Literature Review On

“ Optimal Storage Services In Cloud Computing Ensuring Security “

Priyanka Tingare
Student, Institute of Industrial and Computer Management and Research (IICMR), Savitribai Phule Pune University.

Rohan Chinchwade
Student, Institute of Industrial and Computer Management and Research (IICMR), Savitribai Phule Pune University.
Email:- Chinchwaderohan1818@gmail.com

Rohit kr. Singh
Student, Institute of Industrial and Computer Management and Research (IICMR), Savitribai Phule Pune University.
Rohitsingh30172@gmail.com

Literature Review

Abstract:

Cloud computing has revolutionized the way data is stored and managed. With the increasing volume of data generated by individuals and organizations, the need for efficient and secure storage services in the cloud has become paramount. This literature review aims to explore the current state of optimal storage services in cloud computing and their emphasis on ensuring security. By analyzing existing research and industry practices, this review identifies the key challenges, security requirements, and best practices for achieving optimal storage services in cloud computing environments. The findings of this review contribute to the understanding of secure storage in cloud computing and provide insights for future research and development.

INTRODUCTION:

1.1 Cloud computing has emerged as a promising paradigm for providing on-demand access to a pool of shared computing resources. Among the various services offered by cloud computing, storage services play a crucial role in storing and retrieving large volumes of data for organizations and individuals. However, ensuring the security of data stored in the cloud remains a significant concern for users. This literature review explores the research and advancements related to optimal storage services in cloud computing, with a focus on security measures.

II. BACKGROUND INFORMATION ON CLOUD MODELS AND RELATED WORKS

This section presents a short overview of the cloud computing models. We also offer a summary of related works to our research topic.

A. CLOUD MODELS

1) SOFTWARE AS A SERVICE (SaaS)

The SaaS model facilitates users to access the software and other programs in a cloud. Using the SaaS solution eliminates the need for in-house applications, data storage, and support for the application administration. Companies pay to use the SaaS resources on a user basis.

2) PLATFORM AS A SERVICE (PaaS)

PaaS is a cloud computing service that supports a full software life cycle and allows users to develop cloud applications and services . Programmers and developers do not need to purchase their equipment; instead, they use intermediary equipment and deliver the developed applications to clients over the internet. In PaaS, an individual or a company is not required to buy the software and hardware to develop the applications. Google App Engine, Azure services platform of Google, Amazon's relational database services (RDS) are the key examples of PaaS model.

3) INFRASTRUCTURE AS A SERVICE (Iaas)

IaaS is the cloud computing service delivered in the form of platform in a virtual environment. Clients are not required to purchase servers, data centers, network equipment or space (e.g. Amazon EC2).

4) CONTAINER AS A SERVICE (CaaS)

Based on container virtualization, CaaS has emerged as a cloud model to resolve application development issues in the PaaS environment. The CaaS cloud model is aimed to free the application by making them independent of PaaS environment specifications. Amazon EC2 Container Service (ECS) and Google container engine are examples of CaaS model.

B. RELATED WORK

Information technology has rapid changes in recent years. Cloud computing has added more promising role of IT with the addition of storage for users.
Cloud computing has enabled the vendors to rent out their services at hourly rates. They also rent out the space to users on their physical systems.
However, these services have several security threats for users. In a report, Cloud Security Alliance revealed that abuse, insecure interfaces, and nefarious usage were the vulnerable threats.
These threats have been associated with the application program interfaces and cloud computing. Information security splits into three main objectives, such as integrity, confidentiality, and availability. Security threats to these security goals include a long-term confidentiality issue because one considers that present and past encryption schema are not secure. Information leakage vulnerability is another concern as data is outsourced. Tampering with data also poses threats to

data confidentiality. As new technologies are emerging to meet the users' demands, there is a significant increase in cloud security threats.

These threats are occurring in the form of several unseen exploitation through the cloud computing services and their associated interfaces. It has become essential to counteract the occurred and potential attacks.

Presence of the insecure interfaces is a big challenge to both cloud users and cloud service providers. Cloud services' security and availability mainly depend on APIs that involve in data access and data encryption on clouds. Further research can be undertaken to ensure the security of these APIs and network interfaces. New security proposals can meet the protection challenges of services from intentional and accidental attacks and violation of terms of services.

Furthermore, layered APIs have more complexity as third body operators use cloud services. Actual proprietors cannot access the services. In addition to it, malicious insiders are common threats to cloud services as they violate the services' terms and access the information they are not permitted.

Usually, an employee is the malicious insider who steels the confidential information that belongs to a company or its legal users, An inside malicious user can corrupt the information, particularly in a peer to peer file sharing systems.

||| CLOUD COMPUTING SECURITY

Cloud store the mass amount of users' data, so well-known security is very important. The vendor of the data does not aware about where their data is stored and they do not have control of where data to be placed. Here it searches the security experiments in cloud. Some of the security risks consist of secure data transfer, data separation, security of stored data, user access control, and secure software interface. To promote JAR file compression method and security concern of end users accountability mechanism are used. Here the basic concept is that user's private data should be sent to the cloud in an encrypted form and then with the encrypted data, processing is carried out.

IV. ACCOUNTABILITY FOR THE CLOUD

Accountability become a fundamental concept in cloud that helps for growth of trust in cloud computing. The term Accountability refers to a contracted and accurate requirement that met by reporting and reviewing mechanisms. Accountability is the agreement, to act as an authority to protect the personal information from others. Accountability is for security and protect against use of that information beyond legal boundaries and will be held responsible for misuse of that information. Accountability uses preventive controls. Preventive controls for the cloud include risk analysis, policy enforcement, trust assessment, obfuscation techniques, decision support tools and identity management. Surveying accountability uses detective controls. Detective controls for the cloud including reporting, auditing, tracking, and monitoring. Accountability in cloud motivates, keeping the data usage trackable and transparent.

V. PROPOSED WORK

Cloud computing is a large infrastructure which provide many services to user without installation of resources on their own machine. This is, pay as you use model. Examples of the cloud services are Yahoo email, Google, Gmail and Hotmail. There are many users, businesses, and government uses cloud. So data usage in cloud is large. So data maintenance in cloud is complex. Many Artists wants to do business, of their art using cloud. For example one of the artists wants to sell his painting using cloud then he want that, his paintings must be safe on cloud and no one can misuse his paintings. There is a need to provide technique which will audit data in cloud. On the basis of accountability, we proposed one mechanism which keeps use of data transparent means data owner should get Information about usage of his data. This mechanism support accountability in distributed environment. Data owner should not bother about his data. He may know his data is handled according to service level agreement and his data is safe on cloud. Data owner will decide the access rules and policies.

VI. CONCLUSION:

This literature review has provided an overview of the existing research on optimal storage services in cloud computing, with a focus on security measures. The findings demonstrate that encryption techniques, access control mechanisms, data duplication, integrity verification, auditing, and secure data migration are vital components for ensuring secure storage services in the cloud.

The literature highlights the challenges and opportunities in achieving optimal storage services while ensuring data security in cloud computing environments.

It underscores the importance of adopting a multi-layered security approach and emphasizes the need for ongoing research and innovation to address emerging security challenges in cloud storage services.

Future research should continue to explore novel solutions, such as advanced encryption methods, secure access control mechanisms, and efficient data management techniques, to enhance the security of cloud storage services.

VII. REFERENCES

1.) Rong, C., Nguyen, H., Jaatun, M. G., & Marketakis, Y. (2013). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.

2.) Nair, R., & Shunmuganathan, K. L. (2018). Secure cloud storage services and security challenges: A systematic literature review. International Journal of Information Management, 43, 159-172.

3.) Chowdhury, M. N. K., Boutaba, R., & Rahman, M. R. (2017). Cloud computing for big data analytics: Recent advances and future research challenges. IEEE Journal of Selected Areas in Communications, 35(11), 2547-2564.

4.) Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.

5.) Zhang, R., Liu, L., & Ma, M. (2010). Security models and requirements for healthcare application clouds. IEEE Cloud Computing, 1(3), 46-53.

6.) Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

7.) Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: Implementation, management, and security. CRC Press.

8.) Hamdaqa, M., & Sahraoui, M. (2014). A comprehensive study on cloud computing. Procedia Computer Science, 34, 188-195.

9.) Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. Communications of the ACM, 53(6), 50-56.

10.)Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 3(5), 247-255.