International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST52310399

Secure Data Storage System and Data Leakage Detection

Mr. Tejas Rahane, Mr. Chaitanya Shelar, Mr. Suyash Shelar, Mr. Abhijeet Waghamode, Prof. Rupali Jadhav
Department of Computer Science, Zeal College of Engineering and Research, Narhe, Pune, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 05 May 2023
Published: 26 May 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
452-458

ABSTRACT

Data transmitted across these networks must be secure and private given how large and rapidly expanding they are. Cloud servers are a key resource for data storage. Therefore, cloud servers must be protected and cannot be left open to the prospect of being utilized by hackers for theft or exposure. They require strategic plans for this to guarantee the data's security and privacy. The solution being proposed makes use of three approaches to guarantee data security. The plans involve data encryption, data distribution across several clouds, and granting data sharing authenticity by using a secret key alone. The system is first set up to allow data sharing across a secure channel of encryption using the Lightweight method. After that, data is dispersed among several clusters using the DROP technique, and data is replicated between clouds to prevent any loss. Only a third private key can explicitly grant those with a need for the information access to various data segments. Any unethical request to share data is detected by a trapdoor, which blocks the request and identifies the individual responsible for any data leakage.

Keywords: Energy efficient algorithm, Manets, total transmission energy, maximum number of hop, network lifetime

I. INTRODUCTION

Data is recognized as the most important asset of an organization because it establishes the distinctiveness of every business. It is the main basis for information, knowledge, and ultimately wisdom for making wise judgements and doing appropriate actions. It could be making a building more efficient, curing a disease, increasing a company's revenue, or being in charge of fulfilling goals and enhancing the performance. Furthermore, any organization that wants to improve its performance must have the basic services of data storage, analysis, and sharing. However, the businesses are under tremendous pressure to store the massive amounts of data locally as a result of the data explosion. Additionally, because of the resources available, exploring the data has become challenging.

Due to the cloud's many benefits, including on-demand service, scalability, reliability, flexibility, measurable services, disaster recovery, accessibility, and many others, the majority of enterprises have switched to it for these services. A paradigm called cloud computing makes it possible to have a lot of memory and a lot of processing power at a low cost. It brings a great deal of ease to the cloud by enabling customers to access the desired services across different devices regardless of their location or time. the presentation. Any company that wishes to boost performance also has to have access to the fundamental services of data analysis, sharing, and storage. However, because of the data explosion, organizations are under enormous pressure to locally store the vast amounts of data. Additionally, studying the data has become difficult due to the resources available.

The majority of businesses have shifted to using the cloud for these services due to its many advantages, including on-demand service, scalability, reliability, flexibility, measurable services, disaster recovery, accessibility, and many others. Having a lot of memory and processing power at a low cost is made possible through a paradigm called cloud computing. The way computer services are delivered has changed as a result of cloud computing. A growing number of vulnerable devices (customers) that use outsourcing computing models depend on distant servers (nodes) for data storage and calculation.

An enormous quantity of power is being consumed by an increasing number of cloud data centers throughout the globe. The use of the cloud is developing as a new style of fully distributed computing. It has shifted computing from personal computers and small businesses to expansive information facilities. and improved it for customers and IT businesses by employing blocking large amounts of capital investments. Many studies on cloud computing have focused on certain problems and difficulties that are related to the concept of cloud computing. The service of cloud computing (CC) is provided by data centers, which are wholly dependent on virtualization technology. During the COVID-19 crisis, cloud computing makes it easier to collaborate, communicate, and access crucial web services. Scientific partnerships carrying out these investigations have a variety of goals and employ various techniques to develop the computer frameworks.

Big data can be found in a vast number of little files, hence a key role of the cloud data warehouse is to ensure the security of sensitive data. This can be done using steganography and cryptographic techniques. Information loss, data integrity issues, and botnets all pose serious hazards to the software and data of businesses. Sensitive data security is a critical requirement in modern communication, particularly in the cloud. Numerous data sets have been saved in cloud computing environments, and the number of people using cloud computing services grows daily. Huge advantages of cloud computing include remote storage, mobility, information sharing, cost savings on hardware and software, etc.

Cloud service data leakage is also growing. due to attackers' ongoing attempts to take advantage of the security flaws in the cloud. the engineers and To develop stronger security measures to safeguard sensitive data in cloud computing environments, experts work to identify potential cloud risks and attacks.

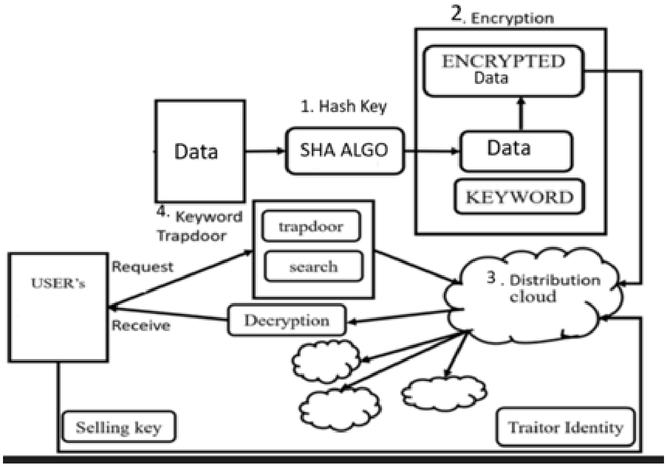
Many data-secure cloud computing models have recently been put out. Moving programmed to the cloud and taking advantage of its benefits is a way to first contrast the security issues with both individual records and the cloud. Businesses that switch from on-premise to cloud-based software face challenges related to data residency, corporate compliance standards, and privacy and third-party party obligations for the treatment of sensitive data.

Corporate rules or governing authorities' policies have an impact on how sensitive information is managed, including where it is kept, what types of data can be collected and retained, and who has access to it. These issues may determine the extent to which businesses are able to comprehend the cost of cloud computing. AES-based document encryption and decryption of information uploaded via cloud computing, admin verification and user locking, the retrieval of client IP information, and distributed database storage, or statistics, are all included in a new, improved framework of security for client identity. As a result, user login information is saved in a single database, and information like files uploaded are encrypted and decrypted. and key are stored in several databases. Given that people rarely use their passwords, one component of authentication is vulnerable to password guessing.

Therefore, in today's environment, cloud computing security is crucial. Overall, paints provide safety and security for the entire cloud-based computer architecture in addition to boosting security for cloud computing. With cloud technology, open information sharing with others is possible. data transfer to a Third-party (cloud service provider) off-website online storage networks, over which data owners have limited control, provide unique privacy risks from illicit sensitive information disclosure through carrier providers, factual accuracy and reliability of outside-carrier information, etc. The cloud enables the exchange of information; careful attention should be given to the full access to management of the preserved information. data is a sensitive truth concerning secrecy that data was encrypted using standard methods up until it was transported to the cloud. The customer encrypts his document and stores it on the cloud server using a traditional public key infrastructure. Only true authorized users are informed of the decryption key. This approach is safe in terms of secrecy; However, this system requires complex, tested, and reliable control and distribution. Even with this solution, prosper because there are more and more clients for software.

II. METHODOLOGY

A. System Design



System Architecture

1. Three methods are used by the system to guarantee data security.
2. The methods include data encryption, data distribution over several clouds, and the authentication of data sharing using a secret key only.
3. Firstly, a system is created for data sharing via a secure channel of encryption with a hash key, using the AES technique to encrypt data.
4. To prevent any loss, the data is then copied between clouds and distributed across other clusters using the DROPS method.
5. The User needs private key permission in order to view the data.
6. The private key might grant explicit users who require the information access to various data segments.
7. A trapdoor is created to identify any requests to provide data that are immoral, prevent such requests, and seek out the person responsible for any data leaks.

B. Modules

1) Owner Aggregated data are transmitted over a wireless interface, like Bluetooth or WLAN. The record is mined for keywords to describe the data.

C. The keyword and file are then converted into a cypher text in accordance with a predetermined access policy.

2) Data User No. 2 the network's users. Each data user is given permission to search an encrypted file based on a set of attributes, such as affiliation, department, and type of staff. In this scenario, a data generates secret keys on terminals with restricted resources and performs the information retrieval operation. The files are recovered, the secret keys are wirelessly transmitted to the public cloud, and then the data are received back. Once the PHR files have been decrypted, the data user checks the correctness of decryption.

3) The public cloud provides virtually infinite computation and storage capacity to handle remote storage tasks and respond to data retrieval requests. The suggested system has a lightweight test algorithm to boost performance.

4) The Key Generation Centre For the entire system, KGC generates public parameters and provides secret keys to data users. His secret key contains a set of attributes specific to the data user in order to provide access control. The KGC can identify the malicious user and invalidate a traitor's secret key if they sell their secret key for money.

III.RELATED WORK

To secure the cloud, Kao et al. [1] presented uCloud, a user-centric key management system. In uCloud, user data is indirectly encrypted with RSA using public keys of users. Instead than being kept on users' computers or servers, the users' private keys are kept on their mobile devices.

The users' private keys are also expressed in the two-dimensional (2D) barcode images, and these keys are then used to decrypt the users' sensitive data. The two crypto-based techniques were supplied by Al-Haj et al. [2] to ensure the data's confidentiality, integrity, and validity. In order to secure the data, they added a cryptographic function employing the hash code and symmetric keys. The elliptic curve digital signature algorithm is used to provide the integrity and authenticity. Additionally, the whirlpool hash function and the advanceencryption standard Galois counter mode are utilized to support authenticity and confidentiality. For the safe exchange of cloud data, Liang et al. proposed a Ciphertext-Policy Attribute-Based Proxy Re-Encryption Scheme [3]. Re-encryption and re-encryption key generation stages have been improved, lowering communication and computational costs. According to the plan, a data owner is permitted to grant others access rights to encrypted data that is kept on a cloud system. Wang et al. in [4] present a file hierarchy attribute-based encryption system. for protecting the information in a cloud environment. This plan employed a tiered access structure paradigm to address the problem of sharing many hierarchical files.

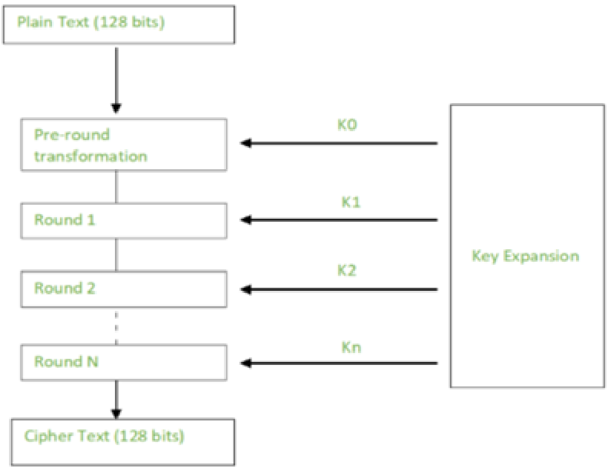
A fair data access control approach for cloud storage was put forth by Liu et al. [5]. To prevent unauthorized access to shared data, the system performs a fair key reconstruction, and none of the users exchanged their shares. The suggested method for obscuring the shared data's decryption key generates a lot of false keys. Additionally, the performance evaluation showed that the communication costs and computation delay were decreased, but the authentication system was not effective in the scheme. Liu et al. present a CP-ABE scheme in [6]. to lower the significant decryption computation cost at the user end, which rises with the complexity of the access policy. This solution made it easier to outsource decryption, adjust revocation attributes, and update policies as user attributes changed. Li et al. [7] suggest a lightweight data sharing strategy (LDSS) for mobile cloud computing. LDSS adopted the CP-ABE technique to improve the structure of the access control tree. Activate the system appropriate for cloud mobile environments. In this system, a significant percentage of the computation from mobile devices is shifted to external proxy servers. A Privilege-based Multilevel Organizational Data-sharing (P-MOD) method was put up by Zouglou et al. in [8]. To successfully handle and share large amounts of data, PMOD strengthens its attribute-based encryption approach by including a privilege-based access structure. To update the file dynamically and increase the effectiveness of the policy in the cloud environment, Li et al. [9] introduced a Linear Secret Sharing method (LSSS) matrix access structure based on an efficient CP-ABE method.

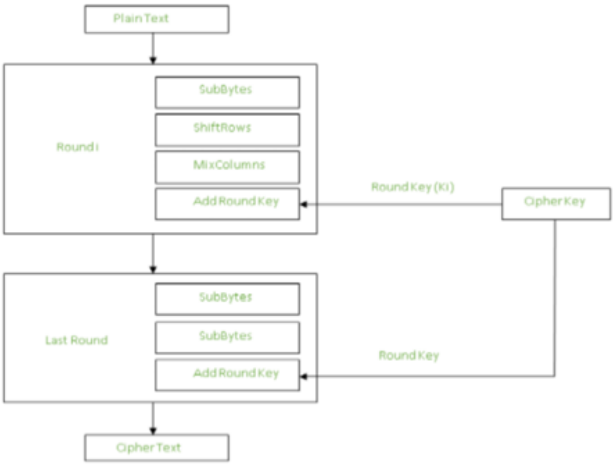
The plan's goals include thwarting selected plaintext attacks (CPA) and lowering the proxy cloud service provider's (PCSP) storage requirements.

IV.ALGORITHM

Advanced Encryption Standard (AES)

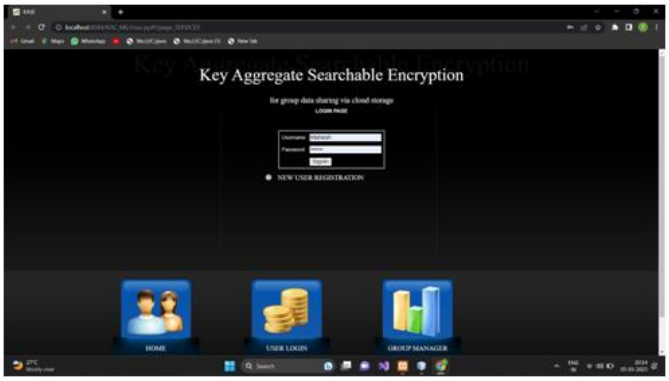
The PHR is encrypted using the AES technique. With a given key, the method does 10 or 14 rounds of encryption depending on whether the input is 128 or 256 bytes. Each Round consists of 4 phases, one of which is SubByte, in which each byte is replaced with a different byte. The following involves shifting an entire row. The following step is mix column, in which columns are blended, and adding round key is the final step. The figure displays one round.





PHR data distribution across various clouds is done via the Drops Algorithm. The file is broken up into several pieces and copied over numerous clouds. A Fig depicts the process for dividing a file into a number of pieces.

V. IMPLEMENTATION



Key Aggregate Searchable Encryption

for group data sharing via cloud storage

LOGIN PAGE

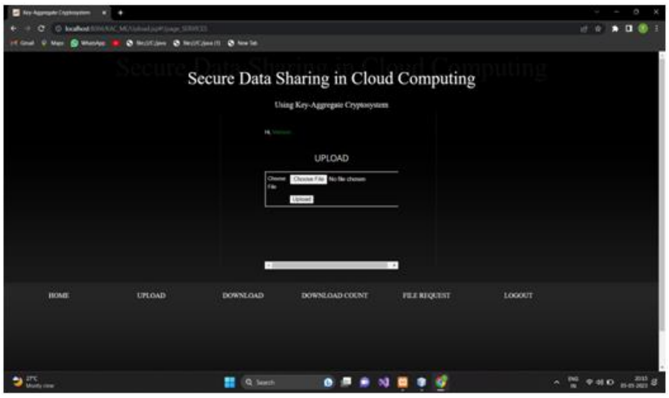
Username

Password

Signin

NEW USER REGISTRATION

Login Page



Secure Data Sharing in Cloud Computing

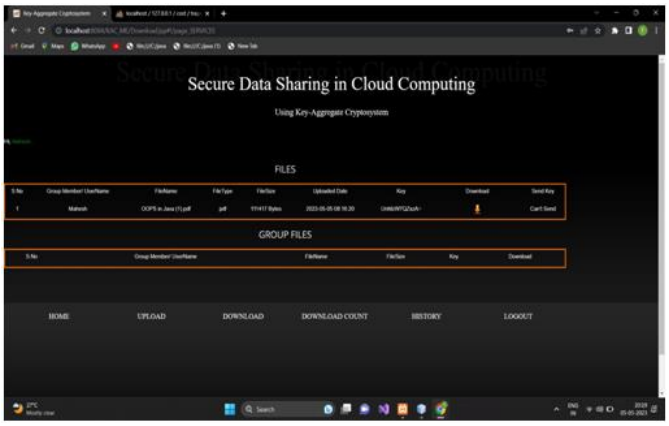
Using Key-Aggregate Cryptosystem

UPLOAD

Choose File: Choose File No file chosen

Upload

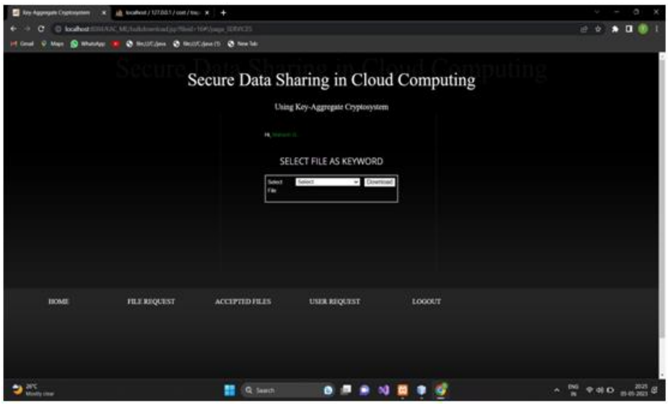
Upload Page


Secure Data Sharing in Cloud Computing
Using Key-Aggregate Cryptosystem
FILES
GROUP FILES
HOME
UPLOAD
DOWNLOAD
DOWNLOAD COUNT
HISTORY
LOGOUT

