Leveraging Machine Learning to Enhance Cloud Security

A.Punitha Rosline[1], S. Sivagurunathan[2]
[1,2] *The Gandhigram Rural Institute (Deemed to be University), Gandhigram, Dindigul – 624 302, Tamil Nadu, India.*

Abstract
Cloud computing is a technology that provides virtual resources via the Internet. It provides end users with on-demand, scalable, and metered services under a pay-per-use paradigm. In today's world, almost every organization depends significantly on this technology for storage, cost savings, infrastructure, development platforms, data processing, and analytics. A cloud service provider (CSP) provides services that consumers may access at any time and from any location using web applications on the Internet. It is critical to secure the security of cloud infrastructure, and many research projects employ various technologies to provide protection against powerful cloud threats. Recently, machine learning has shown considerable promise in terms of increasing cloud security. Machine learning methods, as opposed to traditional methodologies, may automate cloud threat detection with greater accuracy by developing algorithms on real-world information. This article explores some of the most current research on leveraging machine learning as a security technique to protect cloud data from various forms of cloud attacks.

Keywords: Cloud Computing, Cloud Attacks, Cloud Security, Machine Learning.

1.Introduction

Cloud computing is the shared use of virtual resources available over the Internet or a network. It provides instant access to information, scalability, and flexibility, with numerous applications in both business and industry. Cloud computing lowers expenses by allowing firms to exchange information more easily. However, as cloud computing environments become more widespread, developers' security concerns grow. Insufficient security protocols have the potential to erode user trust in cloud-based data [1].

Although cloud computing provides several benefits and capabilities, there are concerns about assuring secure data access and storage. Signs of serious security problems include vendor lock-in, lost multiple leases, losing control, service interruptions and data loss. This article discusses many forms of attacks and security challenges within the context of cloud computing. Security in cloud environments is still difficult. Even well-known cloud service suppliers such as Google and Amazon, who deploy strict security procedures, are vulnerable to cyber-attacks. Cloud security falls into five important categories: safeguarding information, authentication protection, safety of networks, security of infrastructure, and software security [2].

Machine Learning as a benefit, is utilized in cloud computing to invigorate securities against a few sorts of cloud attacks. Many intrusion detection systems that have appeared utilizing machine learning algorithms have substantially boosted the accuracy of attack detection, assuring sustained business operations [3]. In this article, Chapter 2 gives an overview, Chapter 3 lists various attacks, Chapter 4 lists solutions to the attacks and Chapter 5 concludes the article.

2.Overview of cloud computing

Virtual Machines and virtual services are called Cloud Computing (CC). It is the provision of numerous services such as data storage, servers, databases, networks, and software over the Internet. This chapter provides an overview of Cloud technology including its service architecture, deployment model, Cloud attacks, benefits and drawbacks [4].

2.1. Architecture of cloud services

Cloud engineering is primarily categorized into three cloud-service models: Infrastructure-as-a-Service (IaaS), the last layer, which provides the primary base for the other levels; Platform-as-a-Service (PaaS), the core layer, provides an application layer that operates as a service on demand. Software as a Service (SaaS) is the top layer of the cloud computing concept, often known as the cloud service stack. It builds on the preceding two levels, Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). This architecture uses a bottom-up approach.. Figure 2.1 illustrates the internal architecture of cloud computing [5].

