IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

Data Security and Privacy in Cloud Computing

Mr. Pradeep Nayak[1], Ravindra Reddy[2], Suraj S Ankolekar[3], Mohan Raju V[4], C H Rakesh[5]
Assistant Professor, Department of Information Science and Engineering[4]
Students, Department of Information Science and Engineering[1,2,3,5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *Information technology has frequently faced serious problems with data security. Because the data is dispersed throughout the globe in the cloud computing environment, it becomes especially serious. The two main reasons users have privacy and data security concerns with cloud technology are data security and privacy protection. Data security and privacy protection are becoming more crucial for the future growth of cloud computing technology in government, industry, and business, even if numerous techniques on the issues of cloud computing have been researched in both academics and industries. Both the hardware and the software in the cloud architecture are affected by difficulties with data security and privacy protection. This study intends to improve data security and privacy protection for a reliable cloud environment by reviewing various security strategies and difficulties from both software and hardware sides for securing data in the cloud. We conduct a comparative research analysis of the literature related to the data security and privacy protection methods utilised in cloud computing in this paper.*

Keywords: Cloud computing, privacy, SaaS, PaaS, IaaS, data security

I. INTRODUCTION

The upcoming paradigm in computation has been identified as cloud computing. Applications and resources are both made available online as services in the cloud computing environment. The term "cloud" refers to an environment made up of hardware and software resources in data centres that offer a variety of services across a network or the Internet to meet user needs.

The National Institute of Standards and Technology (NIST) defines "cloud computing" as the ability to have universal, convenient, on-demand network access to a shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with little management work or service provider interaction. The explanation claims that cloud computing offers convenient on-demand network access to a pool of shared, programmable computing resources. Applications for computers, network resources, platforms, software services, virtual servers, and computing infrastructure are all examples of resources.

A new computing typology that can offer services on demand and at a low cost is cloud computing. In the cloud paradigm, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service are the three well-known and often utilised service models (IaaS). In SaaS, a cloud service provider deploys software with the necessary data and makes it accessible to consumers via web browsers. With the help of a collection of software tools that can handle activities, a service provider facilitates services for consumers in PaaS. In IaaS, the cloud service provider provides consumers with storage and virtual computers to enhance their business capabilities.

Grid computing and cloud computing are closely connected; however, they are not the same. While cloud computing combines computing and storage resources controlled by various operating systems to offer services like large-scaled data storage and high-performance computing to users, grid computing integrates diverse resources together and controls the resources with a single operating system. Cloud computing has altered the general landscape of grid computing. When compared to grid computing, the cloud computing method of data distribution is novel.

Cloud computing will make it simple to use services on demand. On-demand self-service, omnipresent network connectivity, location-independent resource pooling, quick resource flexibility, usage-based pricing, and risk transference are some aspects of cloud computing. These benefits of cloud computing have sparked a lot of attention from both the business and academic research communities. The world of business is currently changing due to cloud computing technologies.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

Although cloud computing holds great promise for IT applications, there are still several issues that need to be resolved before businesses and individual users may store data and instal apps in a cloud computing environment. Data security has frequently been a significant problem in IT. Because data are dispersed over several machines and storage devices, including servers, PCs, and other mobile devices like wireless sensor networks and smart phones, data security becomes a particularly critical issue in the cloud computing environment. In comparison to traditional information systems, data security in the cloud is more difficult.

Consumer's security concerns need to be addressed in order to make the cloud environment trustworthy before users and businesses utilise cloud computing. The fundamental condition for gaining consumer's trust and getting them to use such a technology is a trustworthy environment. Talked on rating cloud computing hazards. Computing and data storage are the two fundamental types of services offered by cloud computing environments. Customers of cloud services do not require anything to use the cloud computing environment; all they need is Internet connectivity to access their data and complete their computing chores.

Clients do not even know where the data are kept or which machines are doing the processing during data access and computation. Security, administration, and monitoring of resources are three of the main problems with cloud computing. There are currently no established guidelines or criteria for deploying apps in the cloud, and there is no standardisation of control. Numerous cutting-edge methods have been developed and put into use in the cloud, however owing to the dynamics of the environment, these methods cannot guarantee complete security.

In this essay, we will examine several security measures as well as issues related to protecting data storage security and privacy in a cloud computing environment. This study gives a comparative research review of the prior research on cloud computing solutions through data security issues such as data integrity, confidentiality, and availability. Because data privacy is typically associated with data security, cloud technologies and data privacy problems are also explored. By protecting data in the cloud computing environment, comparative studies on data security and privacy might assist to increase consumer confidence.

II. DATA INTEGRITY

One of the most important components of any information system is data integrity. Protecting data from unlawful erasure, alteration, or fabrication is the general definition of data integrity. The admission and rights of the managing entity to certain corporate resources ensure that priceless information and services are not misused, misappropriated, or stolen.

In a standalone system with a single database, data integrity is simply attained. Database constraints and transactions are used to preserve data integrity in the standalone system. which a database management system typically completes (DBMS). To maintain data security, transactions should adhere to the ACID (Atomicity Consistency Isolation Durability) principles.

The usage of authorization is used to regulate data access. It is the process by which a system chooses the level of access that a certain authorised user should have to the system's secure resources. In a cloud system, maintaining data integrity involves protecting information integrity. Unauthorized users should not lose the data or alter it. The foundation for offering cloud computing services like SaaS, PaaS, and IaaS is data integrity.

In addition to large-scale data storage, cloud computing environments typically offer data processing services. Techniques like digital signatures and RAID-type schemes can be used to ensure data integrity.

In a cloud context, where there are many different entities and access points, permission is essential to ensuring that only authorised parties may interact with data. Organizations may boost their trust in the integrity of their data by preventing illegal access. It is expected of cloud computing companies to uphold data accuracy and integrity. However, in addition to consumers and cloud service providers, a third-party oversight system must be developed.

The prerequisite for deploying apps is to remotely check the accuracy of data in the cloud. By combining error correcting code with spot-checking, present the theoretical framework "Proofs of Retrievability" to achieve remote data integrity verification. The HAIL system employs the POR process to examine how data is stored across many clouds. It can guarantee the redundancy of various copies and carry out availability and integrity checks. To validate the data integrity remotely, trusted platform module (TPM) remote checking is suggested.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

III. DATA CONFIDENTIALITY

For consumers to save their private or confidential data in the cloud, data confidentiality is crucial. Data confidentiality is guaranteed using authentication and access control techniques. By improving cloud reliability and trustworthiness, the difficulties with data confidentiality, authentication, and access control may be resolved Customers should avoid directly storing their sensitive data in cloud storage since users do not trust cloud providers and internal threats are nearly difficult to eradicate for cloud storage service providers.

Simple encryption cannot fulfil complicated needs like inquiry, concurrent modification, and fine-grained authorisation due to the key management issue.

3.1 Homomorphic Encryption

Typically, encryption is employed to protect data's secrecy suggested a particular type of encryption system called homomorphic encryption. Additionally, the whole method avoids the need to decrypt the data since it assures that the results of the cypher text algebraic operation are compatible with those of the clear operation following encryption.

The secrecy of data and data activities in the cloud may be resolved by the application of this technology. First put out by Gentry, the completely homomorphic encryption approach is capable of performing any operation possible in plain text without the need for decryption. It represents a significant advance in homomorphic encryption technology.

However, the encryption scheme requires extremely complex calculations, therefore processing and storage are quite expensive. This results in the completely homomorphic encryption being far from having practical uses.

