ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Data Security and Privacy Protection for Cloud Storage: A Survey

B. Rajesh, Shaik Mahabuda[1] Singam Jaya Deepika[2], SirasalaSree Sowmya[3], Turaga Rajya Lakshmi[4]
[1,2,3,4]Chaitanya Bharathi Institute of Technology, Proddatur, A.P, India.

shaikmahabuda@gmail.com[1], singamdeepika363@gmail.com[2], sowmyasirasala21@gmail.com[3], rajituraga1304@gmail.com[4]

ABSTRACT

The new development trends including Internet of Things (IoT), smart city, enterprises digital transformation and world's digital economy are at the top of the tide. The continuous growth of data storage pressure drives the rapid development of the entire storage market on account of massive data generated. By providing data storage and management, cloud storage system becomes an indispensable part of the new era. Currently, the governments, enterprises and individual users are actively migrating their data to the cloud. Such a huge amount of data can create magnanimous wealth. However, this increases the possible risk, for instance, unauthorized access, data leakage, sensitive information disclosure and privacy disclosure. Although there are some studies on data security and privacy protection, there is still a lack of systematic surveys on the subject in cloud storage system. In this paper, we make a comprehensive review of the literatures on data security and privacy issues, data encryption technology, and applicable countermeasures in cloud storage system. Specifically, we first make an overview of cloud storage, including definition, classification, architecture and applications. Secondly, we give a detailed analysis on challenges and requirements of data security and privacy protection in cloud storage system. Thirdly, data encryption technologies and protection methods are summarized. Finally, we discuss several open research topics of data security for cloud storage.

Keywords: Cloud Storage, Data Security, Privacy Protection, Data Encryption, Cryptography, Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE), Data Confidentiality, Data Integrity, Access Control, Secure Data Sharing, Homomorphic Encryption.

I. INTRODUCTION

Cloud storage is essentially a cloud computing system that allows users to store and share data on the Internet. The advantages of cloud storage include unlimited data storage space, convenient, safe and efficient file accessibility and offsite backup, and low cost of use. Cloud storage can be divided into five categories in practical applications, namely, public cloud storage, personal cloud storage, private cloud storage, hybrid cloud storage and community cloud storage. In public cloud, enterprises outsourcedata storage business to cloud storage providers Thedata can be accessed only by authorized user. The advantages of public cloud such as flexibility, scalability and cost saving attract plenty of small and medium enterprises.

Personal cloud, also known as mobile cloud storage, is essentially a branch of public cloud, but differ from public cloud, it provides public cloud storage services for individual users. In private cloud, enterprises need to deploy cloud storage infrastructures and arrange professional staff to manage and maintain servers. This ensures that the private cloud has higher security than the public cloud and the control of data is in the hands of the enterprise itself. But the cost increases dramatically. This storage model is moresuitable for large enterprises with large amount of expensive and sensitive data. Hybrid cloud is a combination of public cloud and private cloud, which inherits all the advantages of both. Enterprises

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

can store expensive and sensitive data in private cloud and other data in public cloud The appeal of this storage model continues to grow. As a new cloud storage mode in recent years, community cloud is very suitable for medical and financial industries. Community cloud provides cloud services for several businesses in a specific community. These businesses have the same concerns or need to work together on some projects. Infrastructure construction and server management can be jointly undertaken by community Cloud members or outsourced to a third party.

II. LITERATURE SURVEY

S. No	Journal Type with year	Authors	Title	Outcomes
1	2009	Goldwasser	Simultaneous hardcore bits and cryptography against memory attacks.	IFirst, we define a new class of strong side-channel attacks that we call "memory attacks", generalizing the "cold-boot attack"
2	2019	Framingham	Essential for digital transformation and multi cloud	With the purpose of taking physical attacks into account in security proofs, leakage-resilient cryptography has been initiated.
3	2009	N. Attrapadung and H. Imai,	Attribute-based encryption supporting direct/indirect revocation modes	Attribute-based encryption (ABE) enables an access control mechanism over encrypted data.
4	2008	Safavi-Naini, and W. Susilo	Public key encryption with keyword search revisited	We then argue that care must be taken when keywords are used frequently in the PEKS scheme as this situation might contradict the security of PEKS.

III. EXISTING SYSTEM

In an existing system there is no security for the stored data, there may be chance to stole the confidential information as well there is no privacy. Although there are some researches on data security and privacy protection, there are still no comprehensive studies on the topic for cloud storage systems. As there is no usage of cryptography in early days so, anyone can readily access the information and abuse the data.

Disadvantages:

1. Data Loss:

System Failures: Cloud storage systems are susceptible to hardware failures, software bugs, or service interruptions, which can lead to data loss.Service Provider Issues: Reliance on third-party cloud service providers introduces the risk of data loss due to their operational errors, outages, or unforeseen circumstances.

2. Less Security:

Vulnerability to Cyber Attacks: Cloud storage platforms can become targets for cyberattacks, exposing stored data to unauthorized access, data breaches, and potential manipulation.

3. Less Privacy:

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Inadequate Encryption: Without robust encryption practices, data privacy in transit and at rest may be compromised, leading to potential unauthorized access.
Data Mining Concerns: Cloud service providers may employ data mining techniques for various purposes, raising concerns about user privacy and the potential misuse of sensitive information.

IV. PROPOSED SYSTEM

To overcome the problem with an existing system here we are implementing Cryptography method for uploading data and providing data confidentiality for the user's data. Here, the cloud server has to approve the data owner and data user's registration. The data owner will upload the file. That data will be encrypted and stored in the database. Here the user will send a message to other user here we are applying IBE technique for transferring messages. The data will be secured by using IBE technique.

