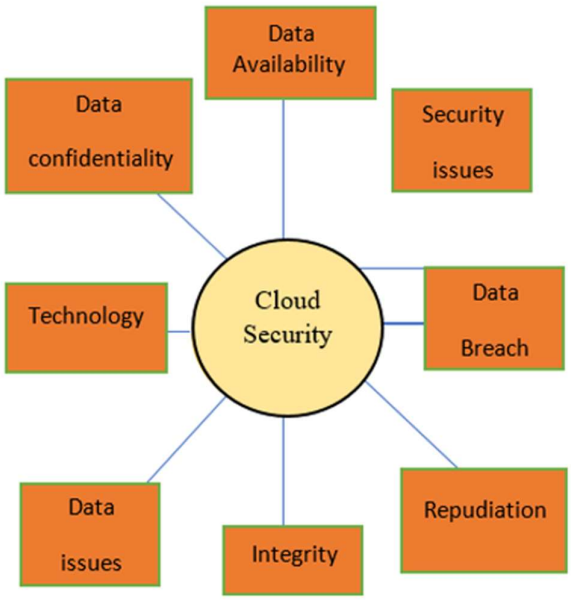

Fig 3 Cloud Security Issue

1. Confidentiality

Protecting sensitive or private material from unauthorised access is the goal of confidentiality measures. As a result, threats to client data or information are included in the category of confidentiality threats. These dangers can result from an outside attack, an insider intrusion, or any other type of data leakage.

Given the dispersed computing model that the cloud provides, external attacks are the most frequent and pertinent. These typically result from cloud application launches in unsafe environments, or they could involve remote software or hardware attacks on the application that was launched [13].

Insider threats or invasions are caused by weak authorization and authentication access provisioning, which can result in unauthorised or unwanted access to information by a person connected to the cloud [14,15]

2. Integrity

Even if the attacker is unable to steal the data due tosecrecy, it is still possible for it to alter, add new information, or remove some specific fragments before reaching its target. Authentic, consistent, and trustworthy data should be stored in the cloud. Additionally, integrity makes sure that a message isn't damaged as it's being broadcast through the media.

Backing up your data, implementing access controls, keeping an eye on your audit trail, and encrypting yourdata are the simplest ways to protect data integrity [14,15]

3. Availability

It implies that individuals can access systems and datawhenever they need to, regardless of the situation— including power outages or natural disasters. Even if you fulfil the other two CIA Triad standards, your firmmay suffer if you lack availability [14,15].

It is a key point of computing infrastructure that persists the functioning even if few components fail. This is critical for mission-critical systems, which cannot tolerate service interruptions and any downtime can result in damage or financial loss during cloud Attacks

A cloud cyber-attack is one that targets off-site serviceplatforms that provide storage, computing, or hosting services via their cloud infrastructure. Attacks on service platforms that use service delivery models [16,17,18,19].

The primary goals of cloud computing cyber-attacks are to get access to user data. Both can cause serious

harm to cloud users and undermine trust in cloud security.

