Communications in Mathematics and Applications
Vol. 13, No. 1, pp. 315–329, 2022
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v13i1.1973

http://www.rgnpublications.com

Review Article

Major Security Threats and Attacks that Facing Cloud Computing with the Main Defence Strategies

Abdullah Safhi* , Adel Al-Zahrani and Aisha Mubaraki

Department of Information Science, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia
***Corresponding author:** safhi.phd@gmail.com

Received: December 17, 2021 **Accepted:** February 21, 2022

Abstract. Cloud Computing (Cloud) enables ubiquitous network access to a pool of shared and configurable resources. It is based on shared services and infrastructure convergence. Cloud computing offers a slew of advantages, including the ability to store large amounts of data and a variety of services, as well as addressing the issue of scarce resources and lowering service costs. Regardless of its benefits, the shift from local to remote computing has created a slew of security concerns and challenges for both consumer and provider. Addressing and evaluating cloud computing challenges is critical. Thus, by discussing cloud computing challenges alongside available and potential solutions, users, developers, and businesses can identify pertinent and timely responses to specific threats, resulting in the best possible cloud computing-based services. The purpose of this article is to discuss the inherent difficulties associated with cloud computing and some critical solutions for overcoming them. This article extracted and analyzed seminal papers in order to contribute to the corpus of literature by highlighting several critical challenges in the cloud computing domain and shedding light on how these challenges affect a variety of domains, including users, sites, and business. The most frequently mentioned challenges include data loss, data breaches, account or service hijacking, insecure interfaces and APIs, malicious insiders, insufficient due diligence, abusive cloud service use, shared technology issues, unknown risk profile, identity theft, business model changes, lock-in, cryptography, cloud data recycling, malware, and untrusted computing. This paper addressed these issues by incorporating previously discovered solutions. There has been discussion of the implications for both researchers and practitioners

Keywords. Cloud computing, Attack, Threats, Solutions and strategies

Mathematics Subject Classification (2020). 68M25, 68P30

1. Introduction

Distributed computing has arisen as a significant focal point of safety research lately [1]. Distributed computing innovation dates as far as possible back to the 1960s, when it was just free on centralized computer frameworks [2]. Distributed computing is anything but an original idea; it is inseparably connected to the framework figuring worldview and related advances, for example, utility processing, group registering, and circulated frameworks overall [3]. The distributed computing model is most generally characterized by NIST (National Institute of Standards and Technology) as a model for pervasive, helpful, on-request network admittance to a common pool of configurable figuring assets (e.g., networks, servers, stockpiling, applications, and administrations) that can be quickly provisioned and delivered with insignificant administration exertion or specialist organization interaction [1]. The innovation is a mix of different advancements like virtualization, bunching, and network registering, among others, that gives low rates to business clients as well as wipes out the expense of keeping an inside server farm [5]. Distributed computing, in the same way as other innovative administrations, has a plenty of advantages. For instance, it empowered the capacity of a lot of information and an assortment of administrations. Additionally, by sharing valuable resources among multiple users, this platform addressed the issue of scarce resources and reduced the cost of services [1]. In spite of the fact that distributed computing has surely known attributes, its security state is as yet intricate and should be addressed appropriately for the business to use cloud benefits all the more proficiently [1].

Distributed computing's development has made a huge number of safety issues. Security concerns go about as a critical obstruction to clients accepting Cloud Computing frameworks. Various reviews of planned cloud clients demonstrate that the essential obstruction to cloud reception is security [3]. Security concerns are a functioning area of examination that should be addressed properly to keep away from security dangers and assaults that cause ruin for both specialist co-ops and customers [1]. Thus, various scientists have researched and examined distributed computing security issues. Khalil *et al*. [6] led an audit study to distinguish the weakest security dangers in distributed computing by zeroing in on both end clients' and sellers' key distributed computing security dangers and investigating the different protections models and instruments [7] gave a review basic examination bearings, for example, portraying a strategy for shielding information from a cloud foundation supplier and a technique for program key interpretation that empowers a product as an administration application to give privacy administrations [8] conducted a review of the security and privacy concerns associated with cloud computing. Various types of known security threats and attacks are classified in this work, as are various types of cloud vulnerabilities, as well as the disadvantages of current solutions [8]. Ryan [9] discussed cloud computing security issues, including data location, storage, security, availability, and integrity. Indeed, this review focuses on one of the most serious security concerns, though it is critical to note that the authors discuss only security concerns without addressing potential solutions [10]. Additionally, [11] presented a taxonomy of virtualized system attacks in terms of the target at various levels, the source, and the attackers' goals. Indeed, they intend to demonstrate the evolution of threats, associated security, and trust assumptions in virtualized systems at various layers, including hardware, operating system, and application [10]. However, there is a dearth of discussion in the aforementioned papers about security issues and their resolutions [10]. Additionally, several papers do not address open issues in the cloud, and several papers do not address cloud security threats and

attacks [10]. Attempts were made in this study to highlight almost all of the cloud computing obstacles in comparison to the solutions presented in previous research to close the gap and help decision-makers adopt and implement cloud computing.