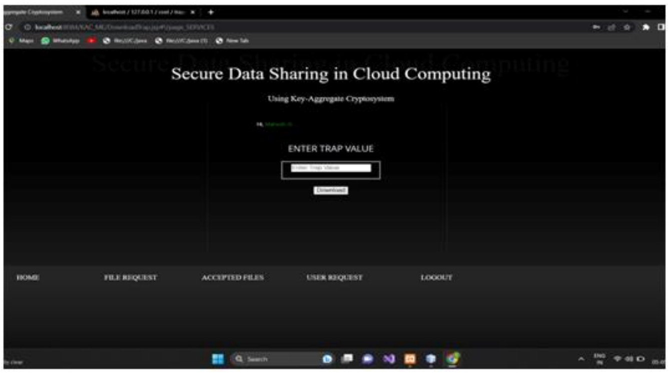
S.No	Group Member/ UserName	FileName	FileType	FileSize	Uploaded Date	Key	Download	Send Key
1	Mahesh	OOPS in Java (1).pdf	pdf	111417 Bytes	2023-05-05 08:16:20	UnkbWYQZsoA-	⬇	Can't Send

S.No	Group Member/ UserName	FileName	FileSize	Key	Download

Download Page



File Search Page



Verification Page

VI.CONCLUSION

In the context of cloud computing and information security, data protection is a difficult undertaking to accomplish. It has been determined that no single technique is effective in guaranteeing the data's complete security from every entity involved in the system, whether directly or indirectly. By including the methods for completely securing the system in the sharing environment, a robust solution may be created. Furthermore, it is anticipated that the disclosed analysis will serve as a milestone for the possible researchers working in the area as well as other emerging applications wanting safe data storage and sharing for its security. This is due to the set of features of the addressed exceptional solutions.

VII. REFERENCES

[1]. Y. Kao, K. Huang, H. Gu and S. Yuan, "UCloud: A usercentric key management scheme for cloud data protection", IET Inf. Secur., vol. 7, no. 2, pp. 144-154, Jun. 2013.

[2]. A. Al-Haj, G. Abandah and N. Hussein, "Crypto-based algorithms for secured medical image transmission", IET Inf. Secur., vol. 9, no. 6, pp. 365-373,Nov.2015.

[3]. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, et al., "A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing", Future Generat. Comput. Syst., vol. 52, pp. 95-108, Nov. 2015.

[4]. S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing", IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1265-1277, Jun. 2016.

[5]. H. Liu, X. Li, M. Xu, R. Mo and J. Ma, "A fair data access control towards rational users in cloud storage", Inf. Sci., vol. 418, pp. 258-271, Dec. 2017.

[6]. Z. Liu, Z. L. Jiang, X. Wang and S. M. Yiu, "Practical attribute-based encryption: Outsourcing decryption attribute revocation and policy updating", J. Netw. Comput. Appl., vol. 108, pp. 112-123, Apr. 2018.

[7]. R. Li, C. Shen, H. He, X. Gu, Z. Xu and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing", IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344- 357, Apr. 2018.

[8]. J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, et al., "An efficient attribute-based encryption scheme with policy update and file update in cloud computing", IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6500-6509, Dec. 2019.

[9]. E. Zaghloul, K. Zhou and J. Ren, "P-MOD: Secure privilegebased multilevel organizational data-sharing in cloud computing", IEEE Trans. Big Data, vol. 6, no. 4, pp. 804-815, Dec. 2020

Cite this Article

Tejas Rahane, Chaitanya Shelar, Suyash Shelar, Abhijeet Waghamode, Prof. Rupali Jadhav, "Secure Data Storage System and Data Leakage Detection", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 3, pp. 452-458, May-June 2023. Available at doi : https://doi.org/10.32628/IJSRST52310399

Journal URL : https://ijsrst.com/IJSRST52310399