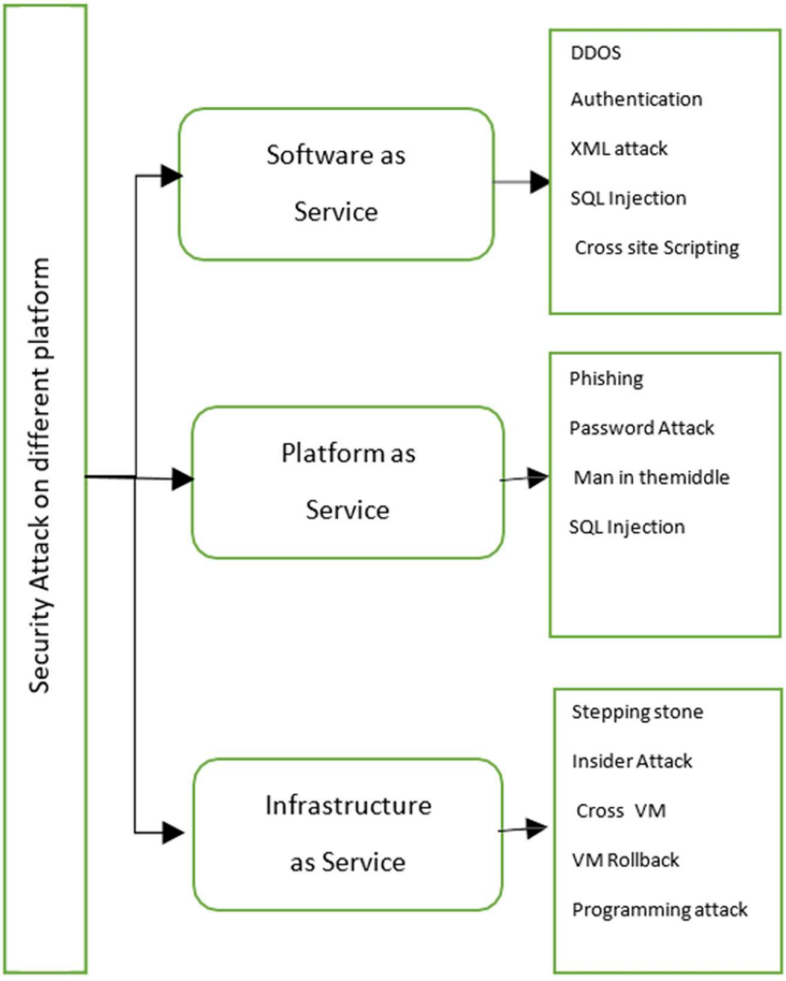

Fig 4 Cloud Attacks

1. Denial of service (Dos) attack

This attack is concern with the service available for users. Distributed denial of service (DDos) makes a multiple Request at a time due to which the service become temporary down or unavailable for users.

2. Authentication Attack

This type of attack targets and attempts to exploit the authentication process used by a website to

verify a user's, service's, or application's identity. Some Authentication attack are Brute force, Insufficient Authentication, Weak Credentials.

3. SQL Injection attack

This attack takes advantage of web application database access. As a result, the intruder tries to gain access to the various database or bypass the authentication security by injecting different commands or SQL statements.

4. Cross- Site Scripting

Cross-site scripting is an attack in which an attacker inserts code into a trustworthy website so that it runs when the victim accesses it. Numerous methods can be used to insert that dangerous code. The most frequent places to utilize it at the end of URLs and on pagesthat host user-generated material. Cross-site scripting. Technically it is client-side attack

5. Phishing attack

The goal of a phishing attack is to trick people for providing their personal information by sending them to a fake link. By using a phishing attackers stole the information can access the cloud services.

6. Man-in-the-Middle attack

The security of the Internet and cloud computing services can be seriously compromised by man-in-the-middle attacks, in which an attacker captures packets sent between clients and servers over a network in order to steal sensitive information or manipulate the packets. Man-in-the-middle attack detection is both important and difficult.

7. Cloud malware injection attack

Cloud computing systems are attacked by cloud malware injection. A hacker will try to introduce a harmful virtual machine or service into the cloud-based system. As a result, it creates malicious SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service) service implementation modules or virtual machine instances (Infrastructure asa service) Malicious Insider attack

A malicious insider, also known as a Turncloak, is someone who maliciously and intentionally uses legitimate credentials to steal information for financial or personal gain. For example, a person who harbours resentment toward a former employer, or an opportunistic employee who sells confidential information to a competitor. Turncloaks have an advantage over other attackers because they are familiar with an organization's security policies and procedures, as well as its vulnerabilities.

8. Cross VM attacks

To keep Virtual Machines (VMs) and processes separate, cloud service providers works to uphold the highest degree of isolation between them. To divide VMs that share a physical network, this logical isolation generates an internal virtual network. Co- residing VMs are susceptible to cross-VM assaultsbecause they use the same virtual network, hardware, and VMM (Virtual Machine Monitor) as one another. From shared memory, network connection other shared resources, or by taking over the non-root machine, a malicious VM may be able to access or command other VMs.

Table 1. Summary related Work

Year	Author	Publisher	Research Purpose	Research Gap
2022	S. H. Alrasheed [19]	IEEE International Conference	This study focuses on cloud computing security, including the difficulties, problems, dangers, and remedies.	It includes Recent Threats but need to implement more ML Methods
2021	S. Mahipal and V. C. Sharmila [20]	IEEE International Conference	They have indicated that there are many sorts of cloud attacks such as virtual machine side channel attacks, hypervisor attacks, virtual machine migration attacks, and so on that make the services unsafe, including hypervisor assaults.	Includes VM ML based attack only. More Attacks need to be added.
2021	S. Wang [21]	IEEE Access (Volume:9)	The process for each machine learning category is described, along with the techniques and advantages. There is also a comparison of several machine learning models.	Machine learning recent threats and attacks needs to implemented.
2021	A. B. Nassif [22]	IEEE Access (Volume:9)	Describe the concepts and strategies used in ML and cloud security in a systematic literature review (SLR).	It includes SLR but does not include any implementation method.
2020	Z. Chkirbene [23]	IEEE International Conference	ways for detecting intrusions based on machine learning. The performance of the suggested model has been assessed using the UNSW dataset, and it	It covers Intrusion detection with ML techniques.

			has been compared to cutting-edge methods.	
2020	A. Mondal[24]	IEEE International Conference	Considers many cloud computing security concerns, such as believe, authenticate, privacy, latency, data splitting, and virtual machine security. discussed how to overcome these issues.	Recent threats need to be included.
2020	A. Patel [25]	ICECA	Trustworthy cloud service providers use a variety of technologies to deliver various services via the Internet, creating a variety of security risks.	It includes different security attacks but need to add countermeasure based on ML methods
2019	D. Jing and H. -B. Chen [26]	IEEE International Conference on ASIC (ASICON)	SVM is combined with a new scaling strategy for binary-classification and multi-classification testing. Its efficacy is measured by its accuracy, detection rate, and false positive rate. The experimental results show that the proposed SVM algorithm outperforms competing alternatives.	Need to include more cloud attacks and ML based solutions.

2019	Bala, Asvija[27]	Research gate conference	Along with a list of obstacles to implementingthem, a full explanation of the various solutions offered against the identified risks is presented.	Need to Implement Recent cloud Threatsemerging in IAAS
2018	D. R. Bharadwaj[28]	IEEE InternationalConference	Traditional multi-tiered architecture Cloud Threat Defense	Need to work on Security Risk over IAAS and solution withML
2018	K. A. Torkura[29]	IEEE InternationalConference	A detailed Security information and machinelearning usage.	Needs ML methods forrecent threats

Conclusion and Future Scope

Data in the cloud is critical, and its security must not be compromised in any way. The researchers use a variety of new technologies and security algorithmsto improve the security of the cloud ecosystem.

Machine learning discovers a vast opportunity to provide more accurate and automated defence against known and unknown cloud attacks. The goalof this survey is to understand a current scenario of research work in the field of cloud security using machine learning.

In future, we proposed a method which can detect the attacks like intrusion detection and DDos attack detection that will use improved machine Learning Algorithm to provide more accurate cloud data security.

References

1. Nhlabatsi et al., "Threat-Specific Security Risk Evaluation in the Cloud," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 793-806,April-June2021, doi:10.1109/TCC.2018.2883063.

2. M. K. Sasubilli and V. R, "Cloud Computing Security Challenges, Threats and Vulnerabilities," 2021 6th International Conference on Inventive Computation Technologies (ICICT), 2021, pp. 476-480,doi: 10.1109/ICICT50816.2021.9358709.

3. M. Saraswat and R. C. Tripathi, "Cloud Computing: Analysis of Top 5 CSPs in SaaS, PaaS and IaaS Platforms," 2020 9thInternational Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 300-305, doi:

10.1109/SMART50582.2020.9337157.

4. https://www.researchgate.net/publication/342492294_Cloud_Computing_Virtualization_of_Resources_Allocation_for_Distributed_SystemsGupta

5. S. Patil, R. Dharaskar and V. Thakare, "Digital Forensic in Cloud: Critical Analysisof Threats and Security in IaaS, SaaS and PaaS and Role of Cloud Service Providers," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2017, pp. 1-7, doi:10.1109/ICCUBEA.2017. 8463984.Li,

6. Naren.J, & Sowmya, S.K. & Deepika, P.. (2014). Layers of Cloud – IaaS,PaaS and SaaS: A Survey.International Journal of Computer Science and Information Technology. Vol. 5 (3). 4477 - 4480.

7. Mohammed J. Sadeeq & Subhi R. M. Zeebaree, 2021."Semantic Search Engine Optimisation (SSEO) for Dynamic Websites: A Review," International Journalof Science and Business, IJSAB International,vol.

8. <https://ideas.repec.org/a/aif/journl/v5y2021i3p148-158.html>

9. Hindreen Rashid Abdulqadir & Nawzat Sadiq Ahmed, 2021."Fog Computing Analysis Based on Internet of Thing: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 137-147.

10. <https://ideas.repec.org/a/aif/journl/V5y2021i3p137-147.html>

11. Butt, U.A.; Mehmood, M.; Shah, S.B.H.; Amin, R.; Shaukat, M.W.; Raza, S.M.; Suh, D.Y.; Piran, M.J. A Review of Machine Learning Algorithms for Cloud Computing Security. Electronics 2020, 9,1379

12. Saranyaa, T., Sridevi, S., Deisy, C., Chung, T.D., Khan, M.K.A.: Performance Analysis of Machine Learning Algorithmsin Intrusion Detection System: A Review. Procedia Computer Science, Vol 171, pp. 1251-1260, 2020.

13. Alzubi, J., Nayyar, A., Kumar, A.: MachineLearning from Theory to Algorithms: An Overview. Journal of Physics: Conference Series, Volume 1142, Second National Conference on Computational Intelligence2018, Bangalore, India.

14. R. Kumar and M. P. S. Bhatia, "A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability," 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON), 2020, pp. 334-337, doi:10.1109/GUCON48875.2020.9231255.

15. Kaiying Feng and Junxing Zhang, "Improving availability and confidentiality of shared data under the multi-cloudenvironment," 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2017, pp. 6-10, doi: 10.1109/ICCCBDA.2017.7951875.

16. Oberoi, Priya, and Sumit Mittal. "SURVEY OF VARIOUS SECURITY ATTACKS IN CLOUDS BASED ENVIRONMENTS." International Journalof Advanced Research in Computer Science 8.9 (2017)

17. G. Nenvani and H. Gupta, ``A survey on attack detection on cloud using supervised learning techniques," in *Proc. Symp. Colossal Data Anal. Netw.(CDAN)*, Mar. 2016, pp. 1_5, doi:10.1109/CDAN.2016.7570872.

18. 2021 International Conference on Information Science and Communications Technologies (ICISCT) | 978-1-6654- 3258-0/21/$31.00 ©2021 IEEE | DOI:

10.1109/ICISCT52966.2021.9670220

19. N. C. S. K. P. J. Vijaya Chandra, "Authentication and Authorization Mechanism for Cloud Security," International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, no.6, 2019 S. H. Alrasheed, M. Aied alhariri, S. A. Adubaykhi and S. El Khediri, "Cloud Computing Security and Challenges: Issues, Threats, and Solutions," 2022 5th Conference on Cloud and Internet of Things (CIoT), 2022, pp. 166-172, doi: 10.1109/CIoT53061.2022.9766571.

20. S. Mahipal and V. C. Sharmila, "VirtualMachine Security Problems and Countermeasures for Improving Quality of Service in Cloud Computing," 2021International Conference on ArtificialIntelligence and Smart Systems (ICAIS),2021, pp. 1319-1324, doi:10.1109/ICAIS50930.2021.9395922. S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez and B. Rubinstein,"Machine Learning in Network AnomalyDetection: A Survey," in *IEEE Access*, vol.9, pp. 152379-152396, 2021, doi:10.1109/ACCESS.2021.3126834

21. S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez and B. Rubinstein, "Machine Learning in NetworkAnomaly Detection: A Survey," in IEEE Access, vol. 9, pp. 152379-152396, 2021, doi: 10.1109/ACCESS.2021.3126834.

22. A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A SystematicReview," in IEEE Access, vol. 9, pp. 20717-20735, 2021, doi:10.1109/ACCESS.2021.3054129.

23. Z. Chkirbene, A. Erbad, R. Hamila, A. Gouissem, A. Mohamed and M. Hamdi, "Machine Learning Based Cloud Computing Anomalies Detection," in *IEEENetwork*, vol. 34, no. 6, pp. 178-183, November/December 2020, doi: 10.1109/MNET.011.2000097

24. Mondal, S. Paul, R. T. Goswami and S.Nath, "Cloud computing security issues & challenges: A Review," 2020 International Conference on Computer Communication and Informatics (ICCCI), 2020, pp. 1-5, doi: 10.1109/ICCCI48352.2020.9104155.

25. A. Patel, N. Shah, D. Ramoliya and A.Nayak, "A detailed review of Cloud Security: Issues, Threats & Attacks," 20204th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 758-764, doi:10.1109/ICECA49313.2020.9297572.

26. D. Jing and H. -B. Chen, "SVM Based Network Intrusion Detection for the UNSW-NB15 Dataset," 2019 IEEE 13th International Conference on ASIC (ASICON), 2019, pp. 1-4, doi: 10.1109/ASICON47005.2019.8983598

27. Bala, Asvija & Rajagopal, Eswari & Balakrishnan, Bijoy. (2019). Security in Hardware Assisted Virtualization for Cloud Computing - State of the Art Issues and Challenges. Computer Networks. 151. 10.1016/j.comnet.2019.01.013.

28. D. R. Bharadwaj, A. Bhattacharya and M. Chakkaravarthy, "Cloud Threat Defense – A Threat Protection and Security Compliance Solution," 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2018, pp. 95-99, doi: 10.1109/CCEM.2018.00024.

29. K. A. Torkura, M. I. H. Sukmana, F. Cheng and C. Meinel, "Security Chaos Engineering for Cloud Services: Work In Progress," 2019 IEEE 18th International Symposium

on Network Computing and Applications (NCA), 2019, pp. 1-3, doi: 10.1109/NCA.2019.893504.