Vol.2, No.4, Page 381- 390, 2024 https://doi.org/10.59628/jast.v2i4.1025 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

Survey on Cloud Computing Security

Fatima Ismail AL-Hadi[1] *, Nagi Ali AL-Shaibany[1] and Sharaf Abdulhak AL-Homdyl[1]

[1]**Department of Information Technology, Faculty of Computer Science and IT, University of Sana'a, Sana'a, Yemen.**

*Corresponding author: fatima2017@su.edu.ye

Abstract

One of the most popular IT subfields today is cloud computing. With a simple Internet connection, it enables users to access cutting-edge information, technology, and infrastructure. Because of the numerous benefits offered, most international organizations have started to move toward cloud computing environments during the last few decades. Companies and organizations find cloud computing appealing because it eliminates the need to plan for provisioning and enables them to start with modest resources and progressively raise them as service demand increases. Cloud computing presents opportunities for research as well as obstacles. The security and privacy of data in cloud systems are important issues. Now that cloud computing technology is developing quickly, it is more convenient for businesses to move their workload there. It asks for a smaller investment and guarantees quick delivery of cutting-edge technologies. Cloud security is of the utmost importance. It is susceptible to cyberattacks that exploit its vulnerabilities in an insecure cloud environment. This puts the cloud environment's assets, resources, and data in danger. In this paper, we reviewed some cloud computing studies about various attacks on cloud computing services. This paper's main objective is to give readers a better understanding of security issues and solutions.

Article Info

Keywords:
Cloud Computing, Attacks, Security, Models, IDS, CIDS.

Article History:
Received: 8-June-2024,
Revised: 16-July-2024,
Accepted: 18-August-2024,
Available online: 30 August 2024.

1. INTRODUCTION

In the IT sector, cloud computing is becoming more and more significant. With its on-demand access to shared computing resources like servers, storage, and apps, it is advantageous for a range of computing tasks and business support [1]. Currently recognized as private, public, hybrid, and multi-cloud cloud computing are the four primary categories [2]. In essence, cloud storage is a platform that allows users to share and store data online. Cloud storage has many advantages, such as inexpensive usage, simple, secure, and efficient file accessibility, limitless data storage capacity, and remote backup [3]. Based on the real-world uses of cloud storage, five categories can be identified: Cloud storage options: shared, private, hybrid, individual, and public [3]. Notwithstanding its advantages, cloud computing presents serious security risks. Data security, or assuring the confidentiality, integrity, and availability (CIA) of information, is the main worry. Furthermore, network security is essential for preventing cyberattacks on the cloud infrastructure [4], security issues are brought up by cloud computing, despite its accessibility and flexibility. Data breaches, leaks, and unauthorized access pose serious risks across multiple cloud layers due to the ease of accessing resources from any location. By utilizing a variety of data encryption methods, strict access controls, and key management, cloud computing offers great security [5]. The security is low in a public cloud, high in a private cloud, and moderate in a Hybrid Cloud [5]. Public clouds are regarded as being less secure since it is more challenging to protect data from hostile attacks [6]. Private clouds are those that the owner or a third party manages. The security levels can be changed in this way to suit the requirements of the business. The hybrid cloud is a conglomeration of various models. Unfortunately, all of the security flaws in the other cloud models are carried over to this one. The community cloud is

Table 1. Comparison of this study to other surveys

Work	Cloud Overview	Security Issues	Security Attacks	SOLUTIONS FOR CLOUD COMPUTING SECURITY
[12]	✓	×	✓	×
[13]	×	×	×	✓
[14]	✓	×	✓	✓
[15]	1	✓	×	×
[16]	✓	✓	×	✓
[1]	✓	✓	✓	×
[7]	✓	✓	✓	✓
[17]	✓	✓	✓	✓
This Survey	✓	✓	✓	✓

one that numerous organizations implement while splitting configuration responsibilities. This may result in the improper management, mitigation, and application of security protocols [6].