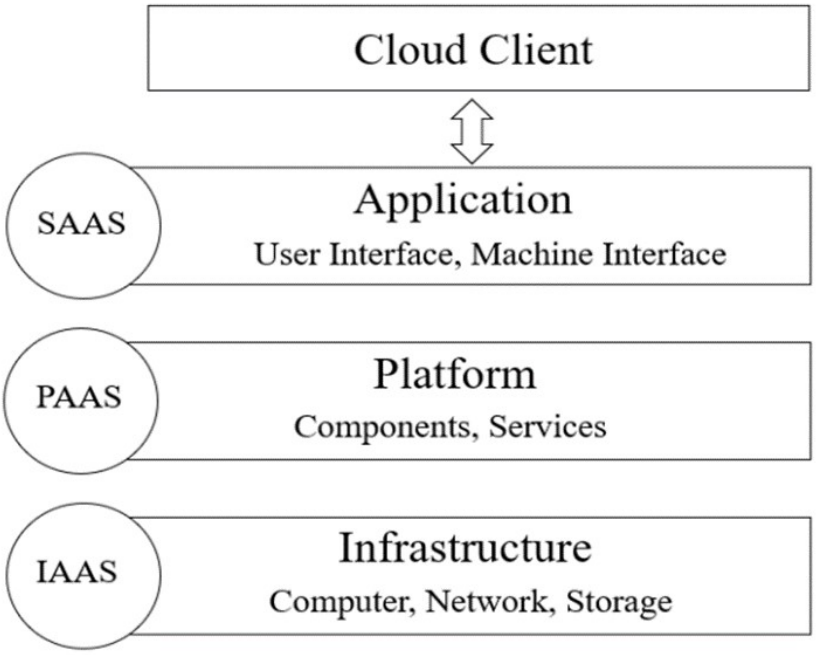

Figure 2.1 Cloud Service Architecture Layers

Software as a Service (SaaS):

SaaS allows users to access software applications housed on cloud infrastructure. These programs do not require installation on users' local devices. Examples include Google Workspace, Microsoft Office 365, and Salesforce [6][7].

Platform as a Service (PaaS):

PaaS offers users platforms and tools to develop, test and deploy applications. It provides a framework for developers to build upon without the complexity of managing underlying infrastructure. Google App

Engine, Microsoft Azure App Service and Amazon Web Services Elastic Beanstalk are other examples [8].

Infrastructure as a Service (IaaS):

IaaS provides consumers with virtual infrastructure resources over the internet. This comprises computer, storage, and networking resources. The resources can be scaled up or down by the user according to their needs. Examples are Amazon EC2, Microsoft Azure Virtual Machines, and Google Compute Engine [9].

2.2 Cloud deployment model

Cloud Computing has a total of four deployment models: Private, Public, Hybrid and Community cloud [10]. Every deployment model has a distinct value proposition along with a list of expenses. Determining the deployment model is therefore a challenging and important choice. Figure 2.2 represents the models for cloud deployment in Cloud Computing [11].

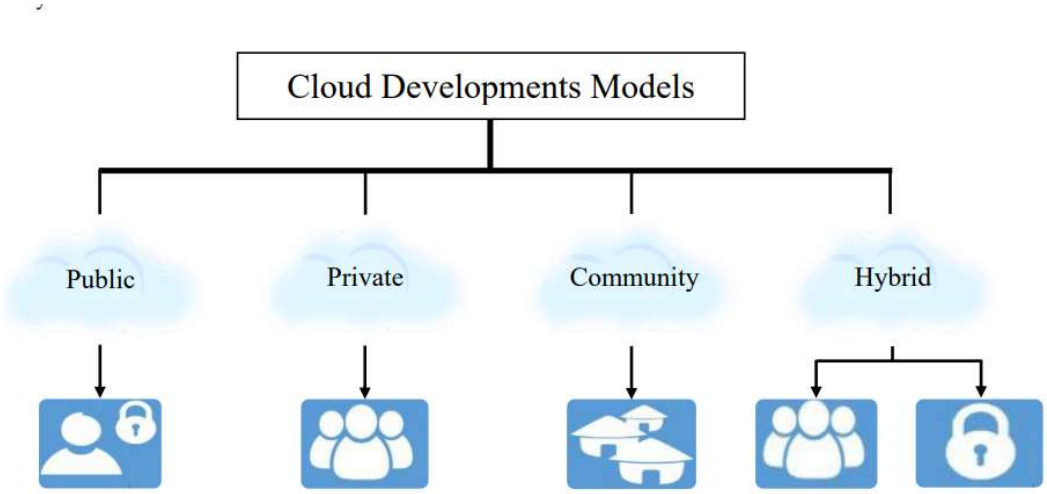

Figure 2.2 Cloud Deployment Model

Private Cloud:

A private cloud arrangement is reserved exclusively for a single enterprise and serves several consumers inside that organization. It's owned, controlled and administered by the organization itself. [12].

