Secure Data Storage for the Database Services in Cloud Computing: A Comprehensive Review

Dr. D. V. Bhavsagar

Assistant professor,
Seth Kesarimal Porwal College of Arts, Science and Commerce,
Kamptee, Nagpur

***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. Despite the numerous advantages that cloud computing services offer, consumers are nonetheless quite concerned about the security of their data. 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. In this essay, we do a comparative review of the prior research on the methods for protecting users' privacy and data security in cloud computing.**

***Keywords*: Cloud Computing, Integrity, Confidentiality, Availability, Security issues, Privacy.**

I. INTRODUCTION

"There are several different definitions of cloud computing, but all of them agree on the way to provide services to users of the network. Cloud computing is an Internet-based development use of technology. It refers to the utilization of computing resources, hardware, and software, available on demand as a service over the web. It offers a variety of services for users of the network, like applications, storage, and various operations and remote printing, etc." [1]. "It typically involves over the web provision of dynamically scalable and sometimes virtualized resources" [2]. For customers to house their data, cloud administration providers give them a mirror image of a limitless amount of space. By transferring the near administrations framework to cloud servers, it provides customers with some assistance in lowering their financial overhead of knowledge administrations. Security concerns have, however, taken center stage in the decision to now source the potential for light data to cloud providers. When it comes to maintaining data security, one common practice is to encrypt information records before customers upload the disorganized data to the cloud.

A new computing typology that can offer services on demand and at a low cost is cloud computing. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are the three well-known and often utilized service models in the cloud paradigm (IaaS). In SaaS, a cloud service provider deploys software together with the necessary data, and customers utilize web browsers to access it. In PaaS, a service provider offers services to users through a collection of applications that can handle particular tasks. In IaaS, the cloud service provider offers storage and virtual computers to subscribers to help them run their businesses more efficiently.

In this article, we'll examine several security measures as well as issues related to protecting data storage security and privacy in a cloud computing environment. This paper gives a comparative research review of the prior research on cloud computing solutions through data security issues such as data integrity, confidentiality, and availability, as shown in Fig. 1. Because data privacy is typically associated with data security, cloud technologies and data privacy issues are also explored. By protecting data in the cloud computing environment, comparative studies on data security and privacy could serve to increase consumer confidence.

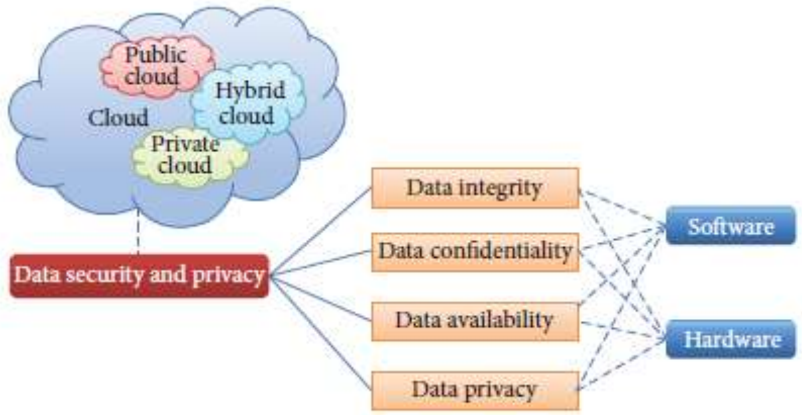

Fig. 1: Organization of data security and privacy in cloud computing

2. Data Integrity

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

3. Data Confidentiality

"For consumers to save their private or confidential data in the cloud, data confidentiality is crucial. Data confidentiality is guaranteed through the use of authentication and access control techniques. By improving cloud reliability and trustworthiness, the difficulties with data confidentiality, authentication, and access control may be resolved" [3]. Users should avoid directly storing their sensitive data in cloud storage since users do not trust cloud providers and internal threats are nearly impossible to eradicate for cloud storage service providers. Simple encryption cannot fulfil complicated requirements like inquiry, concurrent modification, and fine-grained authorization due to the key management issue.

4. 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 vendors are subject to local laws and cloud clients should be aware of such rules, the issue of storing data over transborder servers is a critical worry for clients. Additionally, the cloud service provider must guarantee data security, especially data confidentiality and integrity. The cloud service provider should discuss all of these worries with the client and establish a rapport based on trust.

5. Data Privacy

"Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively" [4]. Privacy has the following elements.

(i) When: a subject may be more concerned about the current or future information being revealed than information from the past.

(ii) How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

(iii) Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

6. Cloud Security Issues

A variety of cloud services, including IaaS, PaaS, SaaS, and models including public, private, and hybrid, are used by organizations. These models and services suffer from a number of cloud security problems. Every service model has some related problems. In order to ensure that the services they offer are secure and to manage consumer identification, security issues are first viewed from the perspective of the service provider. Customer perspective is another viewpoint that confirms the level of security of the service being used.

Insider Attacks

Cloud model is a multitenant based model that is under the provider's single management domain. This is a threat that arises within the organization. There are no hiring standards and providers for cloud employees . So a third party vendor can easily hack the data of one organization and may corrupt or sell that data to other organization.

Outsider Attacks

This is the one of the major concerning issue in an organization because it releases the confidential information of an organization in open. Clouds are not like a private network, they have more interfaces than private network. So hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking .These attacks are less harmful than the insider attacks because in the later we sometimes unable to identify the attack.

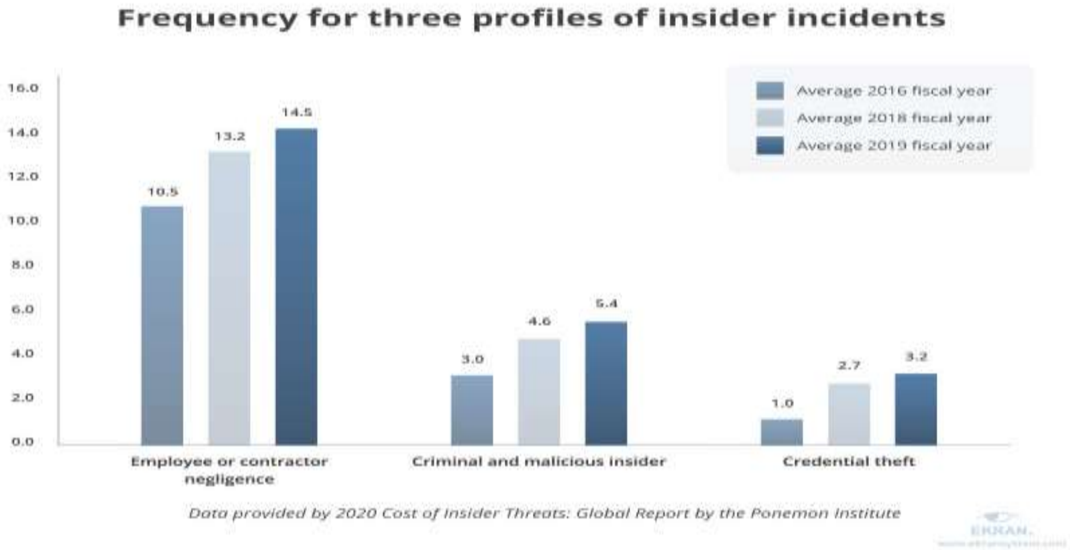

Fig.2: Frequency for three profiles of Insider Incidents

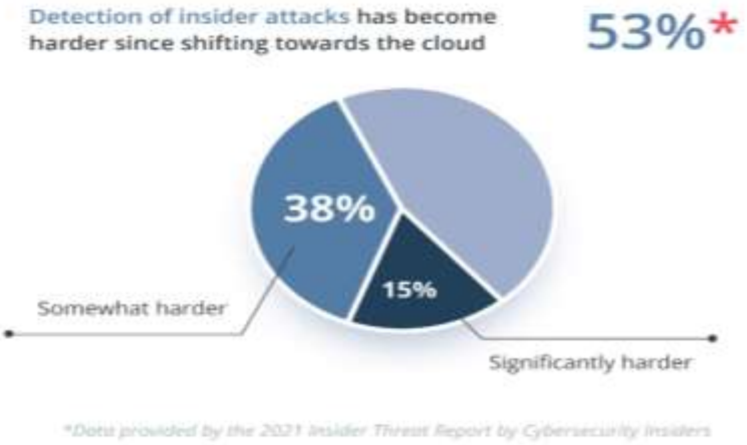

Fig. 3: Detection of Insider Attacks

Data encryption can be used to boost security in a cloud setting. We can protect our data even more effectively if it is dispersed over multiple clouds and encrypted. We can first encrypt any data that the user uploads before storing it on the cloud server. The customer's data will benefit from two-way security thanks to this. Data archiving in a multicloud environment For these purposes, symmetric key or secret key algorithms are the best options. The secret key encryption is another name for the symmetric key algorithm. This cryptographic method encrypts and decrypts data using the same key shared by the sender and the recipient of the data. Symmetric key methods are appropriate for data storage in cloud multi-cloud environments because users should have simple access to their data. The same secret key is used by secret-key encryption methods to encrypt and decrypt data. Because anyone who has the key can use it to decode your data or encrypt their own data and pretend it came from you, you must keep the key safe against access by unwanted parties. Because the same key is used for both encryption and decryption, secret-key encryption is also known as symmetric encryption. When compared to public key algorithms, secret-key encryption techniques are more faster, making them ideal for applying cryptographic changes to enormous data streams.

Conclusion

The ability of systems to self-protect regarding security and privacy is the difficulty in any system from the internet's vital infrastructures, such as cloud computing, according to literature and trends of developing technologies. At whatever stage of an underlying technology, from hardware and software to the core computing infrastructure, secure adaptive approaches are pervasive and can be implemented. In order for a system to be secure, it must be able to defend itself against multiple attacks or hostile users looking for various flaws. Without the actual implementation of adaptive methods for effective client and user experience, cloud computing will continue to be vulnerable to security and privacy concerns. Through STRIDE analysis, this assessment demonstrated the numerous vulnerabilities affecting the various cloud computing components. The study also identifies limitations for several works from the literature, such as grouping security and privacy concerns according to attack mitigation. The review also offered a technical perspective and illustrated the need for adaptable solutions that better address the dangers and weaknesses associated with cloud computing. The study's finding that the majority of publications in the literature lack agreement on how to design and execute efficient cloud security schemes suggests that the implementation of security and privacy in the literature does not strike a balance between integrity, accountability, and privacy. Additionally, user-centric cloud models for privacy protection lack flexibility and control management when it comes to security and privacy policies that safeguard users' sensitive data.

REFERENCES

[1]. Data integrity in cloud computing security, Article in Journal of Theoretical and Applied science.

[2]. Data Integrity in Cloud Computing Security, Journal of Theoretical and Applied Information Technology, 31st December 2019. Vol. 58 No.3, Int 2 Brian O. and others, Cloud Computing, authors: 2020-11- 06, page 6, publish Swiss.

[3]. D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, “Data security over cloud,” International Journal of Computer Applications, no. 5, pp. 11–14, 2021.

[4]. J. Krumm, “A survey of computational location privacy,” Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391–399, 2019.

[5]. Lo, ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari, “A Secure Cloud Computing Model Based on Data Classification”, Elsevier Procedia Computer Science, vol. 52, pp. 1153-1158, 2020.

[6]. Jean Bacon, David Eyers, Thomas F. J. M. Pasquier, Jatinder Singh, Ioannis Papagiannis and Peter Pietzuch, “Information Flow Control for Secure Cloud Computing”, IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 76-89, March 2019.

[7]. Joseph K. Liu, Man Ho Au,Willy Susilo, Kaitai Liang, Rongxing Lu and Bala Srinivasan, “Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud”, IEEE Journal on Network, vol. 29, no. 2, pp. 46-50, 2019.

[8]. Ming Li, Shucheng Yu, Yao Zheng, Kui Renand Wenjing Lou, ”Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131-143, January 2020.

[9]. LI Chaoling, CHEN Yue and ZHOU Yanzhou, “ADataAssuredDeletion Scheme in Cloud Storage”, IEEE China Communications, vol. 11, no. 4, pp. 98-110, April 2014.

[10]. Mauro Gaggero and Luca Caviglione, “Predictive Control for EnergyAware Consolidation in Cloud Datacenters”, IEEE Transactions on Control Systems Technology, vol. 24, no. 2, pp. 461-474, 2019.

[11]. Mahyar Movahed Nejad, Lena Mashayekhy and Daniel Grosu, “Truthful Greedy Mechanisms for Dynamic Virtual Machine Provisioning and Allocation in Clouds”, IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, pp. 594-603, 2021.