Numerous threats, including DoS and DDoS, can compromise cloud security. Defensive strategies require robust intrusion detection systems (IDS). Although AI and ML can greatly enhance IDPS detection and prevention, traditional security measures remain insufficient to counter sophisticated attacks. Nevertheless, effective data mining and intrusion detection necessitate a thorough evaluation of the advantages and disadvantages of AI. [7].

2. RELATED WORKS

There are various studies in the literature discussing the security issues and security attacks of cloud computing. The authors in [8] have addressed the security vulnerabilities with cloud computing and some of the subsequent proposed models to address them in this study, in [9] they have talked about a few cloud computing-related problems and difficulties, provided a comprehensive analysis of data protection, security, and cloud-related challenges and specified the literature review on cloud computing problems and risks, and it also discusses several security difficulties, in [10] looked into pertinent research and surveys on dangers and outlooks and provided an overview of nature-inspired algorithms, their uses, and their value, focusing on issues with cloud computing, in [11] the main objective of the authors are to identify important security risks and concerns that must be taken into account during the sending and development of cloud administrations, as well as the best course of action for reducing those risks and issues. Table 1 provides a comparison between this survey and other surveys. The symbols "✓" and "x" indicate whether or not the domain listed in the column has been discussed in the poll.

3. CLOUD COMPUTING DEPLOYMENT MODELS

Cloud deployment models are the processes that make cloud services available to users. The four deployment models linked to cloud computing are as follows:

3.1. Public Cloud

Computer resources, such as software and hardware, can be shared via public clouds. Applications like file sharing and email, as well as testing and development, frequently use them. The resources are located at the provider's facility, and users pay for each use or occasionally use them for free [18].

3.2. Private Cloud

Even if they are run by a third party, private clouds are exclusive to a single company. Sensitive data is protected by strong security and control thanks to this [19].

3.3. Hybrid Cloud

Hybrid clouds provide flexibility and scalability by combining private and public cloud environments. Applications can migrate between these environments, giving businesses greater control over sensitive information while utilizing public clouds' affordability and scalability. Approximately 58% of multinational corporations employ hybrid cloud models, frequently under the supervision of a single client [14].

3.4. Community Cloud

This sort of cloud is jointly built by many organizations, and it shares the same cloud architecture along with the same requirements, values, and concerns. The cloud community influences the equilibrium between democratic and economic stability [9]. The four cloud computing deployment options are compared in Table 2 in terms of some parameters.

Table 2. Comparison among Public, Private, Hybrid, and Community Clouds [5, 18]

Parameter/Type	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Scalability	Very High	Limited	Very High	Limited
Reliability	Moderate	Very High	Medium to High	Very High
Security	Depending entirely on the service provider	High-class security	Secure	Secure
Performance	Low to medium	Good	Good	Very Good
Cost	Cheaper	High Cost	Costly	Costly
Examples	Amazon EC2, Google AppEngine	VMWare, Microsoft, KVM, Xen	IBM, HP, VMWare vCloud, Eucalyptus	Solas Community Cloud, VMWare

Table 3. cloud computing models security [20]

Cloud model	Security Implication	Security Disadvantages
Scalability	Very High	Limited
Public Cloud	Despite possible security issues, your data is currently safeguarded by a strong firewall and the knowledge of service provider's personnel. You can be sure that your data is secure.	Public cloud security depends on regulations and provider security and is risky because of global access and shared resources.
Private Cloud	The private cloud offers high security as the organization controls the servers and access, with data behind the firewall and a custom architecture.	Due to labor-intensive maintenance and specialized staff, private cloud security is costly. Consequently, when selecting this strategy, cost and possible return on investment are crucial considerations.
Hybrid Cloud	Because it concentrates on particular threats, targeted security is both efficient and economical.	Hybrid cloud security is difficult to manage and detect possible threats because of its complexity.
Community Cloud	Draws financial institutions with improved security and shared security responsibility, as well as high data availability.	In every security breach, you yourself.

4. CLOUD COMPUTING DEPLOYMENT MODELS SECURITY

Each of these four deployment and provisioning models has different effects on security. In Table 3, all of these models are briefly examined along with their security concerns.