Public Cloud:

People all around the world can use public cloud infrastructure, as can major industrial groups. A cloud service provider hosts and manages it in one of their data centers [13].

Community Cloud:

A community cloud setup is utilized by a group of clients that have common goals or requirements. It is frequently shared by many groups in the community. In this type of strategy, the cloud is shared by

several organisations with similar interests or concerns. It can be managed by the member organizations or a third party [14].

Hybrid Cloud:

A hybrid cloud environment connects two or more separate cloud infrastructures, such as private, community, or public clouds, allowing data and applications to be transferred across them [15].

3. Classification of Cloud attacks:

The major purpose of this study is to identify potential attacks on the Cloud environment and effective remedies. Cloud Computing provides services via IaaS, PaaS and SaaS. This article classifies numerous attacks based on the service delivery paradigm of cloud computing. [16]. An attacker can conduct a variety of attacks using cloud vulnerabilities. The primary attacks are summarized in the following subsections:

3.1 Security Attacks on the SaaS Cloud Layer

In the Software as a Service (SaaS) concept, security measures are the provider's responsibility. Software as a service (SaaS) is owned, delivered, and supported remotely by one or more providers. Despite this, many consumers remain dubious of the SaaS model, particularly in terms of data security, which includes data ownership, backup, access, location, availability, identity management, and authentication. The existing articles used Deep Belief Network (DBN) to detect an attack in the SaaS cloud tiers. [17].

3.2 DDoS Attack:

A Denial of Service (DoS) attack intends to make the affected services unavailable to authorized users. In such attacks, the targeted server is inundated with requests, making the service unreachable to legitimate users. This is similar to attempting to access a website and receiving an error message due to server overload, which occurs when the server's processing capability exceeds the amount of requests it gets. As a result, the attacker does not need to flood all "n" servers that offer a given service in the target. They can just flood a single cloud-based address to completely disable the desired service. In existing articles, K-Means Clustering was used to detect DDoS attacks. [18].

3.3 Attacks on Virtual Machine (VM) or Hypervisor

Given virtualization's fundamental role in cloud computing, attacks on Virtual Machines (VMs) or hypervisors pose major concerns. Attackers can gain control of virtual machines by compromising the underlying hypervisor layer. New vulnerabilities, including zero-day vulnerabilities in virtual machines (VMs), can allow attackers to get access to the hypervisor or other virtual machines. For example, consider a zero-day vulnerability in application virtualization software. HyperVM was abused, resulting in the destruction of several websites housed on virtual servers. In previous articles, they employed K-means clustering and Auto encoders. [19].

3.4 Side Channel Attack

These attacks make use of the physical qualities of materials to acquire data that can expose a diagram or pattern of the target system. Side channel attacks are reasonably straightforward since different virtual machines use the same equipment. Equipment sharing can be risky without proper hardware safety precautions. In cloud computing settings, the infrastructure may be mapped and a virtual machine's location is identified. Attackers can then create fresh virtual machines until one becomes co-resident with the target virtual machine Once enabled, the attacker can get critical information from the authorized virtual machine. This type of attack is known as a side-channel attack [20]. In several research publications, Linear Regression (LR) and Quadratic Discriminant Analysis (QDA) are applied.

3.5 Phishing Attacks

In cloud computing, phishing attacks are classified into two forms. The first category includes abusive conduct, which occurs when an attacker uses one of the cloud services to host a phishing attack site. The second type includes using standard social engineering approaches to hijack cloud accounts and services [21]. Existing technologies protect applications against phishing attempts using approaches such as Support Vector Machines (SVM), Logistic Regression (LR), Bayesian Additive Regression Trees (BART), Classification and Regression Trees (CART), and Neural Networks (NN).

3.6 Man-In-The-Middle Cryptographic Attacks

This attack occurs when an attacker resides between two users in a cloud environment. When attackers are positioned in the communication channel, they may intercept and manipulate communications. [22]. Many articles suggested that algorithms like Random Forest (RF), eXtreme Gradient Boosting (XGBoost), Gradient Boosting (GB), and Decision Trees (DT) might enhance the efficiency and accuracy of cloud applications.

3.7 SQL Injection Attack

SQL injection attacks on the HTTP/HTTPS protocol attempt to sneak beyond the Web Application Firewall (WAF) and get unauthorized access to restricted data. SQL injection is a type of web attack in which an attacker enters inputs into a system and executes harmful statements [23]. The victim system is frequently not equipped to handle this input, resulting in data leakage and/or unauthorized access by the attacker. In this situation, the aggressor can access and/or manipulate the data, impacting all areas of security, including confidentiality, integrity, and data availability. Many research studies propose that a hybrid strategy including algorithms such as ANN, SVM, NB, DT, and RF, is utilized to boost online security.

3.8 Port Scanning Attack:

Port scanning is a technique for identifying open, closed and filtered ports on a cloud system. Port scanning allows attackers to acquire information like as the services operating on a system, the IP and MAC addresses connected with a router, gateway and firewall rules via open ports. In a cloud setup, attackers can search for open ports to locate the ports where these services are supplied [24]. In previous publications, SVM analyses real-time network traffic, detecting unexpected patterns that indicate a port scanning attack. Its capacity to analyse high-dimensional data and locate the ideal hyperplane for classification allows it to detect subtle and complicated attacks.

3.9 Malware Injection Attack:

Malware injection attacks in cloud computing include introducing malicious code into the data being transferred between the cloud provider and the end user. This stresses the need of user identification and authorization in ensuring secure data transport. To carry out this attack, the adversary must create a malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), which is then introduced to the cloud system. The attacker further tricks the cloud system into recognizing the new service implementation instance as a legitimate one for the targeted service. However, the cloud system forwards legitimate user requests to the malicious service implementation, where the adversary's code is executed [25]. In this article, a Support Vector Machine is used to protect data against Malware injection attacks.

4. Techniques to secure data in the cloud

Data security in the cloud is essential for preventing unwanted access, data breaches, and other security issues [26]. Here are some ways to secure data in the cloud from the available literature:

Authentication and Identity:

Passwords, security tokens, and biometric techniques such as fingerprint scans are all suitable for strong authentication. Consider utilizing multi-factor authentication to increase security. Manage identities centrally to minimize synchronization concerns while working with numerous Cloud Service Providers (CSPs) [27].

Data Encryption:

Strong encryption techniques are employed to safeguard sensitive data, both at rest and in transit [28].

Malware-Injection Attack Solution:

To guard against malware injection attacks, use client virtual machines in a central storage system handled by a hypervisor. Integrity verification can be performed using mechanisms such as File Allocation Table (FAT) and Interrupt Descriptor Tables (IDT) [29].

Flooding Attack Solution:

Organizing cloud servers into fleets based on different sorts of requests is a solution. We can use a name server to update destinations and states and manage tasks using the Hypervisor. Use of RSA to encrypt Process IDs (PIDs) and authenticate approved customer requests is also a solution. Implementing these measures can help avoid several security risks while preserving the safety and confidentiality of data in the cloud. [30].

Intrusion Detection Systems:

Attacks can be reduced by adopting an Intrusion Detection System (IDS), which improves security by monitoring network traffic, log files and user activity. IDS is a security auditing and monitoring system that gathers data from several sources to detect network policy infractions. [31].

Federated Identity Management:

Federated Identity Management (FIM) is the process of managing identities by allowing users to link their numerous identities, which may then be utilized across many services and organizations, independent of geography. This technique, known as identity federation, enables a collection of businesses to establish trust and work safely. Single Sign-On (SSO) is a sort of federated identity that allows users to access multiple services with a single set of credentials. [32].

