IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

Secure Data Storage System and Data Leakage Detection

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

Abstract: *Given the size and rate of growth of these networks, data carried across them must be secure and confidential. A vital resource for data storage is cloud servers. Cloud servers therefore need to be secured and cannot be left vulnerable to the possibility of being used by hackers for theft or exposure. To ensure the security and privacy of the data, they need strategic plans. The proposed system employs three strategies to ensure data security. The plans call for data encryption, distribution over many clouds, and authentication of data sharing using just a secret key. The system is initially configured to provide data sharing over a secure channel using the Lightweight technique of encryption. Then, to prevent any loss, data is copied between clouds and scattered using the DROP technique throughout many clusters. Access to certain data segments can only be explicitly granted by a third private key to those who require the information. A trapdoor that detects any unethical requests for data sharing stops the requests and identifies the person in charge of any data leaks.*

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

I. INTRODUCTION

Because it establishes the uniqueness of any firm, data is acknowledged as the most crucial asset of an organisation. It is the primary source of knowledge, information, and eventually wisdom for making informed decisions and doing the right actions. It could involve improving a building's efficiency, treating a sickness, boosting a business's revenue, or being in charge of achieving objectives and raising performance. Any organisation that wishes to boost performance also has to have access to the fundamental services of data analysis, sharing, and storage. But because of the data boom, businesses are under enormous pressure to store the enormous amounts of data locally. Additionally, it has become difficult to explore the data because of the resources accessible.

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 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. It offers an as well as storage. Organisations are under tremendous pressure to locally store the massive volumes of data, though, as a result of the data explosion. The resources available have made it more difficult to study the data as well.

Due to the cloud's numerous benefits, including on-demand service, scalability, stability, flexibility, measurable services, disaster recovery, accessibility, and many others, the majority of firms have switchead to using it for these services. getting A significant amount of power is being used by an expanding number of cloud data centres worldwide. A new method of fully dispersed computing is emerging called cloud computing. Large-scale information facilities have replaced personal PCs and small companies as the primary computing platforms. and by using blocking significant amounts of capital investments, improved it for customers and IT firms. Numerous research on cloud computing have concentrated on certain issues and challenges that are connected to the idea of cloud computing. Data centres, which are totally reliant on virtualization technology, offer the cloud computing (CC) service. Cloud computing makes it simpler

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

to work together, communicate, and access essential web services during the COVID-19 issue. The scientific collaborations conducting these projects use a variety of methods and strategies to create the computer frameworks..

Because there are so many small files that make up big data, a crucial function of the cloud data warehouse is to guarantee the security of sensitive data. Steganography and cryptographic methods can be used for this. Botnets, information loss, and problems with data integrity are all significant threats to company software and data. Secure transmission of sensitive data is essential in modern communication, especially in the cloud. Many data sets have been stored in cloud computing environments, and every day, more people use these services. Remote storage, mobility, information sharing, cost savings on hardware and software are just a few of the major benefits of cloud computing.

Data leakage from cloud services is also increasing. because hackers continue to try to exploit the security holes in the cloud. both engineers

Experts are working to identify potential cloud dangers and assaults in order to develop stronger security solutions to protect sensitive data in cloud computing settings.Recently, many cloud computing models that protect data have been released. A approach to compare the security concerns with both individual records and the cloud is to move programming to it and take advantage of its advantages. Companies that migrate from on-premise to cloud-based software confront issues with data residency, corporate compliance rules, privacy, and third-party obligations for the management of sensitive data.

How sensitive information is managed, including where it is kept, what kinds of data can be gathered and retained, and who has access to it, is influenced by corporate rules or regulatory authorities' policies. The degree to which organisations are able to appreciate the cost of cloud computing may depend on these problems. A new, enhanced framework of security for client identity includes AES-based document encryption and decryption of material submitted via cloud computing, admin verification and user locking, the retrieval of client IP information, and distributed database storage, or statistics. As a result, information like uploaded files is encrypted and decrypted and user login information is maintained in a single database.

, and key are kept in several databases. given that individuals.Therefore, cloud computing security is essential in the current situation. Overall, paintings increase security for cloud computing while also providing safety and security for the overall cloud-based computer architecture. Open information exchange with others is made feasible by cloud technology. transfer of information to a third party (cloud service provider)

Off-website online storage networks present distinct privacy threats from unlawful activities, over which data owners have little control.

Sensitive information disclosure through carrier providers, factual correctness and information source reliability, etc. Information exchange is made possible by the cloud; nevertheless, full access to management of the retained information must be carefully considered. Data was encrypted using industry-standard techniques before being sent to the cloud, which is a delicate reality regarding secrecy. The customer uses a conventional public key infrastructure to encrypt his document and put it on the cloud server. The decryption key is only known to genuine authorised users. Although this method is secure in terms of secrecy, it needs sophisticated, tried-and-true control and dissemination. Despite this remedy, prosper as more and more people utilise the software.

II. RELATED WORK

Kao et al. [1] introduced uCloud, a user-centric key management system, to secure the cloud. In uCloud, user public keys are used to RSA-indirectly encrypt user data. The users' private keys are stored on their mobile devices rather than on their PCs or servers.

The two-dimensional (2D) barcode images also contain the users' private keys, which are needed to decrypt the users' sensitive data. Al-Haj et al. [2] provided the two crypto-based methods to guarantee the data's privacy, accuracy, and authenticity. They included a cryptographic algorithm that makes use of the hash code and symmetric keys to safeguard the data. The integrity and authenticity are provided by the elliptic curve digital signature algorithm. To support authenticity and security, the whirlpool hash function and the sophisticated encryption standard Galois counter mode are also used. confidentiality. Liang et al. suggested a Ciphertext-Policy Attribute-Based Proxy Re-Encryption Scheme [3] for the secure exchange of cloud data. Reduced communication and computational costs result from enhanced re-encryption and re-encryption key generation processes. The plan allows a data owner to provide other users access

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

privileges to encrypted data stored on a cloud server. A file hierarchy attribute-based encryption system is presented by Wang et al. in [4].

for safeguarding data in a cloud environment. The challenge of sharing several hierarchical files was addressed by this design, which used a tiered access structure paradigm.

Liu et al. [5] proposed a fair data access control strategy for cloud storage. The system performs a fair key reconstruction to prevent unauthorised access to shared data, and none of the users switched their shares. The proposed approach for hiding the decryption key of the shared data yields a large number of fake keys. The performance review also revealed a reduction in communication expenses and computation delays, but it also revealed that the scheme's authentication system was ineffective. A CP-ABE scheme is presented by Liu et al. in [6].

To reduce the substantial user-end decryption computation cost, which increases with the complexity of the access policy. As user attributes changed, this method made it simpler to outsource decryption, modify revocation attributes, and update rules. A lightweight data sharing strategy (LDSS) for mobile cloud computing is recommended by Li et al. [7]. To strengthen the structure of the access control tree, LDSS implemented the CP-ABE approach. Turn on the system necessary for mobile cloud environments. In this method, a sizable portion of mobile device compute is transferred to external proxy servers. In [8], Zouglou et al. presented the Privilege-based Multilevel Organisational Data-sharing (P-MOD) technique. In order to efficiently manage and distribute massive amounts of data, PMOD improves its attribute-based encryption strategy.

III. LITERATURE SURVEY

1.Using an encryption algorithm, the cloud can store data securely.

2. This paper provided us with the project's fundamental idea. This document is the foundation of the project.

Improved encryption scheme-based hybrid secure cloud storage for data

3. System for secure cloud storage using ciphertext retrieval

4. We learned about encryption techniques in depth and how to make it better from these papers.

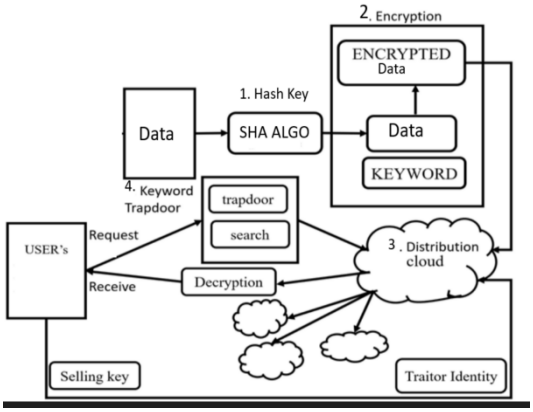
5. These papers taught us how to use and handle ciphertext and how to deal with it.

6. Research Methods to Enhance Secure Data Storage in Cloud Computing

We learned about many issues with cloud storage systems and how to address them from these papers.

IV. METHODOLOGY

System Design



System Architecture

1. The system ensures data protection using three different techniques.

2. The techniques include data encryption, data dissemination over many clouds, and data sharing authentication that uses just a secret key.

3. To begin with, a system is developed for data sharing using an encrypted channel protected by a hash key and the AES encryption method.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

4. The data is then dispersed across different clusters and copied between clouds using the DROPS technique to prevent any loss.
5. To read the data, the User needs private key permission.
6. The private key could provide explicit users access to certain data segments if they need the information.
7. To detect any requests for data that are unethical, stop such requests, and find the individual in charge of any data leaks, a trapdoor is made.

V. CONCLUSION

Data protection is a challenging task to do in the context of cloud computing and information security. It has been established that no one method is capable of ensuring the data's total security from every system participant, whether directly or indirectly. A strong solution may be produced by incorporating the procedures for completely safeguarding the system in the shared environment. In addition, it's predicted that the released analysis would mark a significant turning point for any future academics working in the field as well as for other new applications seeking secure data storage and sharing. This is because the addressed exceptional solutions have a certain set of properties.

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