5. CLOUD COMPUTING SERVICES

The three primary models available in cloud computing are IaaS (infrastructure), PaaS (platform), and SaaS (software). Each offers particular services and means of access [21].

5.1. Infrastructure as a service (IaaS)

IaaS stands for Infrastructure as a Service. It provides on-demand access to servers, networking, and storage, among other cloud computing resources. Amazon Web Services is a well-known IaaS provider (AWS) [22]. The user faces mostly data storage-related security issues at this level [15].

5.2. Platform as a Service (PaaS)

Platform as a Service, or PaaS, offers a cloud-based environment for application development and deployment without requiring infrastructure management. Developers can concentrate on creating their applications since the provider handles everything. Well-known PaaS examples are AWS Elastic Beanstalk and Google App Engine [22]. PaaS security is centered on three main areas: service resilience and uptime, secure authentication, and platform vulnerabilities [7]. Users with this degree of security are in danger when accessing various software platforms [15].

5.3. Software as a Service (SaaS)

Users can download apps via the Internet using a subscription-based model from SaaS (Software as a Service). The administration process and user experience are streamlined by doing away with the requirement for local software installations and updates [22]. "Security issues in the SaaS are authentication, approval, data privacy, availability, and network security"[7]. The user

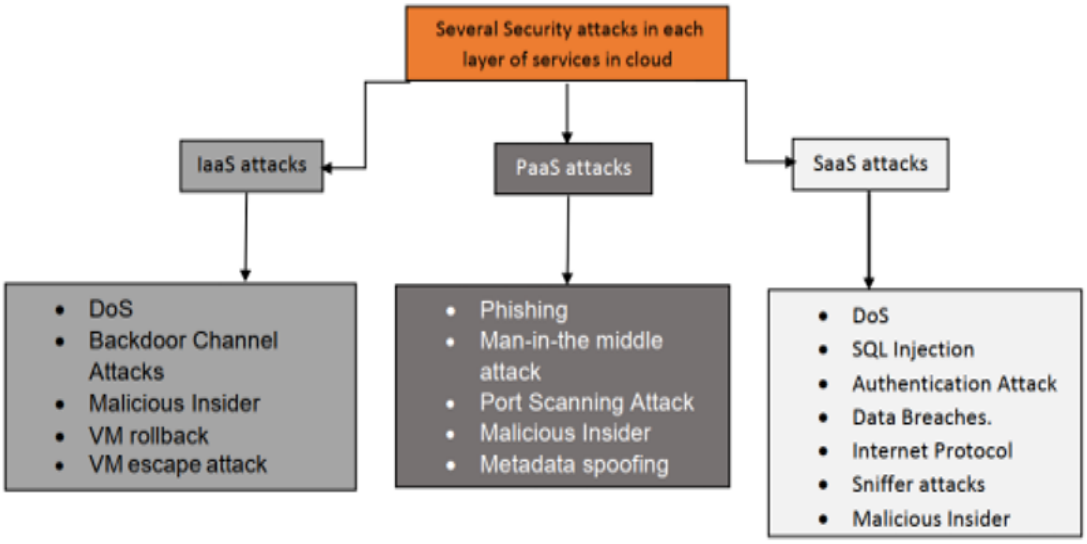

Figure 1. Security Attacks on Cloud Services

faces mostly data storage-related security issues at this level [15]

6. CLOUD COMPUTING SERVICES ATTACKS

Figure 1 and Table 4 list and describe various security attacks on cloud computing services, along with prevention guidelines.

7. EMERGING THREATS

Cloud environments face risks from new threats and vulnerabilities, requiring proactive security measures. Research highlights dangers such as social engineering, insider threats, and targeted attacks on sensitive data [23]. Security challenges in cloud computing are exacerbated by dynamic cyber threats such as malware, phishing, man-in-the-middle attacks, and SQL injections. An essential security strategy is needed to address differences in security abilities among providers in multi-cloud environments, which offer new opportunities for attacks and vulnerabilities [23, 24]. By tackling these emerging threats and less common vulnerabilities with comprehensive risk analysis, prioritized mitigations, and adaptive security strategies, organizations can strengthen their resilience against evolving cyber threats in cloud environments.

8. DATA SECURITY IN CLOUD STORAGE REQUIREMENTS

Although cloud storage provides data access services, it also presents security and privacy issues. Crucial prerequisites consist of [3]:

- Privacy: Data is only accessible to those who are authorized.
- Integrity: Information is reliable and unaltered
- Availability: Data is always available for users to view and edit.
- Fine-grained access control: Exact management of who has access to what.
- Secure data sharing preserves privacy by only sharing information with authorized groups.
- Users have the option to completely delete their data from the cloud.
- Protecting user data from unwanted access is known as privacy protection.

9. TYPES OF CLOUD COMPUTING SECURITY [25, 26]

Five main categories can be used to categorize cloud security:

9.1. Identity security

Complete security, with a focus on user and cloud provider authentication. It is described as a privacy and professional methodology that enables authenticated persons to access resources at the proper time and for the right goals. It improves access to certified users while maintaining the privacy and security of data and apps.

9.2. Infrastructure security

Protect all of the cloud's hardware, including the switches, routers, networks, devices, and data. Companies must confirm their security before doing business. Component isolation is also essential to preventing unrestricted access to sensitive resources.

Table 4. Attacks in Each Service Model [13–15, 17]

Sr.NO	Attack	Description	Prevention
1	DoS	DoS attacks flood the cloud service with bogus requests, consuming the bandwidth and preventing can identify them early and respond effectively. IaaS and SaaS services.	DoS attacks flood the cloud service plan. With real-time traffic monitoring, your team can identify them early and respond effectively.
2	SQL Injection	SQL injection in SaaS lets attackers steal sensitive data.	An organization's response to disruptions that affect project processes is outlined in a business continuity plan.
3	Authentication Attack	By attempting every possible password in an attempt to obtain unauthorized access, SaaS authentication attacks jeopardize authentication attacks jeopardize	Use strong encryption, and change passwords from time to time.
4	Data Breaches	The increased risk of personal data exposure, the loss of encryption keys, shared vulnerabilities, and the necessity of regular backups make cloud data breaches a serious concern. SaaS attack.	For optimal cloud security, data encryption and utilizing a CASB for user alerting, auditing, and monitoring are crucial. .
4	Authentication Attack	By attempting every possible password in an attempt to obtain unauthorized access, SaaS authentication attacks jeopardize data security and integrity.	For optimal cloud security, data encryption and utilizing a CASB for user alerting, auditing, and monitoring are crucial.
5	Internet Protocol	SaaS attacks involve IP flaws like IP spoofing and ARP, which let hackers pretend to be trustworthy devices and possibly steal data	Multi-tenancy cloud providers safely share resources such as orchestration, monitoring, and hypervisors.
6	Phishing	Phishing is a tactic used to trick users into clicking links, which gives attackers posing as reliable sources control over the system, a PaaS attack.	Use a secure web address.
7	Sniffer attacks	Attackers can eavesdrop on network	VPN secures traffic by encrypting all incoming and

		traffic by intercepting unencrypted data through sniffing attacks. Sniffer could be a script, application, service, or SaaS attack.	outgoing data.
8	Backdoor Channel Attacks	Hypervisor attacks in IaaS compromise data fundamentally affecting every virtual machine.	A firewall and antivirus program for double security.
9	Man-in-the middle attack	PaaS assault, A man-in-the-middle attack eavesdrops on communication, giving the impression that parties are speaking with one another when it's the attacker. attacker.	Stronger internal security & thorough employee/contractor checks prevent MITM attacks.
10	Port Scanning Attack	Attackers utilize application scanning attacks to take advantage of holes in the system, PaaS attacks.	Use firewalls and TCP wrappers for network security and access control for improved cloud security.
11	Malicious Insider	The potential for wide-ranging access and covert tracking makes cloud insiders a serious threat. In particular, when users give up key control, system security largely depends on the provider. Insiders can access critical systems and data with unprecedented ease across all service models.	Organizations should concentrate on holistic analysis that integrates data correlation, application monitoring, and threat prioritization to detect insider threats in the cloud.
12	VM rollback	Via an outdated snapshot, an attacker can gain access to a different user's virtual machine (VM) and potentially change user permissions. This is known as a VM rollback attack (Iaas).	Suspend and restart use.
13	Metadata spoofing attack	Someone attempted to use another user's IP address without that person's consent. PaaS attack.	Secure API: Encrypted information, strong authentication.
14	VM escape attack	Harmful software that could affect the hypervisor or other guest virtual . machines	Isolate virtual machines (VMs), use a secure.

9.3. Information security

Systems for processing and storing data should only be accessible to authorized personnel, and verify that third-party suppliers have robust security protocols and unambiguous data handling agreements.

9.4. Network Security

By defending the infrastructure against intrusions and attacks, network security ensures the safety of devices and services. It is essential for web systems, to avoid latency and performance problems.

9.5. Software Security

From design to implementation, security considerations must be integrated into every step of the software development process to ensure security. Regardless of project complexity, each step depends on the others to provide the best protection.

10. CLOUD SECURITY ISSUES

The section focuses on security problems and solutions. It discusses security concerns in cloud computing and their responses. Security issues affect assets through various means. Cloud-specific and universal issues differ greatly. NIST-defined characteristics of distributed computing contribute to cloud-related problems. The cloud environment poses challenges for implementing security measures. [27].

10.1. Data storage and computing security issues

In cloud computing, data is extremely important. Lack of knowledge of cloud location and security procedures by the client. One problem with remote storage is the lack of client awareness. Distributed storage requires reliable management. Client data is kept on cloud server farms. Affordable distributed storage is provided by several providers. To maximize cloud space utilization, data is shared widely and kept in several locations. Excellent data accessibility is ensured by backup servers. Cryptographic methods are used to secure cloud data. Encryption key implementation is necessary for security. Estimating plain content data is not feasible. It is crucial to apply cryptography precisely.

10.2. Virtualization security issues

The sector is adopting virtualized cloud computing. Virtual machines are something that cloud providers need to have faith in. In cloud management, virtualization is essential. Virtualization and having several tenants increase profit, but there are drawbacks. To gain access to services, many attackers use coordinated attacks. In search of virtually and legally acceptable segregation, people search this area.

10.3. Security concerns relating to the Internet and services

Widespread adoption is made possible by virtualized cloud computing. In cloud infrastructure, data transfer requires a transporter. Digital data packets are sent from source to destination over the Internet. Data that travels via several hubs is insecure. New dangers arise from Web 2.0-related problems such as malware injections and MitM attacks. Cloud services are Internet-accessible and present security risks to end users. Many people believe that exchanging information online is unsafe, even with security precautions in place.

10.4. Difficulties with Network Security

The network is a major component of cloud computing, so network issues could have a ripple effect on the entire system. In addition to network congestion, data transfer delays, and even problems with administration access, these problems can be internal, external, or even the result of malevolent users.

10.5. Issues with Trust Management

In cloud computing, trust is essential for the resources used, such as processing power and storage, as well as between the client and the provider. However, trust can be hard to maintain for a variety of reasons.

11. SOLUTIONS FOR CLOUD COMPUTING SECURITY

Increased security risks accompany cloud scalability and flexibility. This section addresses current and future cybersecurity strategies for safeguarding cloud-based systems [28].

11.1. INTRUSION DETECTION IN CLOUD SYSTEMS

Vulnerabilities grow when more systems are moved to the cloud. Permissions, whitelisting, multi-factor authentication (MFA), patching, firewalls, and intrusion detection systems (IDS) are critical security techniques for safeguarding cloud environments [28].

11.2. COLLABORATIVE IDS IN CLOUD SYSTEMS

The goal of Collaborative Intrusion Detection Systems(CIDS) is to increase overall network security by

combining several separate Intrusion Detection Systems (IDSs). CIDS can identify sophisticated threats like DDoS and zero-day attacks that could elude a single IDS by exchanging attack data.

11.3. Firewalls

Data is safeguarded by cloud firewalls (through ACLs) that filter network traffic and limit app access [16].

11.4. Staff Training

To raise the general level of information security, ongoing security training on technical proficiency must be offered [20].

11.5. Data Encryption

Securing sensitive data in the cloud is advised using data protection techniques like encryption, passwords, firewalls, and data storage. Without the encryption key, encrypted data is unusable since it cannot be accessed. Data encryption is the process of utilizing secret keys to transform data into a secret code. Decrypting the data requires an encryption key [29].

11.6. Identity and Access Management (IAM)

In a cloud environment, IAM guarantees authorized access to resources. Effective passwords with expiration dates are essential to identity management. Authentication uses multi-factor authentication or biometrics to confirm the identity of users. Authenticated users are granted access to resources through authorization. IAM preserves cloud security and protects data [14].

12. TAILORING CLOUD STRATEGIES FOR INDUSTRIES

Strategies for effectively managing various cloud deployment models, including public, private, and hybrid, can be tailored to meet specific industry requirements, thereby enhancing their effectiveness [30, 31]. For instance, sectors dealing with confidential information may perceive the private cloud paradigm as beneficial owing to its enhanced security and governance attributes [30]. In contrast, sectors that require scalability and flexibility in computing resources might benefit from a hybrid cloud approach, which combines both public and private cloud services [31]. While beneficial, strategies may have limited applicability in regulated industries such as healthcare or finance due to strict compliance requirements that can restrict the use of specific cloud models or configurations [30]. Therefore, it is crucial for organizations to carefully assess their industry-specific needs and regulatory constraints when implementing cloud strategies to ensure compliance and optimal performance.

13. APPROACHES FOR ENHANCING SECURITY IN CLOUD ENVIRONMENTS

Numerous proposals have been made to improve security in cloud environments through case studies and models. The Artificial Intelligence-Based Architecture (AIBA) model utilizes artificial intelligence to identify, stop, and reduce security risks in cloud systems [32]. The Optimal Risk Access Control Model (ORACM) is an approach that validates risk decisions in cloud computing by considering environment, resource, and subject attributes [33]. The HHODL-IDA utilizes machine learning and anomaly detection to detect security attacks in cloud environments proactively [34]. The models focus on real-time monitoring, adaptive responses, and automated intrusion detection to enhance cloud security. They aim to protect sensitive data and services from cyber threats [35, 36].

14. END-USER CLOUD SECURITY

End-users are vital in cloud security as they must trust service providers with their data, despite limited control over security measures [37]. User-centric approaches enable users to manage their security and privacy in untrusted cloud and IoT environments [37]. Encryption, biometric authentication, and MAC address security are crucial for protecting user data in cloud storage. These solutions help prevent unauthorized access and breaches [38]. Furthermore, involving end-users in IoT device programming can help manage security risks by expanding rules to include security aspects and assisting users in creating custom security rules [39].

15. RECOMMENDATIONS FOR CLOUD

The significance of appropriate device security and control mechanisms for efficient access management. To prevent data breaches, user awareness is essential and calls for funding for workshops, safety training, and information security courses. Because data is stored on several servers, including cloud servers, regular backups are imperative. Even if security measures are unsuccessful, encryption must be used to prevent unwanted access to data.

16. RESULTS

Since the cloud is susceptible to hacking, the services it provides to individuals and businesses are what makes it so important. To stop hackers from causing harm, cloud computing security must be increased. The goal of cloud computing security research is to identify countermeasures for cloud attack threats. Numerous cloud computing security issues and solutions were covered.

The private cloud is the most secure, while the public cloud is the least secure. Community clouds and hybrid clouds have a medium level of security. A few assaults focus on certain service layers, with software-as-a-service (SaaS) being the most susceptible because of popular apps like Gmail.

17. CONCLUSION

With the majority of multinational corporations switching to cloud-based systems, cloud computing has become omnipresent in the modern world. To reduce the organization's vulnerabilities to cyber assaults, which can result in the loss of data and property and a significant financial cost in damage, such a system must be as reliable and safe as feasible. The most common security vulnerabilities that a cloud computing system encounters were discussed in this study, along with remedies to minimize those threats and limit assaults and financial losses.

REFERENCES

[1] S. Swain and R. K. Tiwari, "Cloud security research-a comprehensive survey," *Int. J. Electron. Eng. Appl.*, vol. 8, no. 2, pp. 29–39, 2020.

[2] S. Shakya, "A perspective review of security issues in iot with cloud environment," *J. IoT Social, Mobile, Anal. Cloud*, vol. 4, no. 2, pp. 84–93, 2022.

[3] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," *Ieee Access*, vol. 8, pp. 131 723–131 740, 2020.

[4] K. Dema, N. M. T. Jamtsho, and B. Chhukha, "Intrusion detection system in cloud computing: A literature," 2021.

[5] K. Sharmila, "A review paper on cloud computing models," *international peer reviewed journal (JAC)*, 2020.

[6] M. Á. Díaz de León Guillén, V. Morales-Rocha, and L. F. Fernández Martínez, "A systematic review of security threats and countermeasures in saas," *J. computer security*, vol. 28, no. 6, pp. 635–653, 2020.

[7] U. A. Butt *et al.*, "A review of machine learning algorithms for cloud computing security," *Electronics*, vol. 9, no. 9, p. 1379, 2020.

[8] R. Doshi and V. Kute, "A review paper on security concerns in cloud computing and proposed security models," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, IEEE, 2020, pp. 1–4.

[9] M. Asadullah, R. K. Yadav, and V. Namdeo, "A survey on security issues and challenges in cloud computing," *Int. J. Innov. Res. Technol. Manag.*, vol. 4, no. 4, pp. 43–50, 2020.

[10] H. S. Yahia *et al.*, "Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling," *Asian J. Res. Comput. Sci.*, vol. 8, no. 2, pp. 1–16, 2021.

[11] D. M. Vistro, A. U. Rehman, S. Mehmood, M. Idrees, and A. Munawar, "A literature review on security issues in cloud computing: Opportunities and challenges," *J. Crit. Rev.*, vol. 7, no. 10, pp. 1446–1455, 2020.

[12] S. S. Kalyani, R. Ahmad, S. Joshi, *et al.*, "Comprehensive study on cloud security,"

[13] J. Chavan, R. Patil, S. Patil, V. Gutte, and S. Karande, "A survey on security threats in cloud computing service models," in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, IEEE, 2022, pp. 574–580.

[14] A. Shajan and S. Rangaswamy, "Survey of security threats and countermeasures in cloud computing," *United Int. J. for Res. & Technol.*, vol. 2, no. 7, pp. 201–207, 2021.

[15] P. Chatterjee, S. Mukherjee, R. Bose, and S. Roy, "A review on information security in cloud based system during covid-19 pandemic," *Brainwave, Brainware Univ.*, vol. 2, no. 1, pp. 60–69, 2021.

[16] M. Joshi, S. Budhani, N. Tewari, and S. Prakash, "Analytical review of data security in cloud computing," in *2021 2nd International conference on intelligent engineering and management (ICIEM)*, IEEE, 2021, pp. 362–366.

[17] S. Sansanwal and N. Jain, "Security attacks in cloud computing: A systematic review," in *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, IEEE, 2021, pp. 501–508.

[18] D. M. Bamasoud, A. S. Al-Dossary, N. M. Al-Harthy, R. A. Al-Shomrany, G. S. Alghamdi, and R. O. Algahmdi, "Privacy and security issues in cloud computing: A survey paper," in *2021 international conference on information technology (ICIT)*, IEEE, 2021, pp. 387–392.

[19] N. M. A. Al-Jaser, "A survey on cloud computing security–challenges and trust issues," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)*, vol. 18, no. 5, pp. 1–6, 2020.

[20] K. Jain, M. Gupta, and A. Abraham, "A review on privacy and security assessment of cloud computing," *J Inf Assur. Secur.*, vol. 16, no. 5, pp. 161–168, 2021.

[21] H. Jahankhani, A. Jamal, and S. Lawson, *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021*. Springer, 2021.

[22] H. S. Malallah, R. Qashi, L. M. Abdulrahman, M. A. Omer, and A. A. Yazdeen, "Performance analysis of enterprise cloud computing: A review," *J. Appl. Sci. Technol. Trends*, vol. 4, no. 01, pp. 01–12, 2023.

[23] M. Reece, T. L. J. au2, S. Mittal, N. Rastogi, J. Dykstra, and A. Sampson, *Emergent (in)security of multi-cloud environments*, 2023. arXiv: 2311.01247 [cs.CR]. [Online]. Available: https://arxiv.org/abs/2311.01247.

[24] M. Reece *et al.*, *Systemic risk and vulnerability analysis of multi-cloud environments*, 2023. arXiv: 2306.01862 [cs.CR]. [Online]. Available: https://arxiv.org/abs/2306.01862.

[25] N. S. Shaikh, A. Yasin, and R. Fatima, "Ontologies as building blocks of cloud security," *Int. J. Inf. Technol. Comput. Sci. (IJITCS)*, vol. 14, no. 3, pp. 52–61, 2022.

[26] I. Zulifqar, S. Anayat, and I. Khara, "A review of data security challenges and their solutions in cloud computing," *Int. J. Inf. Eng. Electron. Bus.*, vol. 12, no. 3, p. 30, 2021.

[27] I. Yurtseven and S. Bagriyanik, "A review of penetration testing and vulnerability assessment in cloud environment," in *2020 Turkish National Software Engineering Symposium (UYMS)*, IEEE, 2020, pp. 1–6.

[28] O. Alkadi, N. Moustafa, and B. Turnbull, "A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions," *IEEE Access*, vol. 8, pp. 104 893–104 917, 2020.

[29] P. Kumari *et al.*, "A review: Different challenges in energy-efficient cloud security," in *IOP Conference Series: Earth and Environmental Science*, IOP Publishing, vol. 785, 2021, p. 012 002.

[30] P. Géczy, N. Izumi, and K. Hasida, "Hybrid cloud management: Foundations and strategies," *Rev. Bus. & Finance Stud.*, vol. 4, no. 1, pp. 37–50, 2013.

[31] R. Jenkins, "Hybrid public private cloud computing for the media industry," *SMPTE Motion Imaging J.*, vol. 123, no. 3, pp. 56–59, 2014.

[32] S. R. Mamidi, "Enhancing cloud computing security through artificial intelligence-based architecture," *J. Artif. Intell. Gen. science (JAIGS) ISSN: 3006-4023*, vol. 5, no. 1, pp. 63–72, 2024.

[33] A. R. Arunarani, C. S. Shibi, N. Kanimozhi, G. Sumathy, and A. Maheshwari, "Enhancement of security in cloud computing using optimal risk access control model," in *2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, IEEE, 2023, pp. 1–7.

[34] R. K. Tiwari and S. Murugappan, "Enhancing security in cloud computing and protocols using harris hawks optimizer with deep learning for intrusion detection," in *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, IEEE, 2023, pp. 170–175.

[35] M. S. Oluyede, J. Mart, A. Olusola, and G. Olatuja, "Container security in cloud environments," *Sci. Prepr.*, 2024.

[36] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing cloud security—proactive threat monitoring and detection using a siem-based approach," *Appl. Sci.*, vol. 13, no. 22, p. 12 359, 2023.

[37] M. H. Diallo, "User-centric security and privacy approaches in untrusted environments," Ph.D. dissertation, UC Irvine, 2018.

[38] J. Aslam and K. Kumar, "Enhancing cloud data security: User-centric approaches and advanced mechanisms," *The Sci. Temper*, vol. 15, no. 01, pp. 1784–1789, 2024.

[39] B. Breve, V. Deufemia, *et al.*, "Empowering end-users in the specification of security rules.," in *EMPATHY@ AVI*, 2020, pp. 53–56.