IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.301

Volume 3, Issue 8, May 2023

A Review of the Problem with Cloud Data Security and the Current Countermeasures in Cloud Computing

Mr. Sharan L Pais, Koushik Achar, Krupashree R, Laya R, Manikanta

Alvas Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *One of the computer systems that is developing the fastest is cloud computing (CC). This is the necessary user administration without the need for specific and direct user administration for network resources, primarily information storage. A single platform is offered by CC, a grouping of public and private data centres that serve customers online. The use of the cloud for purposes other than just data storage and processing at cloud assets is required due to the increasing amount of private and sensitive information obtained by supervisory authorities. Sensitive data should not be sent to public clouds, however, due to security concerns brought up by recent data breaches. This document offers a thorough analysis of the study on issues with data encryption, data obfuscation, and data protection, as well as solutions for cloud data storage. Examined are the most recent methods and technologies for cloud data protection. This study also looks at a number of contemporary approaches to cloud security issues. The effectiveness of each strategy is then contrasted based on its traits, advantages, and drawbacks.***

Keywords*:* Cloud

I. INTRODUCTION

Cloud computing (CC) is an innovative idea that allows customers to store data remotely in the cloud for a variety of applications. Companies are migrating some of their computer infrastructure to the cloud, with benefits such as unlimited data storage capacity, easily accessible, secure document availability, and cheap cost of use. Personal cloud storage provides public cloud services, while mutual cloud is ideal for financial and medical industries

Despite the fact that cloud storage has been around for a while, it is still essential for the Internet of Things, smart communities, and electronic commerce. We wrote this report because of how important data security and private preservation are for cloud storage. Give a thorough analysis of the study on issues concerning data security and privacy, data encryption methods, and cloud storage system solutions. The article's main topics are as follows:

To thoroughly examine strategies for using cloud storage systems, issues with data privacy and security, etc.

An overview of data encryption technology and security measures is given. The need for protection has already been emphasised.

Before you finish, review a few common data protection study concerns relating to cloud storage.

II. PROTECTION REGARDING CLOUD SECURITY

- **Data Confidentiality:** Data confidentiality protects customer information from unwelcome parties and ensures accuracy and consistency with the data provided by the transmitter.
- **Data Integrity:** Data integrity is essential for protecting our privacy, as it cannot be changed or replaced.
- **Data accessibility:**Data accessibility, Access Control, and Full Data Deletion enable users to access, upload, and alter information from the cloud at any time.
- **Privacy protection:** Cloud storage providers use privacy security approaches to protect data from malicious agents and interested third parties. However, as the information age progresses, current data security solutions will no longer be adequate and safety worries will become a bigger barrier to digitalization. Data loss, data breaches, data manipulation, denial of service, and other security vulnerabilities affect safe data storage.

DOI: 10.48175/IJARSCT-10299

III. PRESENT SAFETY SOLUTION

As soon as data is moved to the cloud, its security is jeopardised. Data protection may be achieved with the use of encryption. The goal of encrypting data is to employ methods to change a plaintext file or piece of information into an unknown code sequence, or ciphertext. The unique content will be impossible for someone to interpret once they hijack the scrambled message, successfully preserving the data's privacy and avoiding tampering. Those who have access can modify the ciphertext and decode the data using the corresponding private key. The data security procedure in a cloud environment is shown in Figure 1.

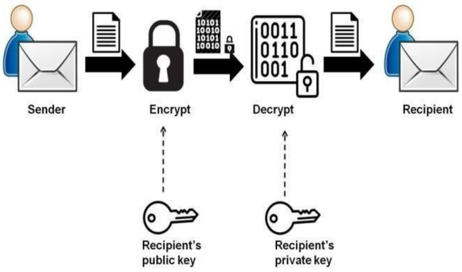

Figure 1. Data Security Process in Cloud

Crypto encryption and asymmetric encryption are two encryption techniques that use a private key to encrypt and decode data. Symmetric encryption requires a consensus key, while public key encryption involves two keys, one for encryption and one for decoding. Public key encryption is more effective as it requires a public key toencode and decrypt the data.