3.2 Encrypted Search and Database

For safe communication, the Diffie-Hellman cryptographic technique is suggested, which is considerably different from the key distribution management system. A hybrid approach that incorporates several encryption techniques including RSA, 3DES, and random number generator has been presented for more flexibility and security. While 3DES is particularly helpful for block data encryption, RSA is effective for establishing secure communication connections through digital signature-based authentication. Additionally, several encryption techniques are explored in order to guarantee the security of user data in cloud computing. and the keys on their own. The fact that this method's delays result from additional communication with the central synchronizer is a drawback. By using group encryption and reducing communication between nodes and the synchronizer, this constraint can be overcome.

For cloud-based databases, Huang and Tso presented an asymmetric encryption technique. The sequence of the public and private keys used for encryption and decryption is irrelevant in the proposed approach since commutative encryption is performed to data more than once. The proposed technique additionally employs a encryption process, demonstrating that the cipher-text data is encrypted once more for duality.

These programmes are extremely helpful in cloud applications where privacy is a major concern. A multikey word ranked search strategy that protects user privacy over encrypted cloud data was suggested, and it can rank the search results while still searching the encrypted cloud data.

3.3 Distributed Storage

A potential strategy in the cloud context is distributed data storage. Security concerns regarding to the data privacy in cloud computing, such as data integrity, intrusion, and service availability. One possibility for ensuring data integrity is to store data across several clouds or cloud databases. Shamir's secret procedure is used to create a polynomial function against each piece of the data that has to be safeguarded against internal or external unwanted access.

The network architecture, the unique pathways for incoming and outgoing traffic, and progressively adjusting the resource allocation in accordance with user demands form the foundation of the personalised measuring approach. The processing and storage resources are necessary for customised measurement, according to International Journal of Distributed Sensor Networks. The allocation of resources at a certain moment based on the customised active technique does not continue to be optimum due to the changeable nature of networks. The system must optimise changes in the user requirements, whether offline or online, and the resource connectivity since the resources may rise or decrease.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

3.4 Hybrid Technique

For data secrecy and integrity, a hybrid strategy that combines key-sharing and authentication methods is proposed. Strong key sharing and authentication procedures can increase the security of the connection between the user and the cloud service provider. The RSA public key technique may be used to distribute keys between users and cloud service providers in a safe manner.

The use of a three-layered data security technique is suggested. The first layer is used to verify the identity of the cloud user using one- or two-factor authentications; the second layer encrypts the user's data to ensure protection and privacy; and the third layer performs quick data recovery through a quick decryption process.

Critical data is isolated in the cloud using an event-based system.

3.5 Data Concealment

Another method for maintaining data secrecy in the cloud is data hiding. Delete and others a camouflage idea for database security was developed in. Data concealing techniques combine actual data with fictitious visual information to inflate the amount of genuine data. However, authorised users can quickly tell the difference between the true data and the phoney data. The volume of actual data is increased overall, but the security of the private data is improved. Making genuine data safe and secure from malevolent users and attackers is the goal of data hiding. A key for the genuine data may be provided via the watermarking technique. Only authorised users have access to the watermarking key, hence user authentication is essential to guarantee the authenticity

3.6 Deletion Confirmation

When people remove their data, deletion confirmation indicates that it cannot be retrieved. Data upon the confirmation of deletion. Because there are several copies in the cloud for data recovery ease and security, the issue is highly significant. All copies of the data should be erased simultaneously when users remove it with confirmation. There are, however, certain data recovery systems that can restore user-erased data from hard drives. Therefore, cloud storage providers should make sure that customers' erased data cannot be retrieved and utilised by other users who are not verified. Encrypting the data before uploading to the cloud storage space is one potential strategy for preventing its recovery and unauthorised usage. The FADE system is built on Ephemerizer-type technology. Before being uploaded to the cloud storage, data are encrypted in the system. When users want to delete their data, the system simply applies a certain approach to all available storage space so that new data may be added to replace the deleted data.

IV. DATA AVAILABILITY

Data availability refers to how much a user's data can be used or recovered in the event of an accident, such as hard disc damage, an IDC fire, or a network failure, as well as how the user can independently verify their data rather than relying solely on the cloud service provider's credit guarantee.