Secure Socket Layer (SSL) :

The Secure Socket Layer (SSL) and its successor, Transport Layer Security (TLS), are protocols for safeguarding cloud data over networks. A suitable SSL/TLS architecture is critical for securing data in transit between clients and cloud services [33].

Table 4.1 summarizes the recent machine learning algorithms to thwart cloud attacks.

Table 4.1 Machine Learning Algorithm for Various Attacks

S.No	Title	Year of Publication	Nature of Attacks	Machine Learning Algorithm Used
1	A Machine Learning-based attack detection and mitigation using a secure SaaS framework [34].	2022	SaaS Attack	Deep Belief Network
2	Detection of DDoS Attacks using Machine Learning Algorithms [35].	2022	DDoS Attack	Random Forest, K –Means clustering, Hybrid approaches
3	Machine Learning For Security: The Case of Side-Channel Attack Detection at Run-time [36].	2019	Side Channel Attack	Linear Regression (LR), Quadratic Discriminant Analysis
4	Detection of E-Mail Phishing Attacks – using Machine Learning and Deep Learning [37].	2022	Phishing Attacks	Support Vector Machines (SVM), logistic regression (LR), Bayesian additive regression trees (BART), classification and regression trees (CART), neural networks(NN)
5	Man-in-the-middle and denial-of-service attack detection using machine learning algorithms [38].	2023	Man-In-The-Middle Cryptographic Attacks	random forest(RF), eXtreme gradient boosting(XGBoost), gradient boosting(GB) and decision tree(DT)
6	Effective way to defend the hypervisor attacks in cloud computing [39].	2017	Virtual Machine Attack	K-Means Clustering, Auto encoders
7	Detection and prevention of SQLI attacks and developing compressive framework using machine learning and hybrid techniques [40].	2022	SQL Injection Attack	Hybrid Approaches ANN, SVM, NB, DT and RF
8	Machine learning classification of port scanning and DDoS attacks: A comparative analysis [41].	2021	Port Scanning Attack	Support Vector Machine
9	Malware Detection Using Honeypot and Machine Learning [42]	2019	Malware Injection Attack	Support Vector Machine

Conclusion

This article explores many cloud attacks and showcases cloud services such as SaaS, PaaS, and IaaS. Although there are several security issues in cloud computing, we have listed some of them in this post, as well as strategies to address them. These strategies might be used to provide secure communication and alleviate security concerns. Client data in the cloud is critical and should be protected at all costs. Researchers employ a wide range of unique technologies and security methods to improve cloud security. Machine learning exposes a wide space for providing more precise and automatic protection against both known and unknown cloud attacks. The major purpose of this survey is to present a recent overview of machine learning-based cloud security research. In the future, we propose an intrusion detection system that uses upgraded and optimized machine learning methods to enhance cloud data security.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing", Communications of the ACM, vol. 53, no. 4, (2010),pp. 50–58.

[2] X. Sun, "Critical security issues in cloud computing: A survey", IEEE, (Nov. 29, 2018), pp. 1–6, doi: 10.1109/ICCCNT.2018.8494006.

[3] M. Saran, R. K. Yadav, and U. N. Tripathi, "Machine learning based security for cloud computing: A survey", International Journal of Applied Engineering Research, vol. 17, no. 4, (2022), pp. 332–337.

[4] O. Malomo, D. B. Rawat, and M. J. Garuba, "A survey on recent advances in cloud computing security", IEEE 2nd International Conference on Collaboration and Internet Computing, vol. 9, no. 1, (2018), pp. 32–48.

[5] L. Alhenaki, A. Alwatban, B. Alahmri, and N. Alarifi, "Security in cloud computing: A survey," International Journal of Computer Science and Information Security (IJCSIS), vol. 17, no. 11, (2019), pp. 68–71.