Cloud computing adoption could be jeopardized by serious security risks, according to the study, which aims to identify those risks and determine how to address them. In other words, the research goal of the article could be stated as follows: In what ways are the most serious cloud computing threats and attacks being countered? Cloud vulnerabilities and threats are the issues that, if resolved successfully, will transform Cloud into a digital fortress for its users [8]. The documentary analytical descriptive strategy will be used in this study, which entails referring to documents and literature such as research, articles, and books and addressing them in the study through description and analysis in order to elicit results and indications. To address the study's topic, this study will evaluate and critique existing publications on cloud computing security issues. It will accomplish this through the use of the following research tools: databases accessible via the Saudi Digital Library and international search engines. A selection of publications was extracted and analysed. To accomplish the study's objective, a qualitative approach is taken in order to adequately describe the phenomenon under investigation. According to Sgandurra and Lupu [10], a quantitative approach examines what occurs during a phenomenon, whereas a qualitative approach sheds light on why it occurs. The descriptive analytical method is used in this study to conduct the research. Descriptive assessments place a greater emphasis on environmental variables and are based on direct observation of an individual's behaviour and events occurring in his or her natural environment [12]. Descriptive research may help us better understand how reinforcement works in nature [12].

This article begins with the article body, then moves on to the discussion section, and finally concludes with the conclusion.

2. Literature Reviews and Discussion

In this section, we will provide the main research articles that discuss and analyse the major Security Threats and Attacks that Facing Cloud Computing with the Main Defence Strategies.

Basu *et al*. [3] study titled "*Cloud Computing Security Issues and Challenges: A Survey*". Cloud computing raises a number of security concerns. These issues are classified as cloud provider security issues and customer security issues. This article discusses the history and business model of cloud computing. Additionally, a few security concerns and challenges are discussed. The following is a list of several cloud computing security concerns:

- *Specialized/privileged access to data*- Location of data - Segregation of data - Data availability - Compliance with regulatory requirements – Recovery - Support for Investigations - Long-term viability

According to Basu *et al*. [3], the major security challenges associated with cloud computing and their solutions discussed in the following:

- *Service-Level Agreement:* The service contract specifies the service level. The goal is to reduce conflict while better understanding your customers' needs.
- *Authentication and Identity Management*: They allow remote data access. Authentication of users and service provisioning (IDM). IDM safeguards users and data. IDMS manages firm data and computing.

- *Data-Centric Security and Protection:* Prevent data leaks and unauthorized cloud provider access. It is impossible to override customer privileges. Apply access control policies.
- *Trust Management:* The service provider must store confidential data. Any trust framework should aim to provide generic parameters for building and managing trust.
- *Access Control and Accounting:* Capture dynamic, attribute- or credential-based access requirements. It should also capture SLAs. CREDENTIAL OR ATTRIBUTE-BASED PO SAML, XACML, and Web services standards allow for secure access control.

Nadeem [8] study titled "*Cloud computing: security issues and challenges*". This article discusses the vulnerabilities of cloud architecture, internet protocols, operating systems and application software, as well as cryptography. Additionally, it identifies cloud security challenges and countermeasures to address them. This article classified cloud security concerns into four components: (1) physical layer, (2) virtualization layer, (3) service provider layer, and (4) user layer, as shown in Table 1.

Table 1. Cloud architecture layers and related security issues

Layer	**Threats**
User Layer	Vulnerabilities in application - Vulnerabilities in browser and APIs - Authentication, Access Control etc.
Service Provider Layer	Access Control issues (Authentication, Authorization etc.) - Transient Data security issues - Policy Enforcing - Trust Management - Audit, Regulations compliance.
Virtualization Layer	Hypervisor and Virtual Machines vulnerabilities - Isolation between Virtual Machines - Access Control issues - Regulations compliance.
Physical Layer	Network vulnerabilities and attacks - Data storage issues - Confidentiality, Integrity, Availability - Database intrusion

The following summarizes the countermeasures against security issues discussed in [8].

- Security must be viewed as a shared responsibility between users and providers of Cloud services.
- Compliance with industry-recognized security standards such as PCI-DSS, IPSec, and TLS, as well as government regulations such as FISMA, not only enables you to earn the trust and satisfaction of your users, but also lays a solid foundation.
- Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), and Firewalls can all significantly reduce vulnerabilities.
- Cloud providers must have a business continuity and disaster recovery plan in place to address both probable and improbable incidents.

Amara *et al*. [1] study titled "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques". This article discusses the architectural principles of cloud computing, the critical security requirements for cloud computing, cloud computing security threats and attacks, mitigation techniques for cloud computing security attacks, and future research challenges. Table 2 summarizes the security risks associated with cloud computing and the mitigation techniques available.