Since cloud suppliers are subject to local laws and cloud customers should be aware of such rules, the problem of storing data across transborder servers is a critical worry for clients. Additionally, the provider of cloud services should guarantee data security, notably data confidentiality and integrity. The cloud service provider should discuss all of these worries with the client and establish a rapport based on trust. Clients should be informed about the application of local regulations and given guarantees about the security of their data by the cloud vendor. The study primarily focuses on data difficulties and challenges related to cost, availability, and security, as well as the location and movement of data storage.

Users' faith in the cloud may be increased by finding data. Users can access transparent storage through cloud storage, which can reduce cloud complexity but also limit users' ability to manage their data storage.

On order to find the data stored in the Amazon cloud, Benson et al. analysed the evidence of geographic replication.

4.1 Reliable Storage Agreement

The most frequent anomalous behaviour associated with untrusted storage is the cloud service providers' potential to delete some of the user's update data, which is difficult to verify by relying just on basic data encryption. A good storage agreement must also let numerous users to modify data simultaneously.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

The Depot suggested by Mahajan can provide fork-join causal consistency and long- term consistency.
It can successfully fend off assaults like discarding and help the adoption of other safety safeguards in the dependable cloud storage environment (such as Amazon S3). Feldman presented SPORC, which makes advantage of the trusted cloud to offer secure real-time communication and collaboration for a number

4.2 Reliability of Hard-Drive

Currently, the primary storage medium in a cloud environment is a hard disc. Hard disc dependability creates the framework for cloud storage.
Based on historical hard-drive data, Pinheiro evaluated the error rate of hard drives. They discovered that, although having significant clustering features, the error rate of hard drives is not directly related to usage frequency or temperature.
The hard disc error rate could not be predicted by the current SMART technology, the relationship between soft mistakes and hard errors on hard discs, and they discovered that only around one-third of hard errors follow soft errors in a predictable manner.

V. DATA PRIVACY

The capacity for seclusion of a person or group is known as privacy.
Information about themselves or themselves, and hence expose only some of them. Following are the components of privacy.

- When: A person could be more anxious about information from the present or the future being exposed than information from the past
- How: While a person could feel at ease if his or her friends can manually seek information about them, the user might not want notifications sent out automatically and regularly.
- Extent: A user may want to have his or her information reported as a hazy area rather than a specific location.

Consumer context and privacy must be safeguarded and utilised correctly in trade. When it comes to managing personally identifiable information in businesses, regulations, procedures, standards, and practises must all be followed.
When users access sensitive data in the cloud, privacy implies that cloud services can stop prospective adversaries from determining the user's behaviour based on the user's visit model (not direct data leakage). Focus has been placed on the Oblivious RAM (ORAM) technology. ORAM technology visits several copies of the data to conceal the users' true visiting objectives. ORAM is a promising solution that has been utilised extensively in software protection as well as in cloud privacy security. as the most advanced implementation.
The privacy concerns vary depending on the cloud environment and may be broken down into four subcategories :

- The best way to provide consumers control over their data while it is stored and processed in the cloud while preventing theft, evil use, and illegal selling.
- How to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is a usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication.
- Who is in charge of upholding the legal standards for personal data.
- How far can cloud subcontractors be adequately recognised, vetted, and determined involved in processing.

5.1`Service Abuse

Service abuse refers to when an attacker uses a cloud service improperly to steal data or harm other users' interests Other users could misuse user information. As a result of the widespread usage of deduplication technology in cloud storage, it is frequently the case that users share the same data that has been saved just once. This will save cloud service providers money and minimise storage space requirements, but attackers still have access to the data if they know the hash code of the files being stored. The sensitive data might then be exposed on the cloud. Therefore, a proof of ownership technique has been suggested to verify cloud users' identities.
Attackers may result in a rise in cloud service costs. A type of attack on the cloud service payment is fraudulent resource use. Attackers may consume specific data to raise the price of cloud service subscriptions. This question was put out by Idziorek, who also conducted study on how to identify and detect fraud in the use of resources.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

