iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51636

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 11 Issue V May 2023- Available at www.ijraset.com

Secure Data Storage Using Erasure-Coding in Cloud Environment

Balakrishna Reddy Mule[1], Rishi Raj Kumar[2], Gude Srinivasulu[3], Gaddam Ranga Uday Sudheer[4], Dr. K. Bala[5]
[1, 2, 3, 4]*Student,* [5]*Professor, Department of Computer Scienceand Engineering, Bharath Institute Of HigherEducation and Research*

Abstract: ***The current storage mechanism currently stores user data on cloud servers. Thus, users give up their rights. You don't have control over the data and run the danger of privacy violations. Encryption technology is often the cornerstone of the traditional privacy protection strategies even if it is not very effective at thwarting assaults from within a cloud server because it cannot be fully analyzed from within. This paper's goal is to offer a fog computing-based three-layer storage structure for resolving the cloud storage issue. Frameworks like the one this study suggests can be utilized to fully utilize cloud storage while preserving user privacy. The Hash-Solomon coding technique also enables the segmentation of data. Then, to ensure privacy, a small amount of data can be stored on local computers and fog servers. The theoretical safety study and experimental assessment have demonstrated the feasibility of our proposal, which is a major advance over the existing cloud storage method. If one data component is missing, all the data information is lost. We shall demonstrate the effectiveness of the system as we secure it. Using this computational intelligence-based method, it is also possible to calculate the distribution percentage that is stored in clouds, fog, and local computers. Through theoretical safety analysis and experimental evaluation, our strategy—which represents a significant improvement over the current cloud storage strategy—has been demonstrated to be workable. If one data component is missing, all the data information is lost. Additionally, the distribution fraction saved can be determined thanks to the computational intelligence employed in this method.***

Keywords: Cloud computing, Erasure coding, BCH Algorithm, Bucket, Access Control List.

I. INTRODUCTION

Like how electricity is outsourced, the phrase "cloud computing" in computer science refers to a kind of outsourcing of computer services. Users can use it with ease. They don't need to worry about the process or the source of the power. Each month, they pay for their usage. The underlying idea of cloud computing is similar: Each server's capacity to safeguard user privacy can be guaranteed by dispersing the user's access to storage, computing power, or specifically designed development environments. This enables consumers to utilize these resources without having to think about how they function. Most of the cloud computing is comprised of Internet-based technologies. The internet is shown in computer network diagrams as a cloud, which is a metaphor and, as such, an abstraction that conceals the intricate internet architecture. It is a kind of computing where related activities are provided "as a service," enabling customers to access technology-enabled services through the Internet (or "in the cloud") without being conscious of or in control of the technologies underpinning these servers. Fog computing, which alludes to the rising challenges in objectively gathering information, includes large data structures and wide cloud systems. As a result, poor-quality content is produced. Fog computing may have a variety of implications on large data and cloud systems. Although this problem can be viewed from a single consistent perspective, inaccurate content distribution has been addressed by the development of metrics that aim to increase accuracy. Networking is made up of a control plane and a data plane. For instance, computing services might be located at the network's edge rather than on servers in a data center thanks to fog computing on the data plane. The problem of erroneous material distribution has been addressed by the development of measurements that aim to increase accuracy, even if this problem can be regarded from a single, recurrent perspective. In contrast to cloud computing, fog computing places an emphasis on closeness while still being applicable in AAL contexts. To protect user privacy, we advise using a TLS architecture based on fog computing. Users' privacy can be successfully protected by the TSL design while yet giving them some amount of administrative authority. As was already said, it is difficult to repel the internal attack. While conventional techniques can stop external attacks, they are useless when CSP is having problems. Our proposal employs encoding technology to divide user input into three sections of different sizes rather than using standard techniques. They will all be missing some essential details required for secrecy. The three data components will be kept on the user's local workstation. Likewise, the idea of fog computing. Furthermore, there are numerous security issues with cloud storage.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

There is a split of data ownership and management for these users since they have no actual control over how their data is physically stored. A theoretical safety study shows that the concept is feasible.

The ratio of data blocks stored on various servers can be appropriately distributed to ensure the privacy of data on each server. The encoding matrix is impenetrable in theory. Hash transformation can also be used to preserve incomplete information. The results of the experiment test showed that it was possible to use this method of encoding and decoding without compromising the effectiveness of cloud storage.

II. METHODOLOGIES

A. Login Module

This activity is offered to the user as soon as they enter the website. The user must enter a working phone number and the password they choose upon registration in order to access the website. If the user's input matches the data in the database table, they can successfully access the website; otherwise, a notice indicating that the login attempt failed is displayed, and the user must provide the proper information again. A link to the register action is also made available when registering a new user.

B. Registration Module

If a new user wants to access the website, they must first register before they can log in. The register activity will begin if you choose the register option during the login procedure.

C. Storage Module

This module applies three different levels of encryption on the original data. The data in each layer can be encrypted using a variety of cryptographic techniques and an encryption key before being saved in the cloud.

D. Recovery Module

Users may access their files using this module from three different storage servers: local computers, fog servers, and cloud servers. We are using the Hash-Solomon coding approach in this situation to split the data into different sections, as seen in the image below. If one data component is missing, the data information is lost.

III. ALGORITHM

A. BCH Code Algorithm

These codes are made up of a large family of powerful random error-correcting cyclic codes known as the Bose, Chaudhuri, and Hocquenghem (BCH) codes. An amazing generalization of the Hamming code for many errors is this family of codes. The only binary BCH codes considered in this lecture note are those. Non-binary BCH codes, such as Reed-Solomon codes, will be explored in the lecture note that follows.

IV. EXISTING SYSTEM

1) Cloud computing technology has advanced in recent years.
2) Unstructured data has rapidly increased, sparking increased demand in cloud storage and propelling innovation.
3) The advancement of computer technology has been fast.
4) The aforementioned tasks make use of Hash-cloud computing has evolved throughout time as a consequence of the work of numerous people.
5) The current storage approach keeps all of a consumer's data fully on cloud servers, putting them in danger of losing their privacy and control over it.
6) Encryption technology is frequently the foundation of privacy protection strategies.
7) These methods fall short in their attempts to prevent inside-the-cloud server assaults.

A. Disadvantage

Alterations in risk perception as a result of expanding the datacenter onto the cloud. Low latency and localization.

©IJRASET: All Rights are Reserved

B. Proposed System

1) The framework can utilize the full amount of cloud storage while maintaining data privacy.
2) If one data component is missing, we lose the data information.
3) The proposed framework employs algorithms based on the bucket concept.
4) To reduce data loss and processing delays, our system uses the bucket notion.
5) We are using the Bose-Chaudhuri- Hocquenghem (BCH) coding algorithm. Highly adaptable, BCH code is used in numerous communications applications and has a low level of redundancy.

V. INPUTS AND OUTPUTS

The interface between the user and the information system is provided by the input design. It entails creating policies and procedures for data preparation, which calls for carrying out the necessary procedures to convert transaction data into a format that can be processed. Users have the option of immediately entering data into the system by typing it in or reading it from a written or printed document while gazing at the computer. User interaction with the information system is facilitated by the input design. It involves developing rules and practices for data preparation, which requires carrying out the necessary steps to transform transaction data into a format that can be processed. User interaction with the information system is facilitated by the input design. It involves developing rules and practices for data preparation, which requires carrying out the necessary steps to transform transaction data into a format that can be processed. What coding convention or order should the data be in? the discussion that directs comments from operations employees. the steps to take while creating input validations and what to do if there are mistakes. If an output meets the user's needs and presents the data in an understandable way, it is regarded as being of high quality. Any system has outputs that communicate the processing outcomes to users and other systems. The most important factor in output design is how the data will be used as the user's primary source of information. The system's capacity to support users in decision-making is increased through effective and clever output design.

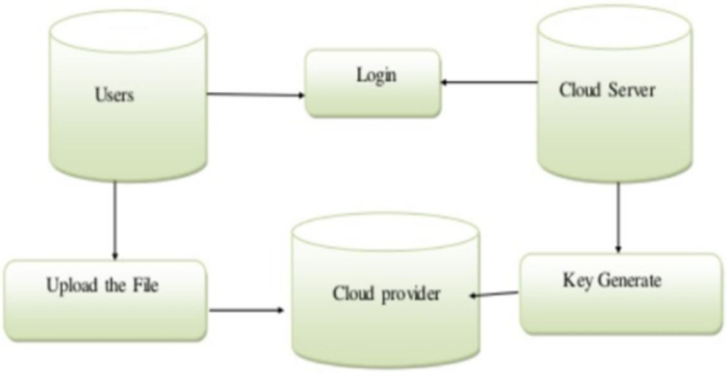
VI. DATA FLOW DIAGRAM

A data flow diagram (DFD), which is a two-dimensional graphic, demonstrates how information is processed and transported in a system. Each data source is represented visually along with the interactions it has with other data sources to achieve a common result.

Before drawing a data flow diagram, one must first: • Identify external inputs and outputs; • Determine the relationships between the inputs and outputs; and • Visually represent how these connections relate to one another and what happens as a result.

VII. ROLE OF DFD

1) This documentation support is understandable to both programmers and non-programmers. DFD does not take into account how procedures are carried out, just what they accomplish.
2) An actual DFD makes assumptions about who processes the data and where it moves.
3) It helps analysts to identify areas of interest in the company and evaluate them by looking at the data that enter the process and how they are changed when they leave.



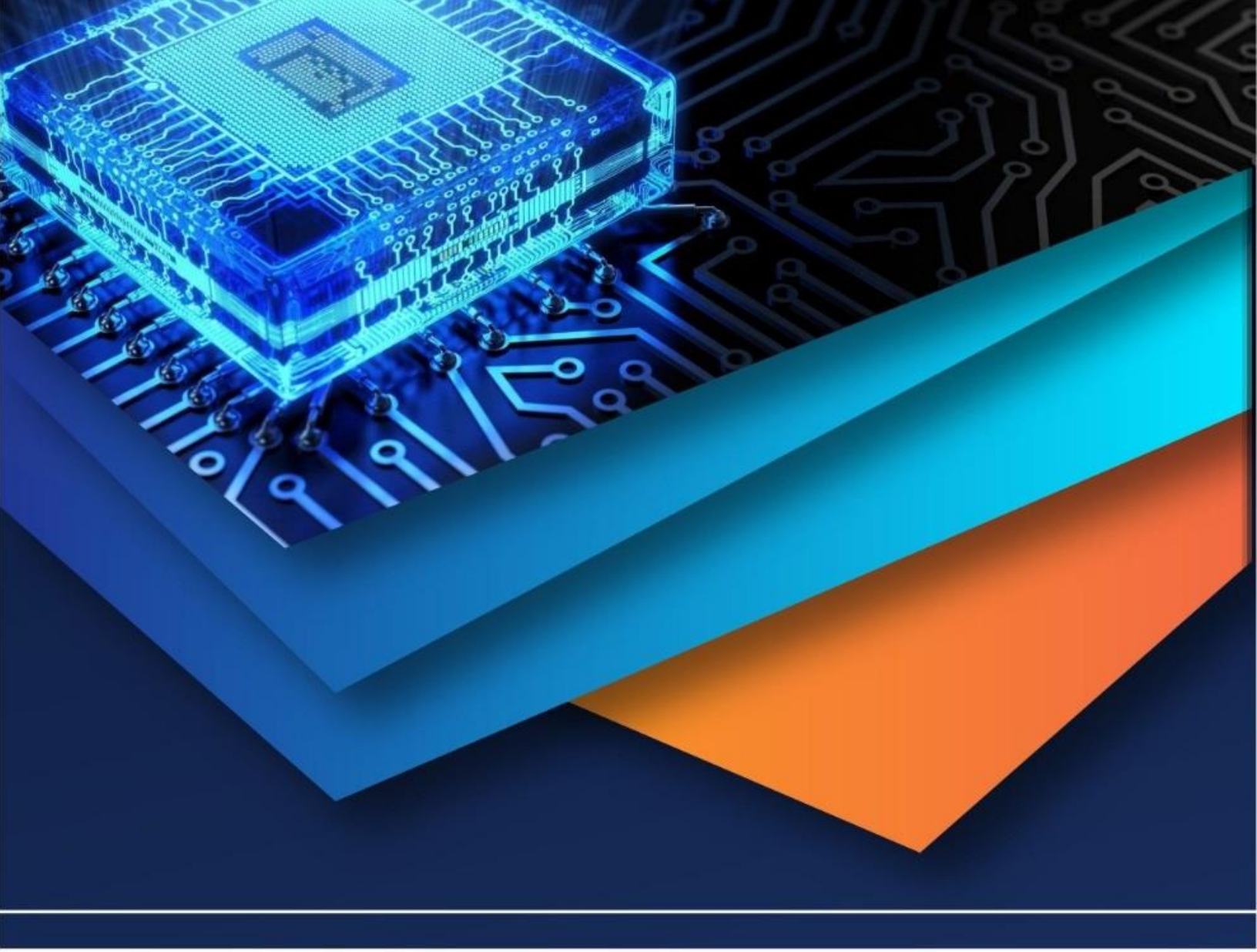
VIII. CONCLUSION

The rise of cloud computing has several benefits. Technology called cloud storage makes it easier for users to increase their storage capacity. However, there are a few security concerns with cloud storage as well. Since they do not really have control over how their data is physically kept, users who store their data in the cloud frequently experience a separation of ownership and management of their data. This is the area where cloud computing has attracted a lot of interest. We create a BCH Code technique and offer theoretical safety analysis, which has shown the idea's validity. The confidentiality of the data on each server may be assured by carefully distributing the number of data blocks kept among many servers. Theoretically, decoding the encoding matrix is not possible. Additionally, it is possible to use this method of encoding and decoding without compromising the effectiveness of cloud storage. To achieve maximum efficiency, we also create a logical, all-encompassing efficiency plan.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.
[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud Computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput, vol. 13, no. 18, pp. 1587–1611, 2013.
[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual Machine and bandwidth allocation in software defined network (sdn) and Cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.
[4] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data Storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.
[5] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv.Comput, 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.
[6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process. vol. 31, no. 3, pp. 464–472, 2016.
[7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-Solomon Codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.
[8] J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.
[9] R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence In wireless sensor networks: A survey," IEEE Commun. Surv. Tuts, vol. 13, no. 1, pp. 68–96, First Quarter 2011.
[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy preserving And copy-deterrence content-based image retrieval scheme in Cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,pp. 2594–2608, Nov. 2016.
[11] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted Urban data sharing framework for ubiquitous-cities," Pervasive Mobile Comput, vol. 41, pp. 219–230, 2017.
[12] Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, "Privacy-preserving smart Semantic search based on conceptual graphs over encrypted outsourced Data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.
[13] J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture Research," J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)