3.1 Cryptography Based On Identity(IBE)

IBE is a public key technique where a private key generator creates a master key pair and private key linked to the user's identity.

3.2 Model With Roles

The data owner encrypts the data locally and stores it in the cloud, while consumers have responsibilities and tasks assigned to them. Roles are assigned based on duties and requirements, and if not assigned, they won't be allowed to access the data.

3.3 Encryption Based On a Attributes (ABE)

Attribute-based encryption involves a combination of characteristics for both encryption and decryption, with the data owner using the customer's public key and the customer's private key to decode the message. It has two advantages: it lowers the cost of internet connections and offers fine-grained permissions, but requires the data owner to use the authorised user's public key.

IV. CLOUD SECURITY

Cloud computing is a popular way for businesses to access data and software applications, but it also has its own security concerns. Security is a major concern, as it combines a wide range of technologies such as networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control, and memory management. Access data is no longer compromised by the loss of a client system in a cloud-based software environment, and the availability of lightning-fast processing power, access to storage, and ease of use all provide amazing benefits for communication. As 69% of all businesses now use cloud computing, Washington, D.C. Most internet Americans use webmail services, online data storage, or both. Cloud computing also poses a number of security concerns, such as the network that connects a cloud's systems having to be secure, data security including encrypting data and making sure the proper guidelines are observed for data sharing, and algorithms used to allocate resources and manage memory being safe.

DOI: 10.48175/IJARSCT-10299

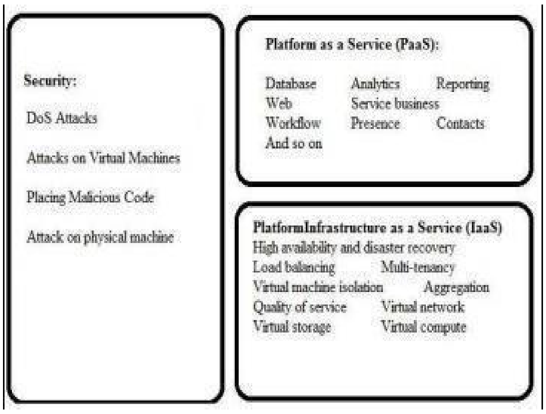

Figure 2.cloud Security View

4.1 Problem with Malware Injection

The most important details of the phrases web browser, significant chance, attacker, system, and web are that once the client's request is processed in the cloud system, there is a significant chance that Meta data will be sent between the web server and web browser. This metadata exchange can be exploited by an attacker, who may attempt to intrusion with malicious code or create their own instance.

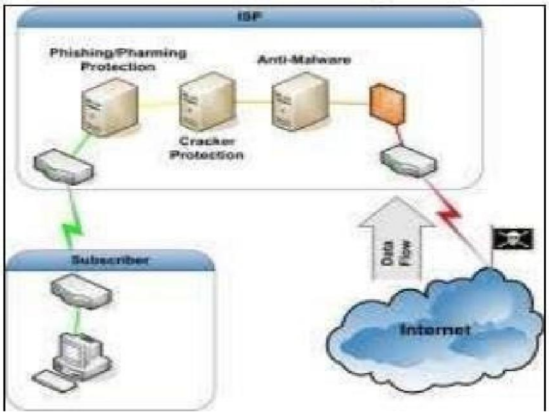

Figure 3. Malware Protection

4.2 The Flooding Attack Issue

A cloud system is a system where each compute server performs a specialised function and communicates with the others inside. When a server is overworked or has reached the threshold limit, it offloads part of its tasks to a nearby server. This sharing strategy allows an attacker to easily produce fake data and pose requests to the cloud server after they have obtained the authorisation to make a request. The server verifies the legitimacy of the requested jobs before executing them and sends them to another server to avoid having to evaluate illegitimate requests. This can lead to system flooding as the enemy can intervene again by stopping one server's routine operations.