[6] K. Munir and S. Palaniappan, "Framework for secure cloud computing", International Journal on Cloud Computing: Services and Architecture, vol. 3, no. 2, (2013), pp. 21–35.

[7] S. Kumar and R. Goudar, "Cloud computing – research issues, challenges, architecture, platforms and applications: A survey", International Journal of Future Computer and Communication, (2012), pp. 356–360.

[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, (2011), pp. 1–11.

[9] S. Dogra and Sahil, "Cloud computing and its security concerns: A survey", International Journal of Innovative Technology and Exploring Engineering, vol. 3, no. 12, (2014), pp. 15–18.

[10] H. Hourani and M. Abdallah, "Cloud computing: legal and security issues," in Proceedings of the International Conference on Computer Science and Information Technology (CSIT), Helsinki, Finland, (2018) ,pp. 13–16.

[11] U. A. Butt, M. Mehmood, S. B. H. Shah, R. Amin, M. W. Shaukat, S. M. Raza, D. Y. Suh, and M. J. Piran, "A review of machine learning algorithms for cloud computing security", Licensee MDPI, Basel, Switzerland, vol. 9, no. 1, (2020), pp. 1–15.

[12] H. B. Patel and N. Kansara, "Cloud computing deployment models: A comparative study", International Journal of Innovative Research in Computer Science & Technology (IJIRCST), vol. 9,(2021), pp. 1–6.

[13] R. Garg, "MCDM-based parametric selection of cloud deployment models for an academic organization", IEEE, vol. 2168-7161, (2020), pp. 863–871.

[14] T. Diaby and B. B. Rad, "Cloud computing: A review of the concepts and deployment models", I.J. Information Technology and Computer Science, vol. 17, no. 3,(2017), pp. 50–58.

[15] N. Thakur, D. Bisen, V. Rohit, and N. Gupta, "Review on cloud computing: Issues, services and models", International Journal of Computer Applications, vol. 91, no. 9, (2014),pp. 1–7.

[16] G. Nenvani and H. Gupta, "A survey on attack detection on cloud using supervised learning techniques", IEEE Xplore, (2016).

[17] R. S. Theja and G. K. Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework", Journal of King Saud University – Computer and Information Science, vol. 34, no. 7, (2022), pp. 123–130.

[18] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 5, no. 6, (2011), pp.83–87.

[19] M. S. Dildar, N. Khan, J. B. Abdullah, and A. S. Khan, "Effective way to defend the hypervisor attacks in cloud computing" ,IEEE, (2017), pp. 1–5.

[20] M. Mushtaq, A. Akram, M. K. Bhatti, M. Chaudhry, M. Yousaf, U. Farooq, V. Lapotre, and G. Gogniat",Machine learning for security: The case of side-channel attack detection at run-time," in Proceedings of the IEEE International Conference on Electronics, Circuits and Systems (ICECS), (2019), pp. 1–6. DOI: 978-1-5386-9562-3/18.

[21] D. Rathee and S. Mann, "Detection of e-mail phishing attacks – using machine learning and deep learning", International Journal of Computer Applications, vol. 183, no. 47, (2022,), pp. 1–7.

[22] S. A. M. Al-Juboori, F. Hazzaa, Z. S. Jabbar, S. Salih, and H. M. Gheni, "Man-in-the-middle and denial of service attacks detection using machine learning algorithms", Bulletin of Electrical Engineering and Informatics, vol. 12, no. 1, (2023), pp. 418–426.

[23] J. Clarke, "SQL Injection Attacks and Defense", vol. 2, (2012), Waltham: Elsevier.

[24] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, and M. Zubair, "Machine learning classification of port scanning and DDoS attacks: A comparative analysis", Mehran University Research Journal of Engineering and Technology, vol. 40, no. 1, (2021), pp. 215–229.

[25] I. M. M. Matin and B. Rahardjo, "Malware detection using honeypot and machine learning", in Proceedings of the 7th International Conference on Cyber and IT Service Management(CITSM 2019), Kuala Lumpur, Malaysia,(2019).DOI: 10.1109/CITSM47753.2019.8965419.

