Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 11-19
Published by *Majmuah Enterprise*
www.majmuah.com

A Systematic Review of Hacking on Cloud Platform

MOHD SAFFUAN CHE MANSOR and MOHAMAD FADLI BIN ZOLKIPLI
School Of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok,Kedah, MALAYSIA
Email : mohdsaffuanchemansor@gmail.com, m.fadli.zolkipli@uum.edu.my | Tel: +60195706969, +60 17-724 7779

Received: February 19, 2023
Accepted: February 20, 2023
Online Published: March 01, 2023

Abstract

The popularity of cloud computing has increased in recent years due to its many benefits. However, the rise in cloud service usage has also made it a prime target for cyber criminals aiming to gain unauthorized access to sensitive information and disrupt operations. This research provides a comprehensive and detail review of cloud hacking and its impact on organizations and individuals. A systematic review approach was employed, which involved a comprehensive search of the relevant literature, including academic journals and conference proceedings. The study's findings present a thorough examination of the diverse methods, tools, and platforms employed by cyber criminals to hack into the cloud and suggest countermeasures that organizations can implement to safeguard themselves against such attacks. This study's findings have significant implications for cloud security and suggest recommendations for future research in this field.

Keywords: cloud hacking; cloud computing; cloud platform; cloud attack

1. Introduction

Cloud computing has experienced exponential growth in recent years, with an increasing number of organizations and individuals relying on its services for their computing needs. Its convenience and affordability have significantly impacted our daily lives (Tiwari et al., 2021) Cloud computing can provide an ideal solution for e-governance, which requires an unlimited supply of central processing power, data storage, and internet connectivity during procedures (Sharma, Singh, Upreti, Kumar, et al., 2021). It also provides convenient access to computing resources such as applications, storage, networks, servers, and other effective services (Choudhar y et al., 2020) (Sharma, Singh, Upreti, & Yadav, 2021). Despite the many benefits of cloud computing, its popularity has also made it a prime target for cyber criminals who are seeking to gain unauthorized access to sensitive information and disrupt operations. During the COVID-19 for example, attackers try to trick people into divulging sensitive information by exploiting their changed behaviour during this health crisis. These types of attack have seen an increase of over 200% since the start of pandemic (Mandal & Khan, 2020). The purpose of this research is to provide a comprehensive and up-to-date review of the state of cloud hacking and its impact on organizations and individuals.

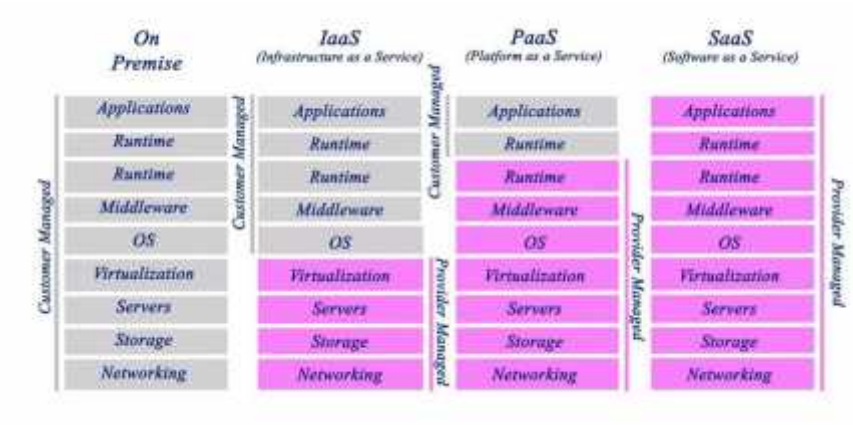

Figure 1 : Cloud Service Model (Tiwari et al., 2021)

The above Figure 1 illustrates the Cloud service models, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS enables clients to rent scalable and automated IT infrastructure from cloud service providers (CSPs) over the internet and provides on-demand access to physical and virtual servers,

storage, and networking resources (Vistro et al., 2020). PaaS enables software developers to utilize the necessary infrastructure to develop, operate, and oversee software applications, providing organizations the capability to deploy, run, and manage custom cloud applications without having to deal with the intricacies of building and maintaining servers and infrastructure (Tiwari et al., 2021). SaaS is a cloud computing where businesses provide access to cloud-based applications over the internet on a subscription basis where a third-party vendor and can be accessed from any location via an internet-connected device (Choudhar y et al., 2020).

The main objective of this research is to examine the various cloud hacking techniques, tools, and platforms that are currently being used by cyber criminals. This study will also explore the countermeasures that organizations can take to protect themselves from cloud hacking attacks. The scope of this study will focus on cloud hacking activities that have been reported in the literature and media, as well as practical case studies. This study will employ a systematic review approach, which will involve a comprehensive search of the relevant literature, including academic journals, conference proceedings, and online sources. The search will be conducted using a variety of keywords related to cloud hacking, and the resulting articles will be screened and selected based on their relevance to the study.

The rest of the paper is carried out as follows. Section 2 introduces literature review which is related to the hacking on cloud platform and the key findings from previous studies. Section 3 will summarize cloud hacking techniques and methods. Section 4 explores cloud security countermeasures. Section 6 concludes this article in the conclusion part and follows with acknowledgement and references.

2. Literature Review

2.1 Overview of the Research Topic

According to (Wang & Chen, 2020) the most common methods include phishing attacks, brute-force attacks, and exploiting vulnerabilities in cloud infrastructure. The study shows that various defence techniques used to protect cloud systems, such as multi-factor authentication, encryption, and security information and event management (SIEM) systems. This paper concluded that a comprehensive security approach, including both technical and non-technical measures, is necessary to effectively protect cloud systems from hacking. However, (Park et al., 2020) found and analysed 50 recent cloud hacking incidents that occurred between 2018 and 2020. Most of the incidents involved the theft of confidential data and were carried out by organized cybercrime groups. The most common method used by hackers to gain access to cloud systems was through phishing attacks. The study concluded that organizations need to adopt a multi-layered security approach and regularly update their security measures to effectively prevent cloud hacking incidents.

Besides that, a study by (Alsaadi et al., 2020) found that the security challenges in the cloud are data breaches and unauthorized access to sensitive information stored in the cloud. The lack of visibility into who has access to what data, making it difficult for administrators to monitor user activity. On top of that, poorly configured systems or applications which can lead to vulnerabilities being exploited by malicious actors. Besides that, insufficient authentication protocols such as weak passwords or lack of two factor authentication (2FA) and inadequate encryption techniques used on data at rest and/or in transit over networks makes it difficult to handle. On the other hands, (Saxena & Gayathri, 2021) discusses four types of attacks in relation to cloud computing including VM-level attacks, compliance issues, isolation failure and management interface compromise. Additionally, it also covers the risks associated with malicious scripts being uploaded to web applications as well as reflected XSS (Cross Site Scripting) threats.

2.2 Key Findings from Previous Research

From the journal found with the keywords of cloud computing, cloud platform, cloud hacking, cloud attack and cloud security, can be illustrate in Table 1 which provides a brief empirical review of the threats to cloud computing. Data breaches is one of the most threatening events in cloud computing. According to the study by (Aljumah & Ahanger, 2020), The data stored, processed, or shared in the cloud environment is often targeted for malicious attacks and is vulnerable due to human negligence or lack of knowledge, as well as vulnerabilities associated with cloud applications.

Additionally, data loss in cloud platform refers to the accidental or intentional deletion or corruption of stored data in the cloud environment (Butt et al., 2020). This can happen due to various reasons such as hardware failures, network outages, human error, security breaches, or other malicious activities. Data loss in the cloud can have a significant impact on an organization's operations, finances, and reputation, as well as on its customers' privacy and trust. In addition to data loss, insecure interfaces and application programme interfaces (APIs) refer to the channels used to access data and functionality in a cloud platform. They are vulnerable to exploitation by malicious actors if they are not secured properly. This can result in unauthorized access to sensitive data, manipulation of data, and exposure of

vulnerabilities (Sharma, Singh, Upreti, & Yadav, 2021). Besides that, account or service traffic hijacking Account or service traffic hijacking refers to unauthorized access and control over a legitimate user's online account or service traffic by a cyber attacker (Aljumah & Ahanger, 2020). This can be achieved through various methods, including phishing, password reuse, and exploiting vulnerabilities in the system or application. The attacker can then use the hijacked account to steal sensitive information, manipulate data, and carry out other malicious activities.

According to (Tabrizchi & Kuchaki Rafsanjani, 2020) denial of service (DoS) attack on a cloud platform occurs when an attacker intentionally floods the system with excessive traffic to prevent legitimate users from accessing it. The purpose of this attack is to interrupt the cloud service's regular operations by overloading its resources and rendering it incapable of handling incoming requests. Malicious insiders in cloud computing refers to individuals who have authorized access to a cloud computing environment malicious purpose, such as theft of sensitive data, unauthorized modification of data, or disruption of normal system operations. They can have separate roles such as employees, contractors, or third-party vendors, who are granted access to the cloud environment (Tabrizchi & Kuchaki Rafsanjani, 2020).

On top of that, abuse of cloud services refers to the unauthorized use of cloud computing resources, such as storage, processing power, or network bandwidth, for malicious purposes (Ahmad et al., 2021). This can include activities such as hosting illegal content, launching attacks on other systems, or using cloud services for cryptocurrency mining. Shared technology vulnerabilities or shared threats or shared security risk is vulnerabilities underlying infrastructure, operating systems, virtualization technologies, and other components that are shared by multiple tenants in a multi-tenant cloud environment (Choudhar y et al., 2020) (Ahmad et al., 2021). Attackers can exploit these vulnerabilities to gain unauthorized access to data and systems, disrupt services, or launch attacks on other tenants.

Virtualization attack in cloud platform refers to malicious activities aimed at exploiting vulnerabilities in virtualization technologies used in cloud computing (Verma & Adhikari, 2020). Some examples of virtualization attacks include hypervisor attacks, virtual machine escape, and virtual network spoofing (Sharma, Singh, Upreti, & Yadav, 2021). According to (Taleb & Mohamed, 2020), cloud malware injection refers to the act of introducing malicious software or code into a cloud computing environment. This can occur through various means, such as exploiting vulnerabilities in cloud systems, phishing attacks on cloud users, or exploiting misconfigurations in cloud infrastructure.

Table 1 : Brief Empirical Review of the Threats to Cloud Computing

Author Name and year	Aim Of Paper	Finding
(Aljumah & Ahanger, 2020)	The focus of this research is on examining security risks related to cloud computing, as well as discussing current methods for mitigating such threats in the cloud environment.	This study recommends the implementation of defence mechanisms like defence-in-depth to guard against malicious attacks. Additionally, organizations are advised to provide training programs for their employees to ensure they can securely and efficiently use cloud services.
(Butt et al., 2020)	The focus of this study was to examine the security threats and concerns associated with Cloud Computing (CC) and Edge Computing, and to propose solutions through the application of Machine Learning algorithms.	An overview of various ML algorithms, such as supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning, used to address security challenges in cloud computing is presented in this review.
(Sharma et al., 2021)	This study intends to develop a classification system of building components for Cloud Computing platforms, which can aid all stakeholders in the shared responsibility model in the deployment of applications using the SPI model.	This study highlights the importance of organizations implementing the SPI paradigm to have control over their usage of CSP resources before deploying any application.
(Tabrizchi & Kuchaki Rafsanjani, 2020)	This study examines the various components of cloud computing and the security and privacy	This study proposes potential solutions such as protecting data with methods like browser

	challenges that arise from these systems.	key translation method, to enhance data privacy in a multi-tenant environment.
(Ahmad et al., 2021)	This study examines major security concerns within each category, from a general artificial intelligence and deep learning perspective.	This study presents an extensive review of the architecture, services, configurations, and security models that enable IoT in a cloud-based environment.
(Alouffi et al., 2021)	The paper examines the security risks linked with cloud computing and explores potential solutions to mitigate these risks.	The paper's analysis of the selected literature shows that data tampering and leakage are frequently discussed topics. In addition, security risks related to data intrusion and storage in the cloud computing environment were also identified.
(Kaja et al., 2022)	The objective of this paper is to review earlier studies on data integrity concerns in cloud computing and examine potential data integrity attacks in the cloud environment, as well as the methods employed to identify and prevent them.	The paper identifies various data integrity concerns in cloud environments such as data breaches, theft, and unavailability. It further offers an in-depth examination of different data integrity attacks and the approaches used to mitigate them.
(Andi, 2022)	The purpose of this paper is to examine the recent developments in cloud security utilizing blockchain, deep learning, and cryptographic models.	The paper examines the latest developments in cloud security through blockchain, deep learning, and cryptographic models.
(Abdulsalam & Hedabou, 2021)	The purpose of this paper is to serve as a point of reference and provide a technical approach for researchers who want to explore the field of security and privacy for cloud computing.	The paper concludes that the current literature on cloud computing lacks flexible, technical solutions to address security threats.