Table 2. Security threats in cloud computing and their mitigation techniques

Threat	**Mitigation Techniques**
Data loss	Backups on a regular basis - By implementing appropriate encryption techniques - By ensuring the security of data in transit - Establishment of robust key generation, storage, and management procedures - Clearly identifying supplier reinforcement and maintenance techniques in a legal manner.
Data Breaches	By encrypting data in transit - To safeguard data, it should be analyzed during both the design and runtime phases - Using robust key generation, storage, and management techniques - Clearly indicating to the provider that persistent media must be wiped prior to being released into the pool - Clearly stating backup and retention strategies on a legal basis - Through the use of robust application programming interfaces (API).
Account or Service Hijacking	In-depth knowledge of security policies and service level agreements (SLA) - Using methods of multi-factor authentication - Strict monitoring to keep an eye out for unauthorized activity - Prevent consumers and services from sharing credentials.
Insecure Interfaces and APIs	Strong mechanisms for authentication and access control - Encryption of data transmission - An examination of the cloud service provider's interfaces - A thorough understanding of the API dependency chain.
Malicious Insiders	Incorporate human resource management (HRM) into a legal contract - Strict supply chain management procedures to follow - Providing adequate clarity regarding security and administrative processes.
Insufficient Due Diligence	Cloud applications and services are implemented using industry standards - Qualitative and quantitative risk assessment - Provide access to relevant logs, data, and infrastructure details.
Abusive Use of Cloud Services	Ensuring that authorization and authentication are robust - Adequate network traffic auditing - Improved monitoring of credit card fraud.
Shared Technology Issues	By implementing more robust authentication and access control mechanisms - Conduct vulnerability and configuration assessments - Keep an eye out for unauthorized changes/activities in the environment - Utilization of service level agreements (SLAs) for patching and vulnerability remediation.
Unknown Risk Profile	Provide access to relevant logs, data, and infrastructure details - Data breach alerting system auditing.
Identity Theft	Password, authentication, and access control mechanisms that are strong.
Changes to Business Model	Provision of a system for controlling and monitoring the offered services.
Lock-IN	Monitoring is accomplished through the use of an Instruction Detection System (IDS), an Intrusion Prevention System (IPS), and a firewall.

Barona and Anita [2] study titled "A survey on data breach challenges in cloud computing security: Issues and threats". This article discussed cloud computing, various cloud models, and the primary security threats and data breach issues that are currently being investigated within the cloud computing framework. This paper examined the significant research and challenges associated with data breach in cloud computing and provided best practices to service providers.

Additionally, it makes an attempt to persuade cloud servers to prioritize their primary concern in this dire economic climate. Cloud computing introduces a slew of security risks. Several of them include the following:

- *Privileged User Access:* Any unauthorized access to the client's confidential information should be verified by a new membership. If not, data leakage will increase. The data owner has complete control over the data. Other users have restricted privileges.
- *Regulatory Compliance:* Cloud providers conduct internal audits on cloud systems and processes but never allow external audits. The cloud provider also refuses to update network security certificates.
- *Data Location:* In cloud computing environments, the client is unaware of the information's storage locations.
- *Investigative Support:* A specific request regarding unauthorized cloud computing customer data access is problematic. Unauthorized access is terminated either locally or remotely (external client).
- *Data segregation:* Through the sharing process in cloud computing, data from one client can be made available to other clients. As a result, multiple clients can access the data concurrently.
- *Recovery:* If the cloud provider's server or data farm used to store customer data fails due to natural disasters or system failures, it is the cloud provider's duty to inform the customer.

This article discussed several novel security approaches used by cloud computing organizations to protect against data breaches. This strategy entails the following:

- *Information-centric security:* Businesses can use an internal security strategy to protect cloud data. It's called data-driven security. This self-insurance method uses data-encoded knowledge.
- *High-assurance remote server attestation:* Trusted computing helps. A trusted screen watches the cloud server. The trusted screen validates. Secure screen development occurs alongside framework and app development.
- *Privacy-enhanced business intelligence:* Bytes are encrypted. Text encryption schemes are adaptable. Crypher text is used for homomorphic encryption and private data recovery (PIR).
- *Privacy and data protection:* All cloud security solutions must include mechanisms for ensuring user privacy.
- *Encryption that can be searched/structured:* This method's foundation is encryption. It hides the data and computations from the cloud.
- *Storage proofs:* This is a SLA between CSPs and their clients. No data will be used without the client's permission.
- *Secure computation aided by a server:* This security feature allows a server and users to compute on cipher text without revealing the original data.
- *Tools:* Authentication and authorization are among the tools used to detect anomalies. These tools can detect malicious activity disguised as benign files.

Sgandurra and Lupu [10] study titled "Cloud security issues and challenges: a survey". This article discussed the fundamental characteristics of cloud computing, as well as security concerns, threats, and solutions. Additionally, the paper discusses several critical cloud topics, including cloud architecture frameworks, service and deployment models, cloud technologies, and cloud security concepts, threats, and attacks. Additionally, the paper discusses a number of open research issues concerning cloud security. This study discusses the following data storage and computing security issues and solutions (Table 3).