[26] S. Sharma, G. Gupta, and P. R. Laxmi ," A survey on cloud security issues and techniques", International Journal on Computational Sciences & Applications (IJCSA), vol. 4, no. 1, (2014), pp. 1–10.

[27] B. P. Gajendra and V. K. Singh, " Achieving cloud security using third party auditor, MD5 and identity-based encryption", in Proceedings of the International Conference on Computing, Communication and Automation (ICCCA), IEEE ,(2016), pp. 1304–1309.

[28] K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm", Journal of Ambient Intelligence and Humanized Computing, (2019), pp. 1–10.

[29] P. Chouhan and R. Singh, "Security attacks on cloud computing with possible solution" ,International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 1,(2016), pp. 1–5.

[30] P. Rana, I. Batra, A. Malik, A. L. Imoize, Y. Kim, S. K. Pani, and S. Rho, "Intrusion detection systems in cloud computing paradigm: analysis and overview", Hindawi in the Complexity journal,(2022), pp. 1–10.

[31] I. A. Mohammed, "Cloud identity and access management – a model proposal", International Journal of Innovations in Engineering Research and Technology, vol. 6, no. 10, (2019), pp. 1–8.

[32] A. Singh and K. Chatterjee, "Cloud security issues and challenges: a survey", Journal of Network and Computer Applications, vol. 79, (2017) , pp. 88–115.

[33] B. Mukhopadhyay, R. Bose, and S. Roy, "A novel approach to load balancing and cloud computing security using SSL in IaaS environment", International Journal, vol. 9, no. 2, (2020), pp. 1–10.

[34] R. S. Theja and G. K. Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework",Journal of King Saud University – Computer and Information Science, vol. 34, no. 7, (2022), pp. 1–10.

[35] C. M. Nalayini and Dr. J. Katiravan, "Detection of DDoS attack using machine learning algorithms", Journal of Emerging Technologies and Innovative Research (JETIR), vol. 9, no. 7, (2022),pp. 1–10.

[36] M. Mushtaq, A. Akram, M. K. Bhatti, M. Chaudhry, M. Yousaf, U. Farooq, V. Lapotre, and G. Gogniat, "Machine learning for security: the case of side-channel attack detection at run-time", in IEEE International Conference on Electronics, Circuits and Systems (ICECS), (2019), pp. 1–6, doi: 978-1-5386-9562-3/18.

[37] D. Rathee and S. Mann, "Detection of e-mail phishing attacks – using machine learning and deep learning", International Journal of Computer Applications, vol. 183, no. 47,(2022), pp. 1–10.

[38] S. A. M. Al-Juboori, F. Hazzaa, Z. S. Jabbar, S. Salih, and H. M. Gheni, "Man-in-the-middle and denial of service attacks detection using machine learning algorithms", Bulletin of Electrical Engineering and Informatics, vol. 12, no. 1, (2023),pp. 418–426.

[39] M. S. Dildar, N. Khan, J. B. Abdullah, and A. S. Khan, "Effective way to defend the hypervisor attacks in cloud computing", IEEE, (2017), doi: 1-5090-5815-0.

[40] W. B. Demilie and F. G. Deriba, "Detection and prevention of SQLI attacks and developing compressive framework using machine learning and hybrid techniques", Journal of Big Data, (2022), pp. 1–10.

.

[41] I. M. M. Matin and B. Rahardjo, "Malware detection using honeypot and machine learning",in The 7th International Conference on Cyber and IT Service Management (CITSM 2019), Kuala Lumpur, (2019), pp. 1–10, doi: 10.1109/CITSM47753.2019.8965419.

[42] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, and M. Zubair, "Machine learning classification of port scanning and DDoS attacks: a comparative analysis," Mehran University Research Journal of Engineering and Technology, vol. 40, no. 1,(2021) pp. 215–229.