3. Cloud Hacking Techniques and Methods

Cloud hacking refers to the unauthorized access, manipulation, theft, or disruption of data or resources stored in cloud computing systems. There are various techniques used by hackers to carry out cloud hacking according to the finding from the study.

Firstly, account or service traffic hijacking refers to the unauthorized access of a user's cloud computing account or service, with the aim of redirecting their traffic to a different destination (Mandal & Khan, 2020) that allows the attacker to gain access to sensitive information or take control of the user's cloud environment.

Secondly, insecure interfaces and application program interfaces (APIs) allow communication between the cloud and user (Sharma, Singh, Upreti, Kumar, et al., 2021). If these are not properly secured, attackers can exploit them to gain access to the cloud environment and steal sensitive information.

Thirdly, malicious insiders involve employees, contractors, or third-party service providers who have legitimate access to the cloud environment but intentionally cause harm by exploiting their access privileges (Chen et al., 2020).

Besides that, virtualization attacks occur when vulnerabilities in virtualization software are exploited by hackers to gain access to the underlying physical server and steal sensitive information. Multiple virtual machines can run on a single physical server (K. & Venkatesh, 2020). Other than that, hackers use cloud malware injection that involves the injection of malware into a cloud environment, allowing attackers to steal sensitive information or take control of the cloud environment (Kimmell et al., 2021).

Finally, denial of Service (DoS) attacks involves flooding a cloud environment with high levels of traffic to disrupt the availability of the services provided (Abdulsalam & Hedabou, 2021).

Cloud computing faces various challenges including reliability issues, misuse, malicious attacks, availability, vulnerabilities from shared technology, traffic hijacking, and data leakage, as revealed by the study. Ensuring privacy and security is crucial for cloud providers. In table 2, both the types of attacks and the corresponding solutions are listed.

Table 2 : Comparative Analysis of Cloud Computing Attacks, Consequences, Solutions (K. & Venkatesh, 2020)

No	Attacks	Consequences	Solutions
1	Maltreatment and Wicked Usage of Cloud Computing	Attackers use botnets to spread spam and malware and find pathways to transmit the malware to numerous PCs, often utilizing the power of the cloud infrastructure to assault other computers on the network.	Infrastructure based security, Access control and Identity management.
2	Malicious Attackers	The attacker's goal is to create malicious software that can infiltrate other machines and, regardless of consequences, the intruder takes advantage of the situation by causing financial disruption to the system.	Storage and Information security management. Also, the privacy management plays a significant role.
3	Usage of apprehensive Application Programming Interfaces	The cloud is frequently accessed by clients via APIs. Attackers attempt to analyse the encryption patterns of both the sender and receiver and capture the activities of the clients.	Authentication management, Access control and security management.
4	Vulnerabilities of Shared Technology	Intruders can attack various virtual machines and utilize their computing resources.	Defence-in-Depth technology and layers of virtualization.
5	Information Leakage or Loss	The attacker makes unauthorized attempts to delete the data before it can be backed up and tries to obtain the encrypted key.	Access Control, Encryption algorithms and Privacy management.
6	Privacy, Account and Traffic Skyjack	Denial of service attacks, man-in-the-middle attacks, and phishing attacks were observed.	Authentication mechanism, security policies for providers and proactive monitoring.
7	Unknown Profile	The aim of the attacker is to gain access to the security policies and code updates.	Infrastructure management and monitoring and alert management.
8	Provider Security Failure	The intruder attempts to gain control over the hardware and access stored data, as well as manipulate the application processes.	Authentication mechanism and Security management.
9	Other Client Attacks	When the communication between clients is disrupted, some clients may attempt to access other clients' information or disrupt their applications.	Privacy management and information security management.
10	Reliability and Availability Issues	The attacker impersonates a cloud provider and runs a hosted application to distribute false results.	Maintenance and Privacy mechanism.

11	Virtual Machine Attacks	The attackers can compromise the resources in a multi-tenant architecture and may attempt to manipulate the number of virtual machines (VMs).	Authorization and authentication mechanism.
12	Distributed Denial of Service Attacks	Botnets have infiltrated multiple virtual machines and use them to generate a large volume of packet traffic from various sources to a web server.	Data storage and backup.
13	Regulatory issues	The issues of authority and data export arise externally.	Security management.
14	Perimeter Security Attacks	The intruders attack the most critical application.	Security and Privacy Management.
15	Intrusion Attack in SaaS	The intruders monitor the custom application and obtain the system logs.	Host-Based and Network-Based Intrusion detection system
16	Intrusion Attack in PaaS	Like SaaS, the system is hosted on a centralized server, with a difference being.	
17	Intrusion Attack in IaaS	A critical issue in IaaS is transparency.	

Employee negligence is a frequent cause of internal attacks, such as sabotage and theft, unauthorized access, and unsafe practices, often resulting from weak cybersecurity measures. Data loss in the cloud is mainly due to human error and hardware or software failures during data migration (Kaja et al., 2022). The use of outdated software and services by employees and workers poses a risk of web browser bugs (Mandal & Khan, 2020). The vulnerability of cloud computing APIs to attacks can be attributed to the absence of encryption, unsecured endpoints, and inadequate authentication (Abdulsalam & Hedabou, 2021). The Migrant attack deceives cloud monitoring systems by using various resources to launch a denial-of-service attack on cloud virtual machine migration processes (Tabrizchi & Kuchaki Rafsanjani, 2020). Conducting insider risk profiling is crucial to comprehend and evaluate the frequency, severity, and potential mitigation strategies for insider threats (Tadapaneni, n.d.). The VM Rollback attack enables cyber attackers to run virtual machines from a prior snapshot without the user's knowledge or consent (Almutairy et al., 2019). An intrusion detection system can enhance network security and scalability by utilizing diverse algorithms to detect black hole attacks (Butt et al., 2020).

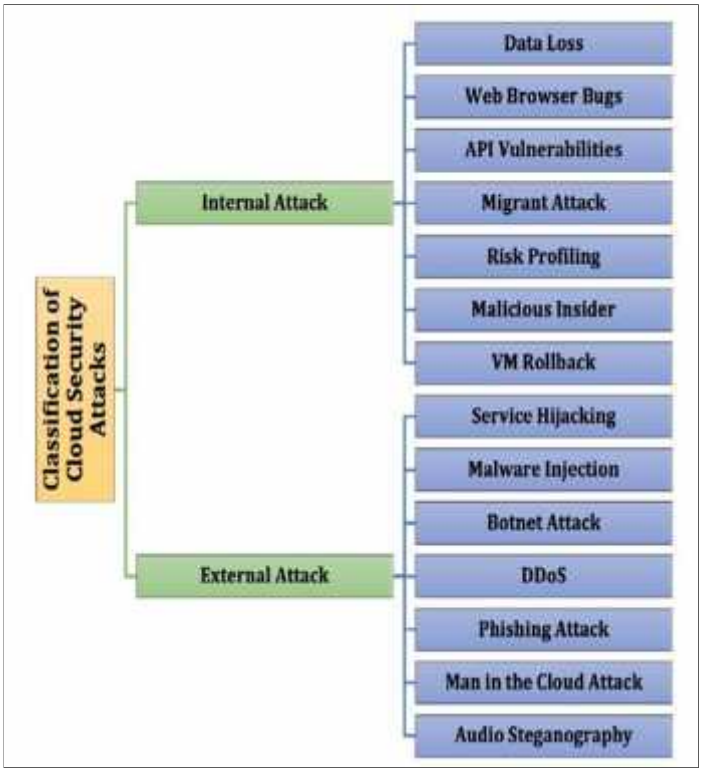

Figure 2 : Classification of Security Issues in Cloud (Reddy, 2022)

As shown in figure 2 above, cloud systems can be vulnerable to exploitation by outsiders or external who gain access using internet connections (Haq & Khan, 2021). Attacks from external sources on the cloud system can cause system failures that can adversely affect regular business operations and lead to significant financial losses for the company using the cloud (Atieh, 2021). Unauthorized system access via the cloud increases the risk of cloud computing services being hijacked (Alouffi et al., 2021). An organization's online system is further exposed to external threats in the form of malware introduced into cloud computing (Haq & Khan, 2021) (K. & Venkatesh, 2020). A dangerous type of attack is when an authorized user is tricked into providing valuable information, such as credentials and personal data, by a fake application that resembles the real one (Basit et al., 2020)."

4. Cloud Security Countermeasures

Cloud security countermeasures are measures taken to protect cloud computing systems from potential security threats and vulnerabilities. These measures include implementing strong authentication methods and access control mechanisms to restrict unauthorized access to cloud resources. Encrypting sensitive data both in transit and at rest to protect against data theft and unauthorized access. Monitoring cloud systems for unusual activity, as well as logging all access to the cloud to detect and respond to security incidents. Securing virtualization environments and virtual machines from security threats. Disaster Recovery and Business Continuity Planning: Planning and implementing measures to ensure that critical systems and data can be quickly restored in the event of a security breach or other disaster. Assessing and managing the risk of cloud adoption and implementing appropriate measures to mitigate those risks. Regularly assessing the security posture of cloud systems to identify and remediate vulnerabilities. Ensuring that cloud systems are compliant with relevant security standards and regulations. By implementing these countermeasures, organizations can reduce the risk of security breaches in the cloud and ensure that their data and systems are protected.

5. Conclusions

To sum up, the growing dependence on cloud platforms has resulted in a rise in hacking attacks on them. According to systematic reviews of these attacks, a range of threats such as insecure interfaces and APIs, account and service traffic hijacking, denial-of-service attacks, malicious insiders, abuse of cloud services, shared technology vulnerabilities, virtualization attacks, and cloud malware injections present significant risks to organizations that use cloud platforms. The need to protect sensitive data and prevent unauthorized access to systems and networks has become more critical

than ever. As a result, it is important for organizations to implement strong security measures and stay up to date with the latest security practices to mitigate the risks associated with hacking on cloud platforms.

In conclusion, hacking on cloud platforms is a growing concern and requires ongoing research and collaboration between cloud service providers and security experts to develop effective solutions to this problem. One of the best ways is by developing and implementing more advanced and sophisticated security measures that can prevent and detect hacking attacks. Besides that, further research is needed to identify the most common types of hacking attacks in cloud platforms and the techniques used by hackers to carry out these attacks. Collaboration between cloud service providers and security experts: Encouraging cooperation between cloud service providers and security experts to address the security challenges in cloud platforms. On top of that, raising awareness among users: Educating cloud users about the risks associated with cloud platforms and the importance of taking proactive measures to protect their data and systems. Finally, development of new technologies: Developing and deploying new technologies, such as machine learning, to detect and prevent hacking attacks in cloud platforms.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

References

Abdulsalam, Y. S., & Hedabou, M. (2021a). Security and Privacy in Cloud Computing: Technical Review. Future Internet, 14(1), 11. https://doi.org/10.3390/fi14010011

Abdulsalam, Y. S., & Hedabou, M. (2021b). Security and Privacy in Cloud Computing: Technical Review. Future Internet, 14(1), 11. https://doi.org/10.3390/fi14010011

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics, 11(1), 16. https://doi.org/10.3390/electronics11010016

Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications, 14(7), 1185–1191. https://doi.org/10.1049/iet-com.2019.0040

Almutairy, N. M., Department of Computer Science, Qassim University, Saudi Arabia;, Al-Shqeerat, K. H. A., Department of Computer Science, Qassim University, Saudi Arabia;, Al Hamad, H. A., & Department of Computer Science, Amman Arab University, Jordan; (2019). A Taxonomy of Virtualization Security Issues in Cloud Computing Environments. Indian Journal of Science and Technology, 12(3), 1–19. https://doi.org/10.17485/ijst/2019/v12i3/139557

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. IEEE Access, 9, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

Alsaadi, E. M. T. A., Fayadh, S. M., & Alabaichi, A. (2020). A review on security challenges and approaches in the cloud computing. 040022. https://doi.org/10.1063/5.0027460

Andi, H. K. (2022). Estimating the Role of Blockchain, Deep Learning and Cryptography algorithms in Cloud Security. Journal of Trends in Computer Science and Smart Technology, 3(4), 305–313. https://doi.org/10.36548/jtcsst.2021.4.006

Atieh, A. T. (2021). The Next Generation Cloud technologies: A Review On Distributed Page | 1 Cloud, Fog And Edge Computing and Their Opportunities and Challenges. ResearchBerg Review of Science and Technology, 1(1), 1–15.

Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, Md. J. (2020). A Review of Machine Learning Algorithms for Cloud Computing Security. Electronics, 9(9), 1379. https://doi.org/10.3390/electronics9091379

Chen, L., Xian, M., Liu, J., & Wang, H. (2020). Research on Virtualization Security in Cloud Computing. IOP Conference Series: Materials Science and Engineering, 806(1), 012027. https://doi.org/10.1088/1757-899X/806/1/012027

Choudhar y, S., Pundir, G. ima, & Singh, Y. (2020). Detection and Isolation of Zombie Attack under Cloud Computing. Inter National Resear Ch Jour Nal of Engineer Ing and Technology (IRJET), 07(01), 1419–1424.

Haq, I. U., & Khan, T. A. (2021). Penetration Frameworks and Development Issues in Secure Mobile Application Development: A Systematic Literature Review. IEEE Access, 9, 87806–87825. https://doi.org/10.1109/ACCESS.2021.3088229

K., N., & Venkatesh, R. (2020). A Survey of Cloud Computing Security Issues and Consequences. Asian Journal of Applied Science and Technology, 04(03), 01–09. https://doi.org/10.38177/ajast.2020.4301

Kaja, D. V. S., Fatima, Y., & Mailewa, A. B. (2022). Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques. International Journal of Research Publication and Reviews, 713–720. https://doi.org/10.55248/gengpi.2022.3.2.8

Kimmell, J. C., Abdelsalam, M., & Gupta, M. (2021). Analyzing Machine Learning Approaches for Online Malware Detection in Cloud. http://arxiv.org/abs/2105.09268

Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. 2020 International Conference on Smart Electronics and Communication (ICOSEC), 837–842. https://doi.org/10.1109/ICOSEC49089.2020.9215374

Park, J., Lee, K., Kim, J., & Choi, Y. (2020). Cloud Hacking Incidents: A Review of Recent Cases. Journal of Computer Security, 19(3), 250–256.

Reddy, B. (2022). *A Study of Security Threats and Attacks in Cloud Computing*.

Saxena, R., & Gayathri, E. (2021). A study on vulnerable risks in security of cloud computing and proposal of its remedies. Journal of Physics: Conference Series, 2040(1), 012008. https://doi.org/10.1088/1742-6596/2040/1/012008

Sharma, A., Singh, U. K., Upreti, K., Kumar, N., & Singh, S. K. (2021). A Comparative analysis of security issues & vulnerabilities of leading Cloud Service Providers and in-house University Cloud platform for hosting E-Educational applications. 2021 IEEE Mysore Sub Section International Conference (MysuruCon), 552–560. https://doi.org/10.1109/MysuruCon52639.2021.9641545

Sharma, A., Singh, U. K., Upreti, K., & Yadav, D. S. (2021). An investigation of security risk & taxonomy of Cloud Computing environment. 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 1056–1063. https://doi.org/10.1109/ICOSEC51865.2021.9591954

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. The Journal of Supercomputing, 76(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

Tadapaneni, N. R. (n.d.). CLOUD COMPUTING SECURITY CHALLENGES. Novateur Publications International Journal of Innovations In Engineering Research And Technology, 7(6).

Taleb, N., & Mohamed, E. A. (2020). Cloud Computing Trends: A Literature Review. Academic Journal of Interdisciplinary Studies, 9(1), 91. https://doi.org/10.36941/ajis-2020-0008

Tiwari, A., Patel, Prof. J., & Sharma, Dr. P. (2021). Vulnerability Assessment and Penetration Testing Approach Towards Cloud-Based Application and Related Services. International Journal of Scientific Research in Science, Engineering and Technology, 395–403. https://doi.org/10.32628/IJSRSET218346

Verma, G., & Adhikari, S. (2020). Cloud Computing Security Issues: A Stakeholder's Perspective. SN Computer Science, 1(6), 329. https://doi.org/10.1007/s42979-020-00353-2

Vistro, D. M., Rehman, A. U., Mehmood, S., Idrees, M., & Munawar, A. (2020). A LITERATURE REVIEW ON SECURITY ISSUES IN CLOUD COMPUTING: OPPORTUNITIES AND CHALLENGES. JOURNAL OF CRITICAL REVIEWS, 7(10).

Wang, Y., & Chen, X. (2020). A Review of Cloud Hacking Methods and Defense Techniques. A Review of Cloud Hacking Methods and Defense Techniques, 153–159.