International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI10.55041/ISJEM.ACME026
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Enhancing Data Security in Cloud Storage using Advanced Encryption Techniques

Thirupathi Sundararajulu [1], R Pavithra [2], Polanki Lakshmi Venkata Swadwika[3], M A Yuvaraj [4], Daksharaju Lokesh[5]

[1,2,3,4,5,6] *Computer Science and Information Technology, Siddharth Institute of Engineering & Technology*

Abstract: The new development trends including Internet of Things, 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, cryptography, access control, privacy protection.

1. 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 outsource data storage business to cloud storage providers The data 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 more suitable 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 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. Usually 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.

2. SYSTEM ANALYSIS

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 research 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 of Existing Systems:

- Data Loss
- Less security
- Less privacy

3. 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 have 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 of Proposed systems:

- Data Integrity
- Increasing security
- Data Confidentiality

SYSTEM ARCHITECTURE

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR, OMR, etc.

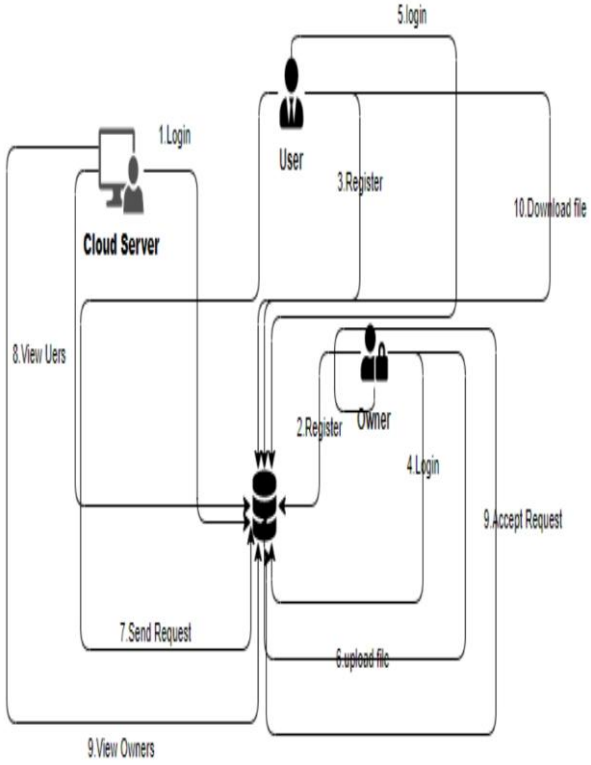

Fig -1: Figure

4. 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 analyze eight elements of data security in cloud storage system: data confidentiality, data integrity, data availability, fine-grained access control, secure data sharing.

FUTURE SCOPE

Future enhancements for cloud storage systems could focus on integrating advanced artificial intelligence and machine learning techniques for real-time threat detection and automated response. Enhancements may also include leveraging blockchain technology for immutable data auditing and enhancing user-centric privacy controls. Continuous research into quantum-safe cryptography will be crucial to mitigate emerging security risks in cloud environments.

REFERENCES

1. [1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, ‘‘Simultaneous hardcore bits and cryptography against memory attacks,’’ in Proc. TCC, San Francisco, CA, USA, 2009, pp. 474–495.
2. [2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. ACM-CSS, New York, NY, USA, 2007, pp. 598–609.
3. [3] N. Attrapadung and H. Imai, ‘‘Attribute-based encryption supporting direct/indirect revocation modes,’’ in Proc. IMACC, Cirencester, U.K., Dec. 2009, pp. 278–330.

BIOGRAPHY

THIRUPATHI SUNDARARAJULU , currently working as Assistant Professor in the Department of Computer Science & Information Technology at Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India. I completed my M.Tech in Computer Science and Engineering from Siddartha Institute of Science And Technology, Puttur and B.Tech in Computer Science and Engineering from Siddartha Institute of Science And Technology, Puttur and I am currently pursuing my Ph.D. in Computer Science and Engineering at Vel Tech Rangarajan Dr.sagunthala R&D Institute Of Science and Technology, Chennai. My research interests include Deep Learning , Big Data , Cybersecurity. I published research papers in reputed journals and conferences. I actively participated in faculty development programs, workshops, and technical seminars. I guided several undergraduate projects and is committed to academic excellence and research innovation.