4.3 Problem with Accountability Checks

The cloud system's payment approach is "No Use No Bill" and the length of the instance, quantity of network data transmission, and the number of CPU cycles used by each user are all noted when a client runs an instance. The legitimate account holder is charged for this type of calculation when an attacker uses the cloud with a harmful service or executes malicious code, which uses a lot of computing resources and storage from the cloud server.

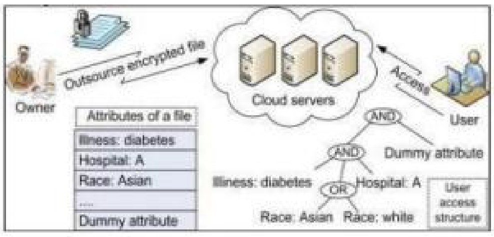

Figure 4 .an example for attributes-based encryption

Cloud providers must ensure that cloud computing environments meet security and privacy requirements, protect data and applications, and demonstrate efficacy in moving corporate data and functions.

4.4 Privacy

Privacy is a major security concern with cloud computing, as personal information is governed by various laws and some countries forbid data storage outside of their borders. Data may be stored within specific countries for privacy legislation based on contractual obligations. Companies must develop privacy and security guidelines for cloud services, and all related security and legal issues, such as data protection, compliance, privacy, and identity management, must be addressed.

4.5 Security of Data Transmission

Encryption methods are used during data transmission to ensure the confidentiality and integrity of data stored in a cloud provider's resources. SSL/TLS algorithms are used to process this data, while homomorphism encryption is used to decrypt it. Man-in-the-middle attacks can be used to prevent unauthorized access.

V. CHALLENGES OF CLOUD COMPUTING

Users can utilise computing power that is greater than what is available in their physical environment in the world of cloud computing. A user must transfer data throughout the cloud in order to access this virtual world. Several security issues consequently emerge.

5.1 . Assurance of Information

Protecting the security, Integrity, and availability of data is a worry regardless of the form that the data may take.

- **Loss of data control:** Outsourcing can cause a loss of data control, so large institutions avoid using cloud-based software. Amazon Simple Storage Service (S3) APIs provide both bucket- and object-level access controls with settings that only permit authenticated access by the bucket and/or object creator. To ensure data privacy, a user must be authenticated using an HMACSHA1 signature of the request using the user's private key, maintaining total control over who has access to their data.
- **Issue with Compatibility:** Cloud providers often build "sticky services" that conflict with each other, making it difficult for customers to switch. Amazon and Microsoft seek interoperability.
- **Failure of the Provider's Security**: Provider security is more important than customer security for small and medium-sized companies, as it is difficult to ensure the correct things are being done.
- **Cloud Provider Fails**: The customer is facing a potential bankruptcy, an outage, or a loss of access to their production systems due to other businesses' actions. The organisation in charge of subscriber data runs the additional risk of not protecting it to the service standards. To ensure that any data can be recovered, users can select a second provider and use automated, routine backups with open source and paid solutions.

VI. SECURITY CONCERNS

In a virtualized system, security is more difficult to manage because you now need to keep track of both the real host security and the virtual machine security. If the security of the real host server is compromised, it will have an impact on all of the virtual machines located on it. Furthermore, a compromised virtual machine could wreck chaos on the host server, which would then adversely affect all other virtual machines using that host.

Host Operating System: To access hosts designed specifically for administration, administrators who have a business need to access control plans must use multi-factor authentication. These administrative hosts are computers that have been fortified, constructed, set up, and designed specifically to protect the cloud administration plane. Audits and records of each of these entries are kept. When an employee no longer needs access to the administration plane for workrelated purposes, the rights and access to those hosts and relevant systems are revoked. **Guest Operating System:** AWS advises customers to follow security best practices, such as disabling password-based access, using multi-factor authentication, and using a privilege escalation method with user specific logging. Clients should also make their own key pairs.

VII. A GUIDE TO CLOUD COMPUTING SECURITY STANDARDS

Security standards define the steps to maintain a secure environment that provides privacy and security of sensitive information in a cloud environment. Protection in depth, or multiple layers of protection, is a fundamental tenet of security. Cloud computing is seeing this kind of layered protection emerge due to managed security services provided by cloud providers.

Scripting Language for Security

- **Assertions:** SAML is an XML-based standard used to share attribute, authentication, and authorization data between online partners, allowing businesses to securely assert a principal's rights and identity. An email address can be used to symbolise an object in a domain
- **Open Authentication:** OAuth is an open protocol that makes secure API authorization simple and standardised for web applications. It protects login information for developers, gives consumers access to their data, and allows users to share information without revealing their identities.
- **OpenID:** OpenID is a free, open-source standard for managing individual access. It allows users to login into a variety of services with a single sign-on device. The OpenID protocol is based on a specific URL verified by the organization that hosts the OpenID URL. It does not require a specific sort of authentication, including conventional authentication methods or nonstandard ones like smart cards.

VIII. CONCLUSION

In this study, a thorough evaluation of data security and privacy preservation for cloud services is given. First and foremost, cloud technology and cloud storage will continue to dominate due to their significant impact on the digital world, corporate digitalization, Internet of Things, and some other sectors. Examine the existing security solutions before analysing the requirements for data protection in relation to cloud storage. Additionally, methods for data obfuscation for cloud storage were outlined. As a tabular formation regarding security threats, cloud security issues and solutions were displayed.

REFERENCES

[1]. Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues,Threats, and solutions. The journal of supercomputing, 76(12), pp.94939532.

[2]. Rambabu, M., Gupta, S. and Singh, R.S., 2021. Data mining in cloud computing: survey. In Innovations in Computational Intelligence and Computer Vision (pp. 48-56). Springer, Singapore.

[3]. Abroshan, H., 2021. A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, 12(6).

[4]. Challagidad, P.S. and Birje, M.N., 2020. Efficient multi-authority access control using attribute-based encryption in Cloud storage. Procedia Computer Science, 167, pp.840-849.

[5]. N. Thangarasu, R. Rajalakshmi, G. Manivasagam, & V. Vijayalakshmi. (2022). Performance of re-ranking Techniques used for recommendation method to the user CF- Model. International Journal of Data Informatics and Intelligent Computing, 1(1), 30–38. https://doi.org/10.5281/zenodo.7108931

[6]. Saxena, R. and Gayathri, E., 2021, October. A study on vulnerable risks in security of cloud computing and proposal Of its remedies. In Journal of Physics: Conference Series (Vol. 2040, No. 1, p. 012008). IOP Publishing.

[7]. Sultan, N.H., Varadharajan, V., Zhou, L. and Barbhuiya, F.A., 2020. A rolebased encryption scheme for securing Outsourced cloud data in a multiorganization context. arXiv preprint arXiv:2004.05419.

[8]. A. Koulouzis, S., Martin, P., Zhou, H., Hu, Y., Wang, J., Carval, T., Grenier, B., Heikkinen, J., de Laat, C. and Zhao, Z., 2020. Timecritical data management in clouds: Challenges and a Dynamic Real-Time Infrastructure Planner (DRIP) solution. Concurrency and Computation: Practice and Experience, 32(16), p.e5269.

[9]. Unal, D., Al-Ali, A., Catak, F.O. and Hammoudeh, M., 2021. A secure and efficient Internet of Things cloud Encryption scheme with forensics investigation compatibility based on identitybased encryption. Future Generation Computer Systems, 125, pp.433-445.

[10]. Yang, P., Xiong, N. and Ren, J., 2020. Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, pp.131723-131740.

DOI: 10.48175/IJARSCT-10299