Advantages:

Data Integrity: Ensuring data integrity in cloud storage enhances trustworthiness by preventing unauthorized alterations. A comprehensive survey enables identification of vulnerabilities, ensuring data remains uncorrupted and reliable. This bolsters the overall quality and dependability of stored information.

Increasing Security: A survey contributes to heightened security by evaluating existing practices and emerging threats in cloud storage. Implementing recommended security measures fortifies defenses against potential breaches, safeguarding against unauthorized access and malicious activities, thereby enhancing the overall resilience of cloud storage systems.

Data Confidentiality: Conducting a survey in understanding and fortifying data confidentiality mechanisms. By assessing encryption technologies and privacy safeguards, the survey ensures that sensitive information stored in the cloud remains protected, mitigating risks of data leaks and privacy breaches.

Architecture:

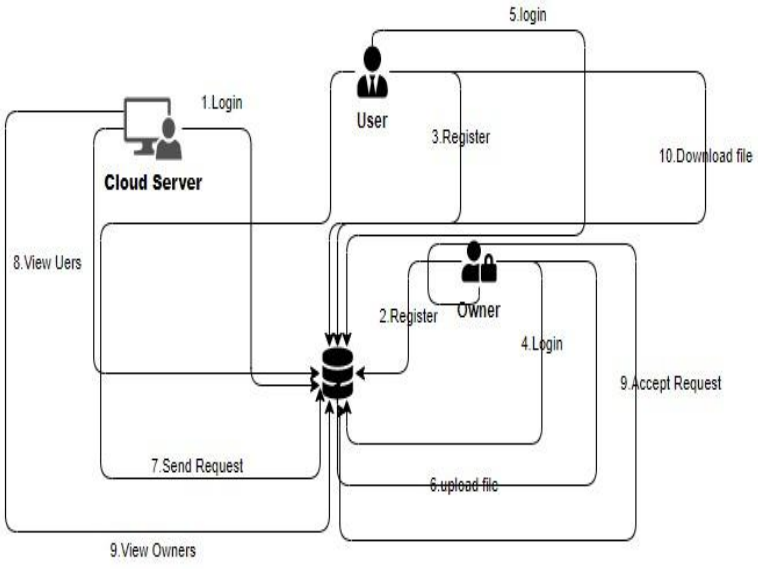


Figure 1:Shows Architecture flow

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

Modules:

Operations of modules explained below.

Data Owner:

Register: Data owner should register into the application with required details.
Login: Data owner must login with valid credentials.
Upload file: Data owner will upload the file.
View file: Data owner can view uploaded files.
View User Request: Data owner can view the requests from users to download the file.
Accept Request: After receiving the request from users' data owner will accept the request.
Logout: Finally, data owner can logout from the application.

Data User:

Register: Data user should register into the application with required details.
Login: Data user must login with valid credentials.
View files: Data user can search the file with the help of keyword and can view the files related to their search those are uploaded by data owner.
Send request: After selecting the file data user can send the request to data owner to get an access for downloading that particular file.
View status: Data user can check their status after sending request to data owner.
Download file: Once after accepting the request by data owner, data user can download the file. **Logout:** Finally, data user can logout from the application.

Cloud Server:

Login: Cloud server must login with default valid credentials.
New registered users: The cloud servers have approved the users' registrations.
New registered users: The cloud server have to approve the Owners registrations.
View data owners: Cloud server can view the data owner's details.
View data user: Cloud server can view the data user's details.
Logout: Finally, Cloud can logout from the application.

V. CONCLUSION

In this paper, we give a detail survey on data security and privacy preservation in cloud storage system. First of all, from the outstanding performance of cloud in the digital economy, enterprise digital transformation, Internet of things and other fields, we confirm that cloud computing and cloud storage will still be the mainstream. We first analyse eight elements of data security in cloud storage system: data confidentiality, data integrity, data availability, fine-grained access control, secure data sharing in dynamic group, leakage-resistant, complete data deletion and privacy protection. Next, we introduce the encryption principles of IBE, ABE, homomorphic encryption, searchable encryption and the research direction of new encryption models. Data encryption technologies and protection methods are summarized. These correspond to the mentioned security requirements. Finally, we put forward some several open research topics of data security for cloud storage.

ISSN: 2582 - 6379
Orange Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2025, Volume 6 Issue 1
www.ijisea.org

References:

[1] Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical Gasp," in Proc. CRYPTO, Santa Barbara, CA, USA, 2012, pp. 868–886.
[2] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," ACM Trans. Compute. Theory, vol. 6, no. 3, pp. 1–36, Jul. 2014.
[3] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," SIAM Journal on Computing, vol. 43, no. 2, pp. 831–871, Jan. 2014.
[4] Z. Brakerski, Y. T. Kalai, J. Katz, and V. Vaikuntanathan, "Overcoming the hole in the bucket: Public key cryptography resilient to continual memory leakage," in Proc. IEEE 51st Annu. Symp. Found. Compute. Sci. (FOCS), Las Vegas, NV, USA, Oct. 2010, pp. 501–510.
[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikey word ranked search over encrypted cloud data," IEEE Trans. Parallel Diatribe. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014. [19] B. Casemore, "Network modernization: Essential for digital transformation and multiload," IDC, Framingham, MA, USA, White Paper US45603019, Nov. 2019.
[6] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in Proc. Int. Conf. Theory Appl. Cryptal. Inf. Secure., Hong Kong, 2017, pp. 409–437.