Table 3. Presents issues and solutions relating to data storage and computing security

Security topic	Security issues	Security solutions
Data storage	Remote data storage - Loss of control - Data pooling, data locality - Multi-location - Complex model for integrity checking	Better security scheme for resident data - File Assured Deletion (FADE) scheme for data – Security - SecCloud protocol for secure storage.
Un-trusted computing	Top down SLAs - Malicious users, downtimes, slowdowns - Dishonest computing, root level error in backups, migration and restoring problem - Weak security solutions for computing models	A non-interactive solution - A lightweight and low-cost solution for e-banking.
Data and service availability	Counterfeit resource usage - Cloud interruption - Hardware availability issue (hardware fault)	A solution for data availability - Proxy re-encryption scheme based on time-based.
Cryptography	Insecure cryptography mechanism, poor key management - faulty cryptography algorithms - Brute force and Dictionary attack	Order-preserving encryption - Cryptography in cloud computing.
Cloud data recycling	Deficient implementation of data devastation policies - Un-used hard discard - Hard disk multi-tenant usage - Resource recycling	Secure data deletion
Malware	Failure of signature based anti-viruses - Cloud malware syncing	Detecting malware

Basu *et al*. [3] study titled "Cloud computing security challenges & solutions - A survey". The paper discussed critical security flaws and the security requirements for an existing Cloud system. A broad overview of these issues has been presented here to emphasize the critical nature of understanding the Cloud computing framework's security flaws and developing appropriate countermeasures. Finally, various cloud security schemes have been compared. The paper as a whole aimed to provide a comprehensive overview of the current state of cloud security and its future prospects. Confidentiality, Integrity, and Availability are the three factors that have been considered in this evaluation of the Cloud system's security (CIA). This study presented these cloud security factors as follow:

- *Confidentiality:* Aliens cannot access company assets. Yours may contain intruder data. Client data may be accessed by CSP employees. Protect the VM's network and image.

- *Integrity:* Protection against asset tampering. Verification of inheritance This may compromise its integrity. Attackers frequently alter WSDL files.
- *Availability:* This safeguards a CSP. Small outages can lead to big losses. Essai de produce If 80% of a resource is used, more resources will be provided dynamically.

According to Basu *et al*. [3], the following are some of the remarkable and beneficial methodologies that have been designed and implemented to address the Cloud System's diverse security requirements:

- *Data Confidentiality*: The main concern with cloud data privacy is keeping users' data safe from prying eyes while keeping cloud service providers in the dark.
- *Virtualization Confidentiality:* Along with data security, CSPs and Cloud users should consider the security of VMs hosted on the Cloud platform.
- *Data Integrity:* CSPs must safeguard both client and cloud data. Regularly evaluate the data. Storage in the cloud prevents data download and comparison.
- *Virtualization Integrity:* Virtualization Integrity concerns the virtualization layer's integrity, from the Virtual Machine metadata to the Hypervisor.
- *Data Availability:* Adaptive Resource Allocation in the Cloud (DARAC). This scheme targets EDoS auto-scaling in the Cloud (differentiating legitimate traffic from malicious).
- *Virtual Machine Availability:* A virtualized IDS for DDoS mitigation was also proposed. Cloud availability is a major concern beyond VMs. IP failover is a cloud service. IBM Smart Cloud enterprise ensures cloud service availability with IP failover.

Kumar *et al*. [7] study titled "Exploring Data Security Issues and Solutions in Cloud Computing". This article examined the various data security issues that arise when cloud computing is used in a multi-tenant environment and proposes methods for resolving them. Additionally, this paper discussed Cloud computing models, such as deployment and service delivery models. Data are critical in any business or Cloud Computing environment; data leakage or corruption can undermine public confidence and ultimately result in the failure of the business. This study classified data security concerns in cloud computing into four major categories:

Security Challenges in the CIA Triad: Breach of CIA can have a significant impact on the cloud computing business, as data is the lifeblood of any enterprise. CIA triad data security is improved at various stages of the data lifecycle. Here are some vital methods:

- Apply data encryption when the data is at rest and also when the data is in transit. Use strong encryption algorithms like AES and RSA.
- Encryption protects data from cloud provider attacks, but not from configuration errors or software bugs. Data changes can be detected using hash methods.
- TPA can be used to verify data integrity.
- The Provable Data Possession (PDP) scheme was initiated to statistically examine the data without retrieving it from cloud storage.
- Never store the encryption keys with the data.
- Adopt proper Identity and Access Management (IAM) techniques.
- Address data duplication, redundancy, backups, and resilient systems.

- Include a failover strategy in case the CSP fails.
- If other methods fail to address the issue of availability, data dispersion can be used.

Security Challenges in the Authentication and Access Control (AAC): AAC establishes and verifies a user's identity to connect to, access, and use cloud resources. Several critical AAC security measures include:

- Always use single sign-on.
- Access control at Amazon Web Services is multi-factor (AWS).
- Biometric authentication is the safest single-sign-on method.
- RSA cryptosystem supports two-factor, knowledge-based, and adaptive authentication.
- To improve data security in cloud computing, IDS, firewalls, and responsibility separation can be implemented on various network and cloud layers.
- Other id management options exist. Try Azure AD, Okta identity management, or McAfee cloud identity manager. Recent trends in corporate infrastructure favour IDaaS.
- It uses XML-based OASIS (Organization for the Advancement of Structured Information Standards) open standards to exchange authentication and authorization data between security domains, while O Auth uses tokens to share private resources.

Security Challenges Due to Broken Authentication, Session and Access Controls: Errors in application domain authentication and session management cause authentication and session control issues. Here are some solutions:

- Consolidate strong authentication and session management controls.
- Eliminate XSS flaws that can steal session IDs.
- The user must be authorized for the requested resource before using a direct reference from an untrusted source.
- A code pattern that prevents attackers from directly targeting unauthorised resources is per user or session indirect object references.
- Automated verification: Verify proper authentication deployment using automation.

Other Data Related Security Issues: These are minor data security issues in cloud computing. Locations of data storage differ in legal systems. Other data security options:

- Due to potential regulatory, contractual, and other jurisdictional issues, CSC should know the data's logical and physical location.
- Establish data location and jurisdiction policies.
- Make use of intelligent data segregation techniques.
- Encrypt backup data to prevent data leakage.

Subramanian and Jeyraj [13] study titled "Recent security challenges in cloud computing". This paper focuses on and investigates the security challenges that cloud entities face. Cloud Service Provider, Data Owner, and Cloud User are examples of these entities. Concentrating on the crypto-cloud, this consists of various Communication, Computation, and Service Level Agreements. It provided the necessary upgrades by researching the causes and effects of various

cyber-attacks. In Table 4, this article discussed the security challenges confronting cloud-based entities.

Table 4. Security challenges confronting cloud-based entities

Level	Threats	Threats issues
Communication level	Security in network level	The issues with respect to network level security are: Domain Name Server Attacks; Prefix Hijacking in Border Gateway Protocol; Issue of Reused IP Addressing; Sniffer Attacks etc.
	Security in application level	The issues to be addressed at this level are: Cookie Poisoning; DDoS; Hidden Field Manipulation; Dictionary Attack; Google Hacking; CAPTCHA Breaking etc.
	Security at host level	The major host level threats are: Viruses, Trojan horses, and worms; Profiling; Password cracking; Foot printing; Denial of service; Unauthorized access.
Computational level	Virtualization challenges	VM level (Virtual layer) security challenges include: VM cloning - VM isolation - VM migration - VM Escape - VM rollback - VM sprawl - VM Hopping/VM Hyper jumps - VM poaching
		Hypervisor level (Virtualization layer) include: Basic information security - Threats in virtual networking - VM-to-VM attack - Security issue with VM introspection - Issues due to virtualized trusted computing (VTC) - Hyper jacking / hypervisor subversion - Issue due to resource sharing - Threats in hypervisor integrity protection and isolation of VM's
		Hardware level (Physical layer): The hardware layer consists of resources like CPU, memory, networking and storage, etc.
Data level challenges	Data in-transit	The following issues can take place: Data Lineage - Data Leakage
	Data-in-rest	The following issues can take place: Data Recovery - Data Reminisce/Sanitization/Removal - Data Backup - Data isolation - Data segregation - Data Lock-in - Data Location
Service level agreements (SLA's)	Customer-based SLA	
	Service-based SLA	
	Multi-level SLA	

Sun [14] Study titled "Security and privacy protection in cloud computing: Discussions and challenges". This paper reviewed the research progress on privacy security issues in cloud computing. A comprehensive privacy security protection framework was proposed. Second, it compared and analyzed the characteristics of several technologies, including access control,

cipher text policy attribute-based encryption (CP-ABE), key policy attribute-based encryption (KP-ABE), fine-grainmulti-authority revocation, trace mechanism, proxy re-encryption (PRE), hierarchical encryption, searchable encryption (SE), and multi-tenant, trust. Finally, it discussed current issues and future research directions. This study concentrated on privacy security issues in cloud computing which presented in Figure 1.

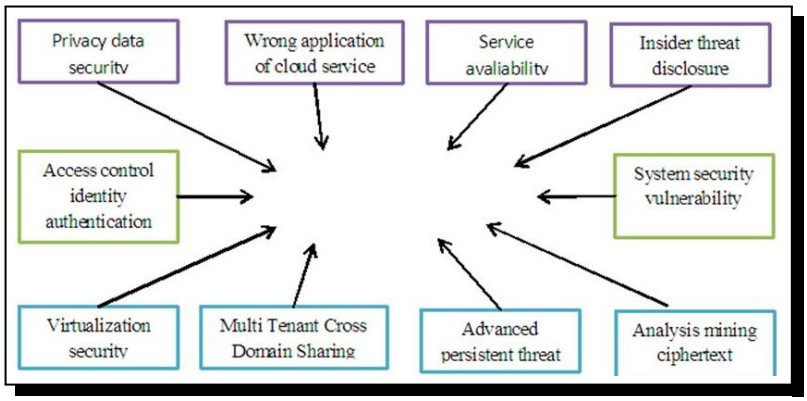

Figure 1. Privacy security issues in cloud computing

Sun [14] paper proposed a comprehensive cloud computing privacy protection security system based on a variety of technologies, including access control, trust, attribute-based encryption, search encryption, and others, as illustrated in Figure 2.

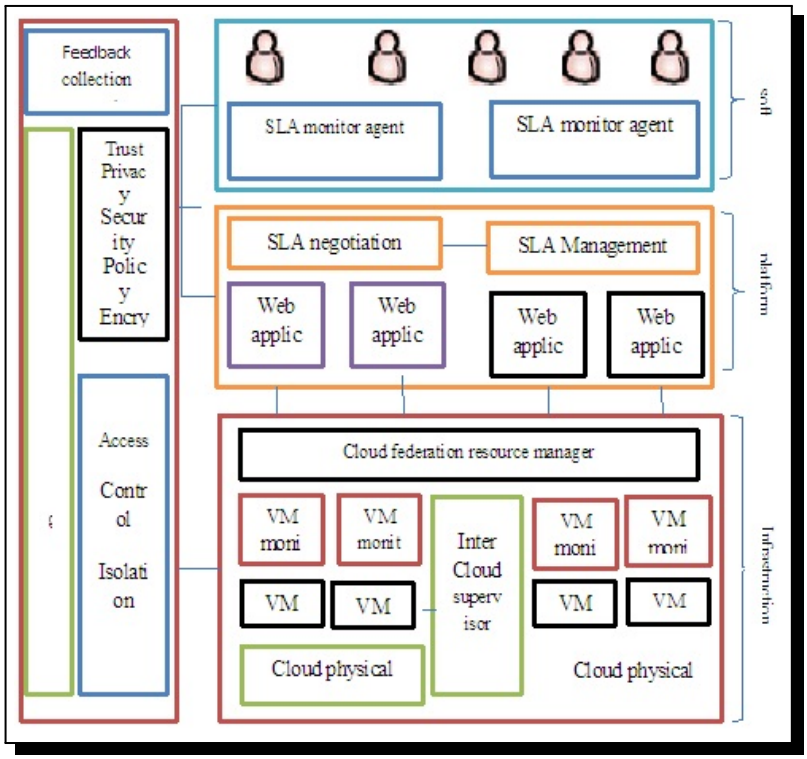

Figure 2. Cloud computing system's privacy protection framework

Amara *et al*. [1] study titled "A survey on security challenges in cloud computing: issues, threats, and solutions". This survey's narrative review covered cloud security issues, threats,

and vulnerabilities. This research looked into the components of cloud computing as well as the security and privacy issues that these systems face. This work also presented a new classification of recent security solutions in this field. This survey also discussed open issues and proposed future directions. This paper focused on the security challenges faced by cloud entities like cloud service providers, data owners, and cloud users. Cloud security issues can be divided into five categories, as shown in Figure 3: security policies, user-oriented security, data storage security, application security, and network security. Additionally, as illustrated in Figure 4, this study discussed security attacks and threats in cloud computing.

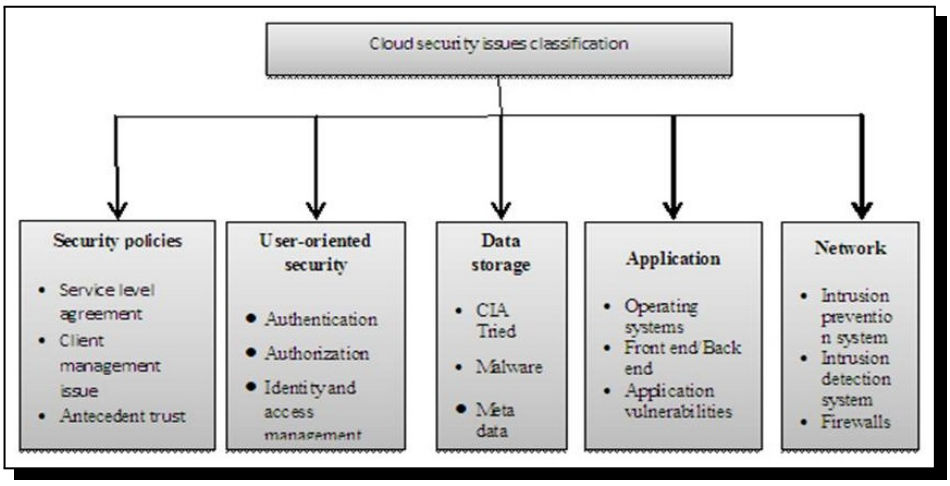

Figure 3. Cloud security issues

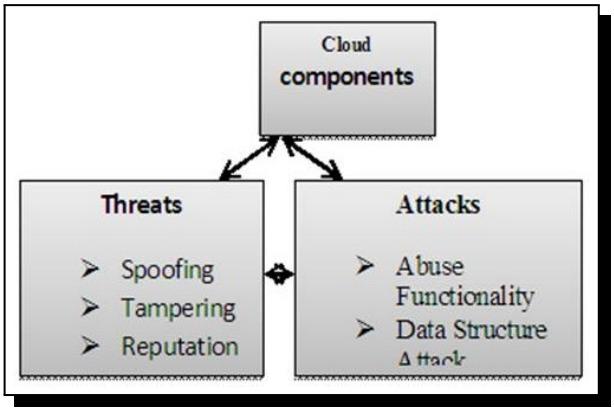

Figure 4. Security attacks and threats in cloud computing

3. Discussion

Basu *et al*. [3] classified the challenges/concerns associated with the cloud on-demand model as shown in (Figure 5).

Service-Level Agreement, Authentication and Identity Management, Data- Centric Security and Protection, Trust Management, and Access Control and Accounting are five solutions proposed by [3] to address cloud computing security challenges. In the same vein, Amara *et al*. [1] and Sgndurra and Lupu [10] proposed some mitigation techniques to address data

loss, data breaches, account or service hijacking, insecure interfaces and APIs, malicious insiders, insufficient due diligence, abusive use of cloud services, shared technology issues, unknown risk profile, identity theft, business model changes, lock-in, cryptography, cloud data recycling, malware, and un-trusted computing. Subramanian and Jeyraj [13] outline the security challenges that cloud-based entities face at various levels, including communication, computation, data, and service level agreements (SLAs). Kumar *et al*. [7] classified data security concerns in cloud computing into four major categories and strategies for addressing these challenges in their study. Security Challenges in the CIA Triad, Authentication and Access Control (AAC) Security Challenges, Security Challenges Due to Broken Authentication, Session and Access Controls, and Other Data Related Security Issues are among the challenges. Basu *et al*. [3] proposed some remarkable and advantageous methodologies that have been designed and implemented to address the Cloud System's various security requirements. Data Confidentiality, Virtualization Confidentiality, Data Integrity, Virtualization Integrity, Data Availability, and Virtual Machine Availability are some of the methodologies used.

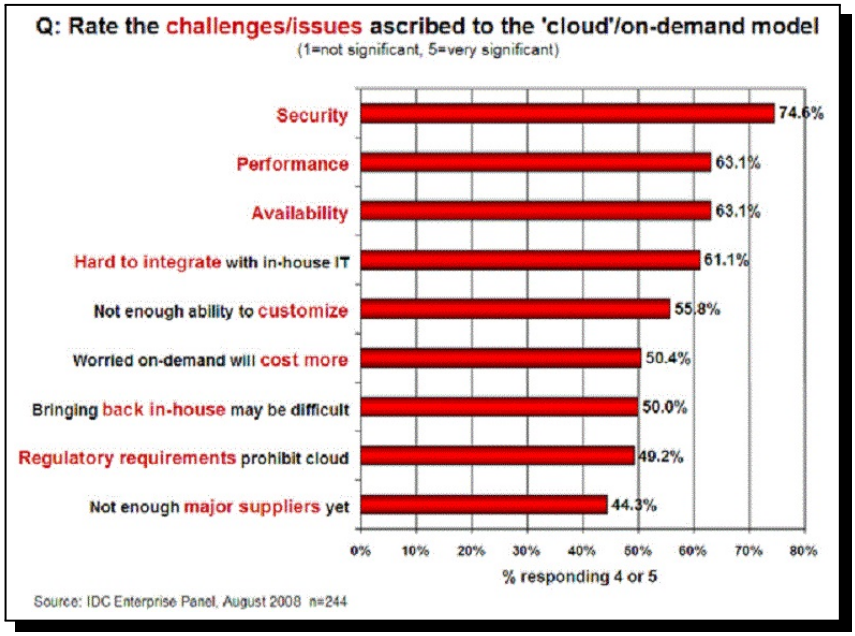

Figure 5. Rate the challenges/issues ascribed to cloud on-demand model (source [3])

Regarding privacy protection, Sun [14] paper framework stated that physical isolation and associated policy management rules are typically used at the infrastructure layer. Encryption, trust, and privacy policies are primarily used at the platform and software application layers. Of course, these technologies are not application-specific and require additional analysis.

To achieve comprehensive cloud security, Tabrizchi and Rafsanjani [15] affirmed that all cloud components must be protected against known and unknown attacks. Insider attacks are detected using an indicator. This indicator will help secure the cloud system [1]. To automate defenses and enforce data governance principles, invest in cloud cyber security platforms that use automation and AI ([1], [16]). Organizations can more easily identify and classify potential threats by automating the process using behavioral analytics ([17], [4]).

