iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56893

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 XI Nov 2023- Available at www.ijraset.com

A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption

Dr. C. Dhanusha[1], B. Kamaladharshini[2]
MCA., MBA., M.Phil., PGDCA., Ph.D., Assistant professor, Department of Software Systems and Computer Science, KG college of Arts and Science, Coimbatore, Tamilnadu, India
Department of Software Systems and Computer Science, KG college of Arts and Science, Coimbatore, Tamilnadu, India

Abstract: This work is entitled "A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption". In today's digital era, the need for secure storage mechanisms is paramount due to the increasing amount of sensitive data being generated and shared. Cloud storage has emerged as a popular solution for storing and accessing data remotely. However, concerns about data privacy and security have arisen, leading to the development of innovative approaches to ensure the confidentiality and integrity of stored data. Cloud computing provides a solution to reduce the adverse environmental impacts and saves energy.

I. INTRODUCTION

Cloud computing has shown remarkable development in recent decades. In the era of cloud computing, secure storage of data is of utmost importance to protect sensitive information from unauthorized access and data breaches. To address these concerns, our project focuses on developing a cloud secure storage mechanism based on data dispersion and encryption techniques. This project draws the attention on the various methods enforced on the cloud environment to make it more energy efficient. One of the main objectives considered in cloud computing is to provide reliable QoS(Quality Of Service).It refer to technology that manages data traffic to reduce packet loss , latency and jitter on the network. While the use of fault tolerance mechanisms through redundancy improves query reliability in the presence of unreliable wireless communication and sensor faults, it could cause the energy of the system to be quickly depleted. Therefore, there is an inherent trade-off between query reliability vs. energy consumption in query-based wireless sensor systems. This system is implemented using python.

A. Technology Used

Data dispersion involves breaking the data into smaller pieces and storing those pieces across multiple locations or servers in the cloud. This dispersal technique enhances data security and availability. Data encryption ensures the confidentiality of data even if it's stored in the cloud. Pattern Matching for dispersed and encrypted data to maintaining data integrity. TPA (Third Party Auditing) used in CSSM (Cloud Secure Storage Mechanism) for auditing and verifications. TPA can access to the necessary information and keys to verify the integrity and correctness of the dispersed and encrypted data**.**

II. PROBLEM STATEMENT

In the current digital landscape, the continued reliance on traditional storage methods has become a prominent issue. Organizations adhering to conventional on-premises servers and physical storage devices face several pressing challenges. One of the primary concerns is the inherent limitation in scalability, as traditional storage solutions struggle to accommodate the exponential growth of data in a cost-effective manner. Additionally, the maintenance and management of on-premises infrastructure demand substantial financial and personnel resources, posing financial constraints for many organizations. Security is another critical problem, as local storage lacks the sophisticated encryption and redundancy features often inherent in modern cloud storage solutions.

A. