iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43751

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Enhancing Security of Data in Cloud Storage Using Decentralized Infrastructure

Mr. Ram Prashath R[1], Surya Prabha J[2]
[1]*Assistant Professor,* [2]*Scholar, Department of MCA. Karpagam College Of Engineering, Coimbatore, India*

Abstract: ***Nowadays, a considerable amount of data is stored in the cloud, which must be kept safe against unauthorised access. Various algorithms are employed to ensure data privacy and security. Every system's goal is to achieve confidentiality, integrity, and availability (CIA). The existing centralised cloud storage, on the other hand, does not have these CIA qualities. Decentralized cloud storage is used in conjunction with hash algorithm used to improve data security and storage approaches. It efficiently aids in the protection of data against manipulation or the deletion of a portion of data. A data connects the blocks that hold data in a block chain. Each block contains a hash value that is stored in the following block. As a result, the possibilities of data loss are reduced.***
Keywords: Decentralized Cloud Storage, SHA-512, Advance Encryption Standard, Encrypt, Decryp,CIA.

I. INTRODUCTION

Nowadays, instead of using local storage devices, cloud storage is used to store and retrieve data that is based on the internet in order to gain a more trustworthy, secure, and available data. However, because the information is sensitive and should not be shared with anyone without permission, an encryption method is used to turn the plain data into cypher text, and a decryption method is used to recover the original data. As a result, the encryption algorithm is critical in making data more safe. To do these operations, various mathematical calculations are performed, and the process can also be explained realistically. This process gives data CIA qualities and ensures that data is secure. will remain safe and unique. Encryption and decryption require data to be divided into chunks of data. There are several algorithms available for this operation, which are classified into two groups. The first is symmetric encryption, which encrypts and decrypts data using the same key. After the encryption method is employed, the data is changed into an unreadable format. In order to recover the original message, the intended user must know the key that was used during the encryption process. The approach then reverses its procedure, resulting in data that is intelligible. The second way is asymmetric encryption, which generates two keys, one for encryption and the other for decryption. The Hash algorithm, commonly known as the Advance Encryption Standard (AES), works with keys up to 128 bits in length. This algorithm supports three alternative key lengths: 128, 192, and 256 bits. To transform plain text into cypher, this encryption is based on key length, and to improve data security, this algorithm repeats its process numerous times called rounds. It employs ten rounds for 128 bits, twelve rounds for 192 bits, and fourteen rounds for 256 bits. Except for the last round in each scenario, the remainder of the rounds are all equal. After executing this procedure on data, an encrypted data block in unreadable form is obtained. The reverse procedure of the AES algorithm must be performed on encrypted data in order to recover the original data.

II. LITERATURE SURVEY

Cloud computing is a new paradigm that attempts to deliver computational resources, large amounts of data storage, and flexible data sharing services. The rapid rise of data produced persuades businesses and users to outsource their data to cloud storage systems, owing to cloud-top characteristics. However, the security and encrypted data of sensitive data outsourced to decentralized cloud servers is becoming a big problem. Before storing data in the potentially untrustworthy cloud, it must be encrypted. Traditional encryption techniques place a significant burden on data owners in terms of managing files and encryption procedures. They have major security, efficiency, and usability problems, and some of the techniques are ineffective for protecting cloud data.

III. PROJECT ANALYSIS

A. Existing System

Traditional cloud storage, which stores all data in a single location called centralised cloud storage, increases the risk of data loss. When contrasted to decentralised cloud storage, security is a concern. since the data might be monitored and controlled by the owner of a centralised cloud It can be tampered with or stolen. With a pressing need for access, Each individual wants to be able to get their info quickly and easily more secure.

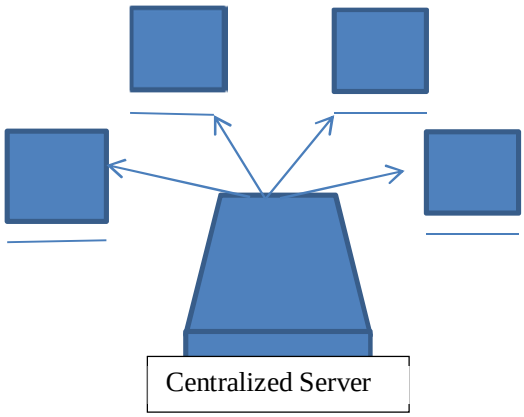


Fig.1 Centralized Server

B. Proposed System

The data owner stores data on a cloud server under the suggested paradigm. Intruders will constantly be attracted to cloud servers in order to steal valuable data. The owner of the data shares a key with the data user for security purposes. The AES method is employed to render the data unreadable by intruders. As a result, intruders are unable to steal the information. Data are linked to each other using the SHA-512 hashing method, and if data are found to be missing, we have devised a mechanism that allows data users to determine which data is being attacked by hackers.

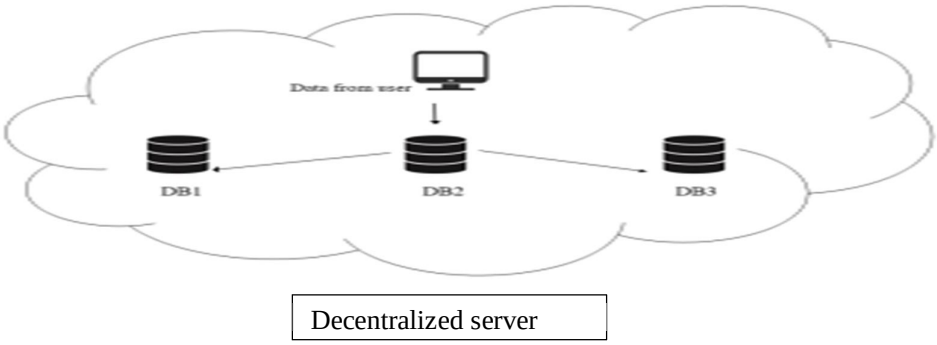


Fig. 2 Decentralized Server

Figure2 depicts the structure of decentralised cloud storage. Data from users is saved on various databases assigned by the server in order to create a duplicate of the data; however, when data is stored on different servers, it is broken into chunks. This means that there is enough of storage space for data, and the cost of storing data on a cloud server is low. There is no single entity that owns and controls the data. Another benefit of decentralised cloud storage is that it is a constantly live network that allows data to be accessed at any time.

IV. FLOW OF WORK

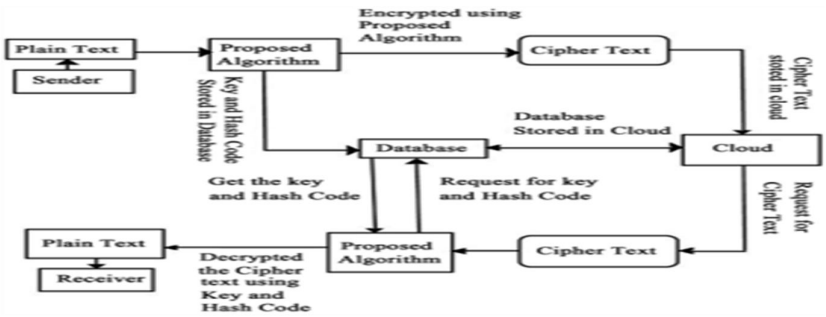


Fig. 3 flow of work

As seen in the diagram above, plain data is first encrypted with the AES technique and then stored on the cloud as a hash value. The SHA 512 algorithm is used for hashing. The data can only be decrypted by the authenticated user.

V. CONCLUSION

As per the literature and study we can say that there are certain limitations of centralized storage. So to enhance the security of data we can use decentralized cloud storage. This project suggests a secure and efficient way to store data on cloud. Hash Algorithm-based cloud storage with data encryption gives data security in decentralized structure. The proposed model is suitable to implement the Decentralized structure. The hash algorithms used to implement the system model is efficient and required less time and give high security for the data which is being stored on cloud. This kind of architecture makes the system more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in data files of user for their benefits.

VI. FUTURE SCOPE

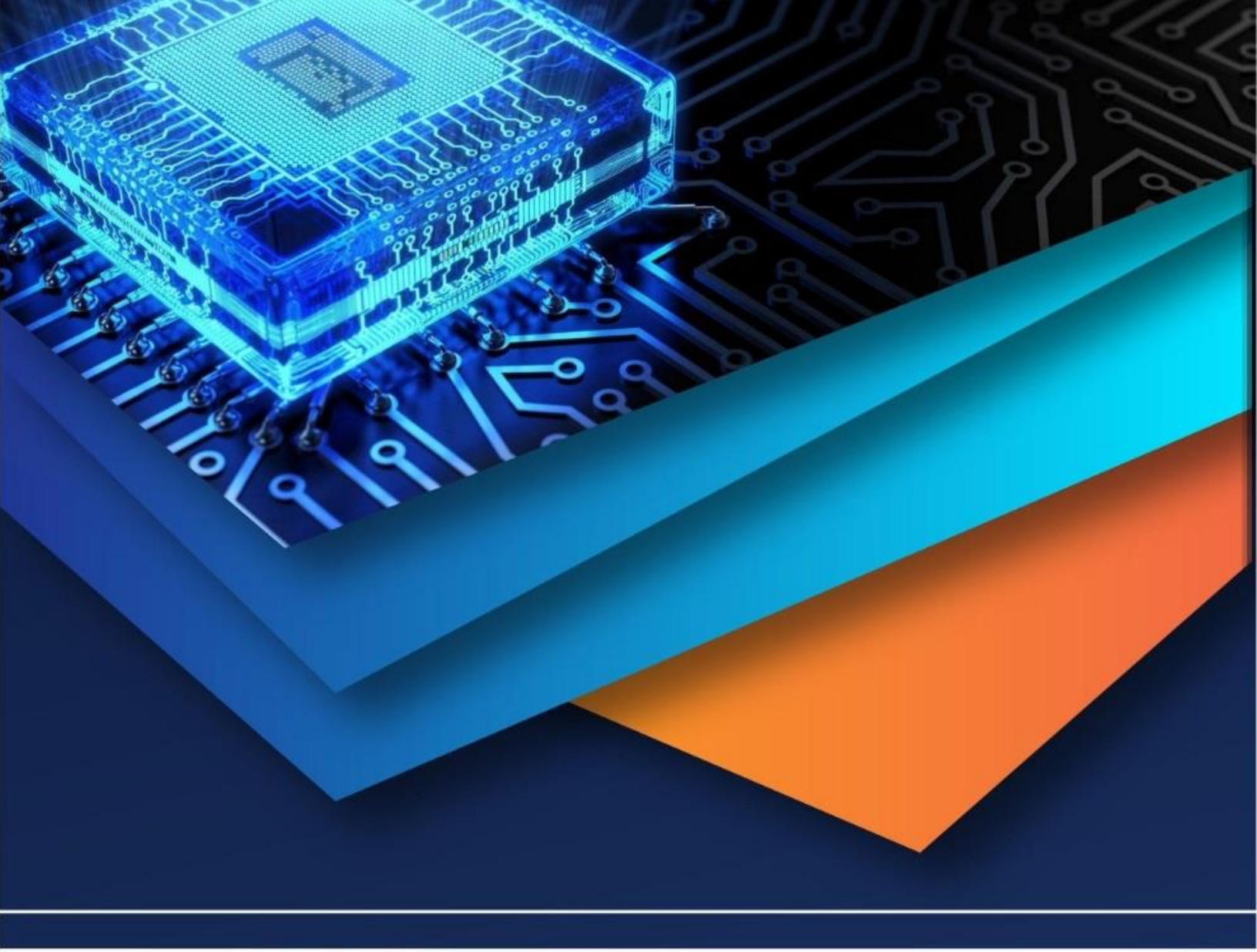
Though the suggested system can provide data security and reliability using decentralised cloud data, it has a number of security flaws. Different assaults against decentralized data exist, such as the Fork problem scale, to name a few. As a result, greater attention can be paid to preventing future attacks.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy Attribute-based encryption, Proc. of IEEE Symposium of Security and Privacy, Oakland, CA, USA, May 20-23 2007, pp.321-334.

[2] Z. Wan, J. Liu and Robert H. Deng, HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. IEEE Transaction on Information Forensics and Security, Vol. 7(2), 2012, pp.743-754.

[3] M. Li, S. Yu, Y. Zheng, K.Ren and W. Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption, IEEE Transaction on Parallel and Distributed Systems, January 2013, Vol.24, pp.131-143.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY