CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES

Aqeel Ahmed[1], Sandeep Kumar[2], Azhar Ali Shah[3], Arifa Bhutto[4]

IICT, University of Sindh, Hyderabad, Pakistan

*Corresponding E-mail: [1]dotaqeel@gmail.com , [2]smjavailable@gmail.com, [3]azhar.shah@usindh.edu.pk, [4]arifa.bhutto@usindh.edu.pk

ABSTRACT

Objective: Cloud computing security is a mushrooming service that has identical features to conventional IT security. It offers protecting sensitive information from data theft, loss and destruction. One of the advantages of cloud services is that you can work at scale. But is the system secured properly? The system is vulnerable to attacks from many directions e.g., unsecure network, data losses, data breaches, cyber-attacks, reduced control etc. Therefore, we have new opportunities to deliver security solutions that meet new challenges. This paper discusses on these issues and provide remedial suggestions which can be focused on improving the system.
Research Method: This paper presented a details of issues faced during cloud computing security through a comprehensive literature review.
Findings: The main drawback of current cloud service implementations is that they are unable to offer high levels of security. Transmission paths that involve a third party must also meet a security requirement. To guarantee a high level of security, privacy, authenticity, integration, speed, scalability, and dependability when using cloud services, many factors must be improved. Perhaps a promising area of research to address cloud computing security issues will be an automated service level agreement, a third-party trustee, or a new extension.
Originality: This study will help the practitioner in understanding the challenges faced in cloud computing security. It will support in developing a propoer security system to an efficient cloud computing system.

Keywords: Cloud Architecture, Security issues, challenges

1. INTRODUCTION

According to Sian John - a Cyber Senior security strategist at Symantec, “Cybersecurity can be understood as traffic and vehicle safety. If a car hasn't changed in the last 30 years but has a lot of safety features, it may not look very nice, but it can save lives with seat belts and airbags. Features in cars ensure good manners, grace and attitude, some focus on physical safety to remind you of risks, and some features are built in for user safety” (Sarder & Haschak 2019).

In the history of cloud computing, the intentional or unprepared disclosure of data is common. This compromises data protection and privacy of cloud storage (Lo'ai & Saldamli 2021). The first type of risk is accidental data disclosure due to design flaws in the provider's cloud software. For example, a bug allowed unauthorized users to view documents from Google Docs (Holzner & Conner 2009). The history of cloud computing is full of cases of willful or unprepared data disclosure. This compromises data protection and privacy of cloud storage. The first type of risk is accidental data disclosure due to design flaws in the provider's cloud software. For example, a bug allowed unauthorized users to view documents from Google Docs, while Flicker and Facebook also skipped users' private pictures due to bugs (Mahmood 2013; Lindholm 2021; Phan et al. 2021).

By 2025, the amount of data stored in the cloud will reach 100 zettabytes (Walzberg et al. 2022). Cloud adoption has reached a critical juncture, and not just the average internet user, but most, if not all, businesses are expected to move more workloads from traditional on-premises storage to the cloud (Golec et. al. 2021). While many issues need to be identified, analyzed, and resolved, this white paper attempts to examine cloud computing security and has the ability to report ona myriad of aspects of vulnerable security areas and their subsequent solutions (Ahmad et. al. 2022).

A few queries that need to be addressed are:

a. Access control for privileged users
b. Legal Compliance
c. location of the data
d. data separation
e. Data protection and recovery support
f. investigation support
g. Long term viability

It is strongly recommended that these issues be assessed and addressed along with other risks (Mohammad & Pradhan 2021; Singh & Phulre 2021). Some of the reviews could be (Nimmy et. al. 2022):

a. organizational skills and maturity
b. Technology and Data Risks
c. Application migration and performance risk
d. risk people
e. risk Process
f. risk Policies
g. Advanced supply chain risks

This paper is divided into five sections. Section I is providing a historical background of cloud computing and the risks associated with it. Section II go into detail in the architecture of cloud computing and the nomenclature used for cloud computing in this paper. Section III provides how each module in cloud computing is integrated with each other and doing their particular tasks. Proceeding forward, section IV gives detail on how their components can be compromised and will have security issues. Moreover, it discusses those issues in detail. Lastly, Section V summarizes the discussion and provides solutions as well as prospects in this domain.

2. CLOUD ARCHITECTURE

According to the NIST, Cloud Computing Reference Architecture, there are five main influencers exposed to cloud computing and its security implications. This article is about the cloud Perceptions of threats and risks by consumers and cloud service providers (Koltyukova 2021; Devarakonda 2021; Sharma 2021). Cloud architecture components shown in table 1 and figure 1 (Bharathi et. al. 2021).

Table 1: Users in NIST Cloud Computing Reference Architecture (Bharathi et. al. 2021)

User	**Definition**
Cloud Consumer	A person or organization who fosters a business relation and consumes the services offered by a cloud provider.
Cloud Provider	A person, or an organization or a legal entity that is responsible for offering their services to the parties interested.
Cloud Auditor	A party or an entity that has the power or ability to freely assess cloud services, the operations of information systems, and the level of performance and the extent of security offered by the cloud implementation
Cloud Broker	A party, person or an organization that has the duty to manage the efficiency level of utilization and delivery of cloud services and who oversees the negotiation relations between cloud service providers and cloud computing users.
Cloud Carrier	A middle person that connects and transports cloud services from cloud service providers to cloud users.

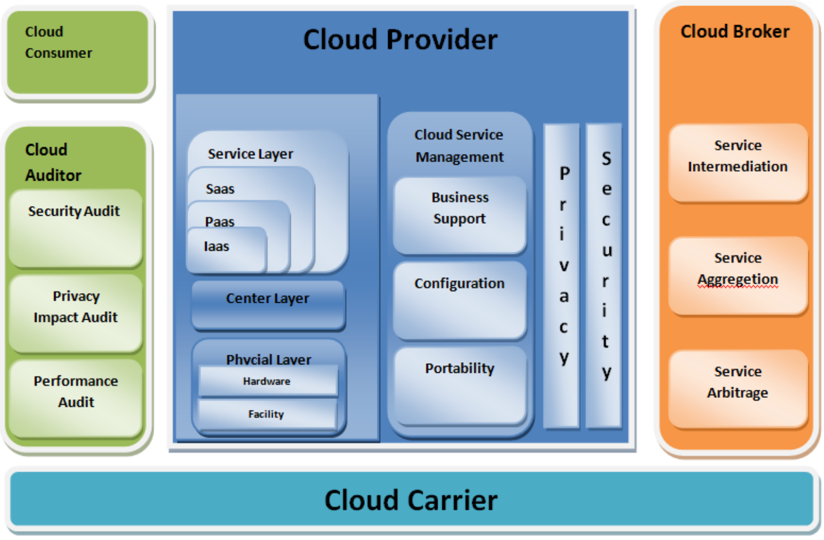

Figure 1: Users in NIST Cloud Computing Reference Architecture (Bharathi et. al. 2021)

3. THE CLIENT MODULE

The client module consists of three components. Access control component, splitting and merging encryption decryption components. How each component works is explained separately (Hogan 2011).

3.1 ACCESS CONTROL CLIENT COMPONENT

The access control component authenticates and authorizes the cloud user. The simplest authentication mechanism is a username and password. However, this is too weak an authentication method for the cloud Calculation. The user logs in with their user data (username, password) and cloud access control. The component randomly generates a password for two sessions. One is sent to the user's official email address and the other to the user's mobile phone number. These two session passwords can be used to authenticate the user. After authentication is complete, the access control module takes a backseat and the rest of the data access and storage is done by splitting and combining and encrypting and decrypting components (Iftekhar et. al. 2021; Rouhani et. al. 2021).The permission model shown in figure 2 (Rouhani et. al. 2021).

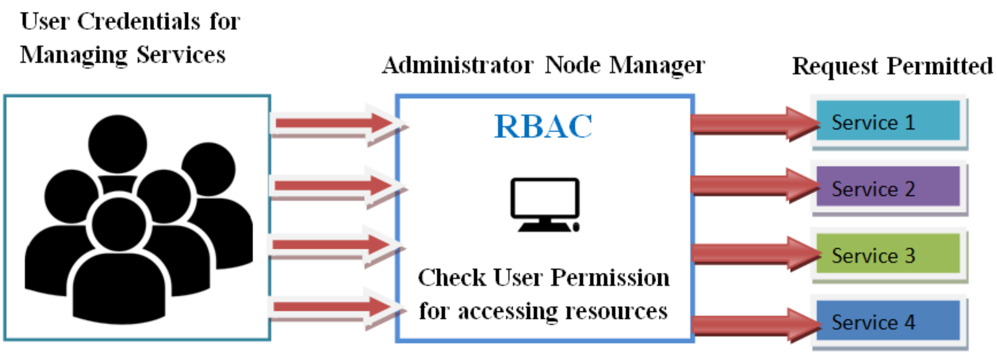
User Credentials for Managing Services
Administrator Node Manager
Request Permitted
RBAC
Check User Permission for accessing resources
Service 1
Service 2
Service 3
Service 4

Figure 2: RBAC Role Based Access Control Permission Model (Rouhani et. al. 2021)

3.2 SPLITING AND MERGING COMPONENT

After authentication, the user gets access to the cloud storage. When the client wants to send data, the data is first divided by division using the division algorithm. The data can be extracted and a fusion algorithm is used to display the original form of the data. The split algorithm divides the data into even and odd bits of information, and then the merge algorithm reverses the process (Wang et. al. 2021).

3.3 COMPONENT OF ENCRYPT AND DECRYPT

After the data has been split by the split and merge component, it is dispatched to the encryption/decryption component. An encryption/decryption component after applying AES encryption methods that send encrypted data to cloud storage. A server in which the data is saved or stored in the public storage server component and the key is in the personal data component. The same mechanism is used when retrieving data from memory. The key is taken from the private data component and the data from the public data component is returned to the split and merge component after the data is decrypted using the merging algorithm to create the original data (Dinesh & Krishna 2022; Gill et. al. 2022; Abdulsalam & Hedabou 2022). Encryption and Decryption Architecture model shown in figure 3 (Gill et. al. 2022; Abdulsalam & Hedabou 2022).

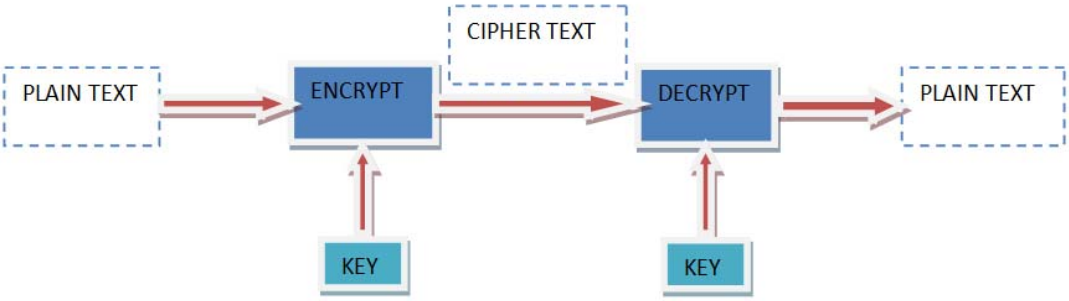

Figure 3: Encryption and Decryption Architecture (Gill et. al. 2022; Abdulsalam & Hedabou 2022)

3.4 THE SERVER MODULE

The cloud server module in our architecture also consists of three components. These components include Authentication component, identity component and public data component. How it works The components are explained as follows (Pivoto et al. 2021).

3.5 AUTHENTICATION COMPONENT

The authentication component functions with the identity component of the server module very closely. When the server receives a data access authorization request, the authentication module must randomly generate two session passwords and send one of them to the user's official email account and the other to the mobile phone number. The user is then authenticated after verifying the user's session passwords (Ibrahim et al. 2022).

3.6 PRIVATE DATA COMPONENT

The Personal Data component is not only responsible for storing user access data (login information). However, it is also responsible for storing the private keys needed to decrypt the data store in the public area of the cloud storage. Only the owner of the data can access the personal data section of the cloud storage and perform operations such as updating, deleting and adding data. The user cannot perform operations with data in the field of personal data (Reis et al. 2021).

3.7 PUBLIC DATA COMPONENT

A public bean stores data that is shared among all authorized users of specified data. All data stored in the public data area is available in encrypted form. Owners not only for this creation of data in this component, but also for various data operations (Reis et al. 2021).

4. SECURITY ISSUES AND CHALLENGES IN CLOUD COMPUTING

Cloud computing comes with some critical security threats. If mismanaged, businesses can suffer leaks and data leakage. Cloud computing is comparatively more flexible and it also saves the cost as it enables the employees/users to remotely have an access to data. The benefits of cloud computing are backed by the literature too. However, the concerns pertaining to security are more elusive. Verily, a third party mobility of the data has some potential threats in itself (Shaikh & Meshram 2021; Ahmad et al. 2022).

4.1 UNAUTHORIZED ACCESS

The ability to deploy functionality as needed through self-service capabilities improves the efficiency of launching PaaS and SaaS products. However, this has the potential to heighten the possibility of unauthorized use. Organizations that do not take assistance from IT department, and when the users of that organization use some services and other applications without taking a green signal from IT department are at an increased risk of cybercrimes (Shaikh & Meshram 2021).

4.2 REDUCED VISIBILITY AND CONTROL

A decision to move towards a cloud computing model may result in organizations losing a considerable amount of control and visibility, and some policy and infrastructure responsibility shifts to the cloud service provider. Unauthorized access, data replication and mishandling can lead to problems with data protection in the cloud and may also minimize the efficacy of security controls. The execution of strategies related to responding the incidents in order to locate the unusual activity on the part of user can assist in mitigating such risks. The issue that most of the organizations face while using cloud computing is the limited amount of visibility (Shaikh & Meshram 2021).

4.3 UNSECURE APIs AND INTERFACES

APIs as well as interfaces that lack security may aggravate the issues of cloud computing. The importance of APIs for individualized communication is vital, but simultaneously they possess a potential threat. Companies are enabled by APIs to customize the cloud functions as per their needs. Apart from that, APIs also possess the facility to encrypt data, access it and discover it if the need be (Shaikh & Meshram 2021).

4.4 SYSTEM VULNERBILITIES

Since the infrastructure of cloud networks is intricate, and since it is also handled by a third party, the systems are at an increased risk of experiencing vulnerabilities. Hackers may make their most by hunting on the loopholes left by the systems. Operating systems that have not been secured or the storages that have been unguarded always potentially remain on the verge of a major data theft or a security breach (Shaikh & Meshram 2021; Ahmad et al. 2022).

Users feel comfortable sharing data in cloud but the danger to leaked or lost data always looms (Shaikh & Meshram 2021). Cloud facilitates smooth data storing, but it also puts data online, therefore a danger of data being stolen or leaked always lurks. Invitations links or emails facilitate data sharing or data exchange, and hence they remain available to malicious entities or hackers (Ahmad et al. 2022).

4.5 DATA BREACHES, LOSS, OR LEACKAGE

Users feel comfortable sharing data in cloud but the danger to leaked or lost data always looms (Shaikh & Meshram 2021). Cloud facilitates smooth data storing, but it also puts data online, therefore a danger of data being stolen or leaked always lurks. Invitations links or emails facilitate data sharing or data exchange, and hence they remain available to malicious entities or hackers (Ahmad et al. 2022).

4.6 MALICIOUS INSIDERS

Companies also face threats related to cyber security from inside the organization too. Verizon's 2020 Data Breach Investigation Report highlighted that as many as 30% breaches in data were an inside job (Ahmad et al. 2022).

4.7 MISCONFIGURATION

If a cloud's infrastructure is configured in a wrong way, it may also result in the leakage of data. If a company does not configure properly, its data and other related applications might come under a threat of cyber-attack (Shaikh & Meshram 2021; Ahmad et al. 2022).

4.8 CYBERATTACKS

Attackers and criminals related to cybercrimes keep improving their linking and hacking capabilities, and they become aware of the prime targets in no time (Ahmad et al. 2022).

4.9 HIJACKING OF ACCOUNTS

Keeping weak passwords, many people increasingly become an easier target for phishing attacks or they become vulnerable to losing their data with the help of stolen passwords or breached security (Shaikh & Meshram 2021). In the world of cloud computing, hijacking of accounts has always been a gnawing and most obnoxious concern as the reliance on cloud computing has increased over the years to run business related affairs (Ahmad et al. 2022).

5. CONCLUSION

Cloud computing has experienced a paradigm shift when it comes to leveraging existing technologies. Incline's cloud services appear to be gaining traction as part of society especially these days. The cycle of introducing new technological innovations is getting shorter and shorter. For many purposes, including reducing capital costs, the use of cloud services should be considered an integral part of the investment. In any case, several issues impede broad deployment and layers of detection. The main drawback of current cloud service implementations is their inability to provide high levels of security. In addition, a security requirement is required to cover transmission paths involving a third party. In order to improve the use of cloud services, many aspects need to be improved to ensure a high level of security, privacy, authenticity, integration, speed, scalability and reliability. Perhaps an automated service level agreement, a third-party trustee, or a new extension will be an exciting area of research that will cover the security issues associated with cloud computing.

REFERENCES

Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: technical review. Future Internet, 14(1), 11.

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in iot-based cloud computing: A comprehensive survey. Electronics, 11(1), 16.

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in iot-based cloud computing: A comprehensive survey. Electronics, 11(1), 16.

Bharathi, P., Annam, G., Kandi, J. B., Duggana, V. K., & Anjali, T. (2021, July). Secure file storage using hybrid cryptography. In 2021 6th International Conference on Communication and Electronics Systems (ICCES) (pp. 1-6). IEEE.

Devarakonda, E. K. (2021). An Acceptable Cloud Computing Model for Public Sectors (Doctoral dissertation, Walden University).

Dinesh, K.V., & Krishna, N.G. (2022). Cloud computing and its variable techniques in obtaining data. Journal of Engineering Sciences, 13(1), 11-18. https://jespublication.com/issue.php?cid=24&scid=78

Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., Haq, I. U., Jhanjhi, N., ... & Masud, M. (2022). Security and privacy aspects of cloud computing: a smart campus case study. Intell. Autom. Soft Comput, 31, 117-128.

Golec, D., Strugar, I., & Belak, D. (2021). The Benefits of Enterprise Data Warehouse Implementation in Cloud vs. On-premises. ENTRENOVA-ENTerprise REsearch InNOVAtion, 7(1), 67-76

Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011). Nist cloud computing standards roadmap. NIST Special Publication, 35, 6-11.

Holzner, S., & Conner, N. (2009). Google docs 4 everyone. FT Press.

Ibrahim, M., Mohamed, B., & Hassan, M. F. (2022). An adaptive authentication and authorization model for service-oriented enterprise computing. Kuwait Journal of Science, 49(1).

Iftekhar, A., Cui, X., Tao, Q., & Zheng, C. (2021). Hyperledger fabric access control system for internet of things layer in blockchain-based applications. Entropy, 23(8), 1054.

Koltyukova, V. (2021). EDGE-CoT: next generation cloud computing and its impact on business (Doctoral dissertation).

Lindholm, S. (2021). Facebook as a tool to integrate: A qualitative-and quantitative historically contextual analysis of the use of Facebook among international students at Stockholm University in 2011–and how they use it 10 years later in 2021.

Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences, 33(7), 810-819.

Mahmood, S. (2013). Online social networks: Privacy threats and defenses. In Security and Privacy Preserving in Social Networks (pp. 47-71). Springer, Vienna.

Mohammad, A. S., & Pradhan, M. R. (2021). Machine learning with big data analytics for cloud security. Computers & Electrical Engineering, 96, 107527.

Nimmy, S. F., Hussain, O. K., Chakrabortty, R. K., Hussain, F. K., & Saberi, M. (2022). Explainability in supply chain operational risk management: A systematic literature review. Knowledge-Based Systems, 235, 107587.

Phan, A., Seigfried-Spellar, K., & Choo, K. K. R. (2021). Threaten me softly: a review of potential dating app risks. Computers in human behavior reports, 3, 100055.

Pivoto, D. G., de Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. Journal of Manufacturing Systems, 58, 176-192.

Reis, L. H., de Oliveira, M. T., Mattos, D. M., & Olabarriaga, S. D. (2021, June). Private Data Sharing in a Secure Cloud-based Application for Acute Stroke Care. In 2021 IEEE 34th International Symposium on Computer-Based Medical Systems (CBMS) (pp. 568-573). IEEE.

Rouhani, S., Belchior, R., Cruz, R. S., & Deters, R. (2021). Distributed attribute-based access control system using permissioned blockchain. World Wide Web, 24(5), 1617-1644

Sarder, M. D., & Haschak, M. (2019). Cyber security and its implication on material handling and logistics. College-Industry Council on Material Handling Education, 1-18.

Shaikh, A. H., & Meshram, B. B. (2021). Security issues in cloud computing. In Intelligent Computing and Networking (pp. 63-77). Springer, Singapore.

Sharma, A. (2021). A comprehensive study of cloud computing security. Asian Journal of Multidimensional Research, 10(10), 549-557.

Singh BG, S., & Phulre, D. (2021). Detail Study of Cloud Infrastructure Attacks and Security Techniques. International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN, 2347-5552.

Walzberg, J., Burton, R., Zhao, F., Frost, K., Muller, S., Carpenter, A., & Heath, G. (2022). An investigation of hard-disk drive circularity accounting for socio-technical dynamics and data uncertainty. Resources, Conservation and Recycling, 178, 106102.

Wang, H., Zhang, Y. L., Han, D. D., Wang, W., & Sun, H. B. (2021). Laser fabrication of modular superhydrophobic chips for reconfigurable assembly and self-propelled droplet manipulation. PhotoniX, 2(1), 1-13.