4. Conclusion and Future Work

Massive opportunities have opened up as a result of cloud computing threats and attacks. Cloud computing is a collection of technologies such as virtualization, clustering, and grid computing that not only provides low rates to business users but also eliminates the costs associated with maintaining an internal data centre. While cloud computing has well-understood characteristics, its security state remains complex and must be addressed appropriately in order for the industry to more efficiently utilize cloud services. This article discusses a variety of cloud computing security features and issues, including data loss, data breaches, account or service hijacking, insecure interfaces and APIs, malicious insiders, insufficient due diligence, abusive use of cloud services, shared technology issues, and an unknown risk profile. Additionally, it encompasses difficulties associated with CIA Triad Security Challenges, Authentication and Access Control (AAC) Security Challenges, Security Challenges Due to Broken Authentication, Session, and Access Controls, and Other Data Security Issues. All of this is in addition to the Cloud System's numerous security requirements. The most common threats and attacks are against data confidentiality, virtualization confidentiality, data integrity, virtualization integrity, data availability, and virtual machine availability. Additionally, it discusses how to avoid these problems in the future. These contributions to research are both theoretical and practical in nature. Theoretically, this study focuses on the most pervasive challenges across a range of fields, assisting scholars in developing a holistic understanding of these issues and validating the methods used to address them. This study incorporates previously identified solutions to address these issues. These solutions would benefit organizations and users who interact with cloud computing platforms in practice. While some progress has been made, there is still much more work to be done to secure cloud computing from attackers. To effectively address cloud computing security concerns, technological solutions must be complemented by appropriate legislation and regulation.

Competing Interests

The authors declare that they have no competing interests.

Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] N. Amara, H. Zhiqui and A. Ali, Cloud computing security threats and attacks with their mitigation techniques, in: *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (CyberC), 2017, pp. 244 – 251, DOI: 10.1109/CyberC.2017.37.

[2] R. Barona and E. A. M. Anita, A survey on data breach challenges in cloud computing security: Issues and threats, in: *2017 International Conference on Circuit, Power and Computing Technologies* (ICCPCT), pp. 1 – 8, 2017, DOI: 10.1109/ICCPCT.2017.8074287.

[3] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury and P. Sarkar, Cloud computing security challenges & solutions – A survey, in: *2018 IEEE 8th Annual Computing and Communication Workshop and Conference* (CCWC), 2018, pp. 347 – 356, DOI: 10.1109/CCWC.2018.8301700.

[4] M. A. Elmagzoub, D. Syed, A. Shaikh, N. Islam, A. Alghamdi and S. A. Rizwan, A survey of swarm intelligence based load balancing techniques in cloud computing environment, *Electronics* **10**(21) (2021), 2718, DOI: 10.3390/electronics10212718.

[5] M. Kaur and H. Singh, A review of cloud computing security issues, *International Journal of Grid Distribution Computing* **8**(5) (2015), 215 – 222, DOI: 10.14257/ijgdc.2015.8.5.21.

[6] I. M. Khalil, A. Khreishah and M. Azeem, Cloud computing security: A survey, *Computers* **3**(1) (2014), 1 – 35, DOI: 10.3390/computers3010001.

[7] P. R. Kumar, P. H. Raj and P. Jelciana, Exploring data security issues and solutions in cloud computing, *Procedia Computer Science* **125** (2018), 691 – 697, DOI: 10.1016/j.procs.2017.12.089.

[8] M. A. Nadeem, Cloud computing: security issues and challenges, *Journal of Wireless Communications* **1**(1) (2016), 10 – 15, DOI: 10.21174/jowc.v1i1.73.

[9] M. D. Ryan, Cloud computing security: The scientific challenge, and a survey of solutions, *Journal of Systems and Software* **86**(9) (2013), 2263 – 2268, DOI: 10.1016/j.jss.2012.12.025.

[10] D. Sgandurra and E. Lupu, Evolution of attacks, threat models, and solutions for virtualized systems, *ACM Computing Surveys* **48**(3) (2016), 1 – 38, DOI: 10.1145/2856126.

[11] F. B. Shaikh and S. Haider, Security threats in cloud computing in: *2011 International Conference for Internet Technology and Secured Transactions*, pp. 214 – 219, 2011.

[12] A. Singh and K. Chatterjee, Cloud security issues and challenges: A survey, *Journal of Network and Computer Applications* **79** (2017), 88 – 115, DOI: 10.1016/j.jnca.2016.11.027.

[13] N. Subramanian and A. Jeyaraj, Recent security challenges in cloud computing, *Computers & Electrical Engineering* **71** (2018), 28 – 42, DOI: 10.1016/j.compeleceng.2018.06.006.

[14] P. Sun, Security and privacy protection in cloud computing: Discussions and challenges, *Journal of Network and Computer Applications* **160** (2020), 102642, DOI: 10.1016/j.jnca.2020.102642.

[15] H. Tabrizchi and M. K. Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions, *The Journal of Supercomputing* **76**(12) (2020), 9493 – 9532, DOI: 10.1007/s11227-020-03213-1.

[16] A. Verma and S. Kaushal, Cloud computing security issues and challenges: A survey, in: A. Abraham, J. L. Mauri, J. F. Buford, J. Suzuki and S. M. Thampi (eds.), *International Conference on Advances in Computing and Communications*, 2011, pp. 445 – 454, Springer, Berlin — Heidelberg, DOI: 10.1007/978-3-642-22726-4_46.

[17] S. Zhang, S. Zhang, X. Chen and X. Huo, Cloud computing research and development trend, in: *2010 Second International Conference on Future Networks*, 2010, pp. 93 – 97, DOI: 10.1109/ICFN.2010.58.