5.2 Averting Attacks

Numerous shared resources are made possible by cloud computing on the Internet. Denial of Service (DoS) assaults should be able to be stopped by cloud computing platforms. The need for security services in cloud computing was examined by Shen. The authors recommend combining cloud services for trusted platform support services (TPSS) with trusted computing platform (TCP) (TSS). Confidentiality, dynamically creating trust domains, and dynamic of the services should all be features of the trusted model. Users must move their data onto cloud infrastructures only on the basis of trust. Neisse examined hypothetical assaults on the Xen cloud platform in order to assess cloud services based on trust. The key to cloud computing's widespread adoption is data security and consumer trust.

Yeluri examined security difficulties in the cloud when implementing the services with a focus on the cloud services from a security point of view. The main components for guaranteeing security in cloud computing include identity management, data recovery and management, confidentiality, trust, visibility, and application architecture.

5.3 Identity Management

A platform for using a variety of Internet-based services is provided by cloud computing. But in addition to its benefits, involving a reliable third party raises the security risk. Involving a dependable third party increases the possibility of user heterogeneity, which has an impact on cloud security. Using a trusted third party independent technique for Identity Management to use identity data on untrusted hosts might be one answer to this issue.

To stop data leakage and privacy loss in the cloud, many degrees of protection can be implemented. New business services that are based on demand are offered via cloud computing. Through the dynamic virtualization of hardware, software, and datasets, cloud networks have been created. The management of trust reputations and cloud security infrastructure is essential for improving cloud services.

VI. CONCLUSION

The newest and most promising technology for the next wave of IT applications is cloud computing. Data security and privacy concerns are a roadblock to the cloud computing industry's fast expansion. Any firm must reduce the cost of data processing and storage, and analysis of data and information is always the most crucial activity for decision-making in all enterprises. As a result, no companies will move their data or information to the cloud unless customers and cloud service providers have established a level of confidence.

Researchers have put out a variety of approaches for data protection and to achieve the maximum level of data security in the cloud. Making these methods more efficient will help to close many gaps, though. In order to cloud computing to be accepted by users of cloud services, more effort must be done in this area. In order to establish confidence between customers and cloud service providers, this study examined several methods for data security and privacy, with an emphasis on the storage and usage of data in the cloud.

REFERENCES

[1]. N. Leavitt, “Is cloud computing really ready for prime time?” Computer, vol. 42, no. 1, pp. 15–25, 2009.

[2]. P. Mell and T. Grance, “The nist definition of cloud computing,” National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009.

[3]. F. Berman, G. Fox, and A. J. G. Hey,Grid Computing: Making the Global Infrastructure a Reality, Volume 2, John Wiley and sons, 2003.

[4]. M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preserving audit and extraction of digital contents,” IACR Cryptology EPrint Archive, vol. 186, 2008.

[5]. Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[6]. N. Kshetri, “Privacy and security issues in cloud computing: the role of institutions and institutional evolution,” Telecommunications Policy, vol. 37, no. 4-5, pp. 372–386, 2013.

[7]. R. Latif, H. Abbas, S. Assar, and Q. Ali, “Cloud computing risk assessment: a systematic literature review,” in Future Information Technology, pp. 285–295, Springer, Berlin, Germany, 2014.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

[8]. A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic ˇ concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[9]. Z. Mahmood, "Data location and security issues in cloud computing," in Proceedings of the 2nd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT '11), pp. 49–54, IEEE, September 2011.

[10]. D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," in Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS '11), pp. 2852–2856, chn, August 2011.

[11]. A. Pandey, R. M. Tugnayat, and A. K. Tiwari, "Data Security Framework for Cloud Computing Networks," International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178– 181, 2013.

[12]. D. A. Klein, "Data security for digital data storage," U.S. Patent Application 14/022,095, 2013.