IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134157

DATA SECURITY and PRIVACY PROTECTION for CLOUD STORAGE

T R Muhibur Rahman[1], Nishitha Yerigeri[2], Surabhi .K[3], Jayasree. T[4], Santhosh B[5]

Associate Professor, (Computer Science Engineering),Ballari Institute Of Technology And Management, Ballari,India[1]

8th semester B.E.(Computer Science Engineering), Ballari Institute Of Technology And Management, Ballari, India[2]

8th semester B.E.(Computer Science Engineering), Ballari Institute Of Technology And Management, Ballari, India[3]

8th semester B.E.(Computer Science Engineering), Ballari Institute Of Technology And Management, Ballari, India[4]

8th semester B.E.(Computer Science Engineering), Ballari Institute Of Technology And Management, Ballari, India[5]

Abstract: At the forefront of this trend are the Internet of Things, smart cities, digital transformation of businesses, and the global digital economy. Due to the enormous amount of data collected, the strain on data storage is only going to increase, propelling the quick growth of the entire storage business. The ability to store and manage data makes cloud storage systems an essential component of the modern world. Governments, businesses, and individual users are currently actively moving their data to the cloud. An enormous volume of data can yield enormous riches. On the other hand, this raises the possibility of risks such data leakage, illegal access, revelation of sensitive information, and privacy disclosure. There are research on data security and privacy protection security, but systematic surveys on the topic in cloud storage systems are still lacking. In this study, we conduct a thorough literature review on data encryption technologies, privacy and security concerns, and relevant countermeasures for cloud storage systems. In particular, we begin by providing an overview of cloud storage, including its definition, categories, architecture, and uses. Second, we provide a thorough examination of the difficulties and specifications related to Cloud storage's data security and privacy protection systems. Thirdly, a summary of data encryption technologies and security techniques is provided. In conclusion, we address various unresolved research issues related to cloud data security storage.

Keywords: cloud storage, encryption, data security, access control, and privacy defense

I. INTRODUCTION

A cloud-based system that lets user's store and exchange data online is basically what cloud storage is. Unlimited data store capacity, easy, safe, and effective file accessibility, remote backup, and inexpensive use are some benefits of cloud storage. In practical terms, cloud storage can be categorized into five types: storage in the public and private clouds, hybrid cloud data backup, personal cloud computing, as well as communal cloud data backup. Businesses use cloud storage providers to handle their data storage needs when using public clouds. Data accessibility is restricted to authorized users only. Little and medium-sized businesses are drawn to the general public cloud because of its advantages, such as financial savings, scalability, and flexibility. In essence, personal cloud storage—also known as mobile cloud storage—is a subset of public cloud storage, with the exception that it offers public cloud storage services exclusively to individual users. Businesses using private clouds must set up cloud storage infrastructures and hire qualified personnel to handle server maintenance and management. This guarantees that the organization retains control over its data and that the private cloud is more secure than the public cloud. However, the price rises sharply. This kind of storage works better for big businesses that handle an abundance of sensitive and pricey data. Combining the best features of both public and private clouds, hybrid cloud reaps their benefits. Businesses can store certain data in public clouds and costly, sensitive data in private clouds. This storage approach is growing in popularity. Community cloud, a relatively new cloud storage model, is ideal for the financial and medical sectors. The availability of cloud services to several enterprises within a community through community clouds. These companies typically share similar issues or need to collaborate on certain tasks. Members of the community cloud can work together to develop the infrastructure and administer the servers, or they might contract these tasks out to another party.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.134157

II. LITERATURE REVIEW

1. Chittumothu Srividhya et al. [1] implemented a mechanism for Data Security, confidentiality of information on every server, bucket concept, recovery of lost data. They used Bucket, BCH CODE Algorithms in Privacy and Data Security Protection for Cloud Storage. They insisted regarding cloud computing mechanism for privacy and data security in cloud. Regarding cloud computing customers to increase their storage space is cloud storage.

2. Ishu Gupta et al. [2] Proposed Cloud computing, data confidentiality and security, data storage, data security, and data sharing, IoT, machine learning, cryptography, watermarking, access control, differential privacy, probabilistic approaches. Many approaches have been explored to deal with this challenge. They used cryptography based models, access control based models, differential privacy using models based on machine learning.

3. Saumya Kumar et al. [3] developed Data Security, threats, Data Protection, Privacy, Cloud computing security, Risks, Cloud Computing. This deals With the advent of cloud computing and different security situation, and it also deal in details about the ways to protect the information and also about the approaches. The simplest definitions from different other are "Cloud Computing is a network-based method of supplying reliable, inexpensive, simple, and easy provisioning of IT related resources".

4. P. J. Sun [4] developed cloud computing, attribute-based encryption, trust, privacy, and access control. Grid, distribution, and utility computing concepts are all combined in cloud computing. They summarize several significant ABE modes, including proxy re-encryption, hierarchical encryption, multi-authority, fine-grained, trace mechanism, CP-ABE, and KP-ABE.

5. Pan Yang et al. [5] proposed cloud storage, encryption, data security, access control, and privacy defense .They used data encryption technology. Cloud computing, data privacy and security, data protection.

6. Alok Katiyar et al. [6] developed Information security, Information concealer, Denial of facilities, Cloud information, Concealment about Cloud Data Protection and Security Storage. They used service models within the cloud example are Software One Service (SaaS), Platform One Service (PaaS) Infrastructure One Service (IAS).

7. Sangeetha et al.[7**]** developed Data security, Privacy protection. They used security models in relation in relation to cloud computing are Security of Cloud Implementation Models, Security of Service Delivery Models, and they've been used cloud security controls, Data encryption is not the only aspect of cloud data security computing. Data security requirements vary depending on the three service models—SaaS, PaaS, and IaaS.

8. Tarasvi Lakum et al. [8**]** proposed Cloud computing, privacy, and security data that is not in use, Data in use and data in transit are used in this Cloud Computing Data Security and Privacy Protection Storage. This offers an examination of security issues with cloud storage. When using machine services, cloud computing can be applied remotely as on-demand software. They deal with the cloud computing data security issue. First, we outline three categories of data protection concerns: data security qualities, cloud features, and data life cycle. Next, we described the standard methods for safeguarding data for every category in this classification.

III. PROPOSED METHODOLOGY

To overcome the problem with an existing system here we are implementing Cryptography method for uploading data and providing data confidentiality in the user's favor data. Here, the remote server has to approve the owner of the information and data user's registration. The person who owns the data will upload the file. That data will be encoded and kept within the database. User will be in the database here. In this instance, the user will send a message to other user here we are applying IBE technique for transferring messages. The information will be secured by using IBE technique.

Advantages:

- Data Integrity
- Increasing security
- Data Confidentiality.

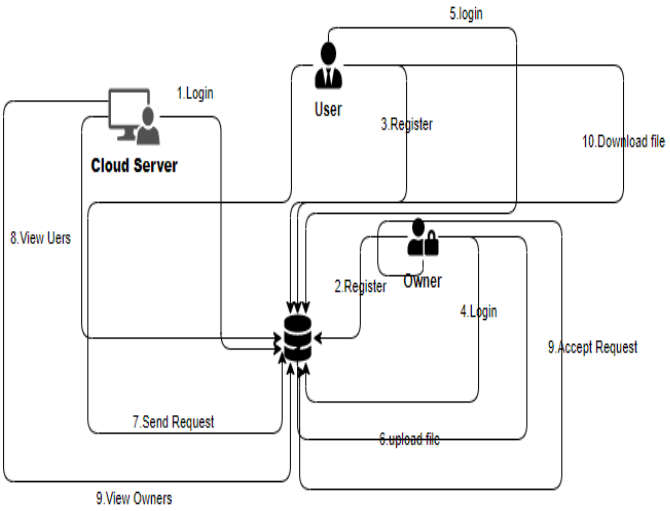
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134157

IV. SYSTEM DESIGN AND ARCHITECTURE



V. DETAIL IMPLEMENTATION OF MODULES

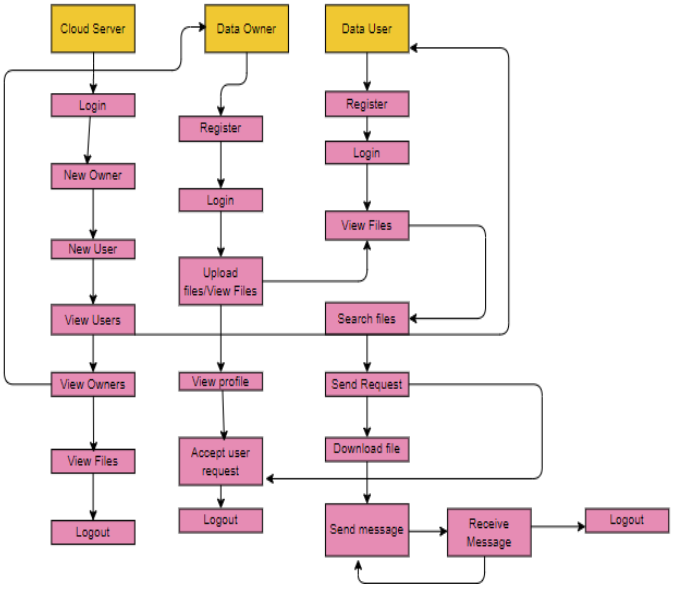


Fig. 1 Flow Chart

Modules:

This project contains 3 modules namely Owner, user, and cloud server of data. 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.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.134157

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 needs to use a legitimate login credentials.
View files: Data user can look through 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 to approve the users' registrations.
New registered users: The cloud server have to approve the Owners registrations.
View data owners: Cloud server can view the all data owner's details.
View data user: Cloud server can view the all data user's details.
Logout: Finally, Cloud can logout from the application.

VI. FEASIBILITY STUDY

The project's viability is analysed a business proposal with a very basic project plan and some cost estimates is submitted during this phase. The proposed system's viability must be investigated during system analysis. This is to make sure the business won't be burdened by the suggested method. A basic understanding of the system's primary requirements is necessary for feasibility study.

The following three factors are crucial to the feasibility analysis:

- Economic feasibility
- Technical feasibility
- Social feasibility

Economic feasibility:

The purpose of this study is to evaluate the system's potential financial impact on the company. The corporation has a finite amount of money to dedicate to system research and development. The costs have to make sense. Because the majority of the technologies utilized were publicly available, the developed system was also possible to be implemented within the allocated budget. All that needed to be bought were the personalized goods.

Technical feasibility:

The purpose of this study is to evaluate the system's technical needs, or its technical feasibility. Any system that is created must not place a heavy burden on the technical resources that are available. High demands will result for the technical resources that are accessible as a result. As a result, the client will face strict requirements. Since deploying the designed system will only require minimum or null changes, it must have modest requirements.

Social feasibility:

Evaluating the degree of user acceptability of the system is one of the study's objectives. This involves teaching the user how to operate the technology effectively. The system must be accepted by the user as a requirement rather than as a danger. The techniques used to familiarize and educate the user about the system will determine the extent of acceptance by the users. Since he is the system's last user, his confidence must be increased in order for him to offer some helpful critique, which is greatly appreciated.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.134157

VII. CONCLUSION

This study presents a survey of cloud computing systems' privacy and data security preservation has been provided. The next step is to put in place a system for protecting the privacy and security of information kept in the cloud. First off, we are able to verify that cloud computing and cloud storage will remain popular due to the cloud's exceptional performance in the enterprise digital transformation and the digital economy, Internet of things, and other domains. The eight components of cloud data security storage systems that we first examine are fine-grained access control, availability, confidentiality, integrity, and secure sharing of data.

REFERENCES

[1] Chittumothu Srividhya et al. Deepthi B, "Data Security and Privacy Protection for Cloud Storage", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 02, no. 07, pp. 875-881, 2022
[2] Ishu Gupta, A. K. S, C.N. L, R. B et al. " Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions", IEEE ACCESS, vol. 10, pp. 71247-71277, 2022.
[3] H. J. S. Saumya Kumar, " Privacy and Security in Cloud Computing: A survey", International Journal Of Innovation Research In Technology, vol. 8, no. 11, pp. 750-754, 2022
[4] P. J. Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions", IEEE Access, vol. 07, pp. 1-33, 2019.
[5] N. X, J. R, Pan Yang, "Data Security and Privacy Protection for Cloud Storage: A Survey", IEEE ACCESS, vol. 08, pp. 131723-131739, 2020.
[6] A. P. S, A. S, A. P. S, P, Alok Katiyar, et al. "A Paper on Data Security In Cloud Computing", International Research Journal of Engineering and Technology (IRJET), vol. 07, no. 06, pp. 216-224, 2020.
[7] M. R.Sangeetha, et al. "Data Security In Cloud Computing", Journal of Emerging Technologies and Innovative Research (JETIR), vol. 06, no. 09, pp. 67-73, 2019.
[8] B. R. Tarasvi Lakum, al. "Data Security in Cloud Computing: A Survery", International Journal of Advanced research in science, pp. 14917-14923, 2020.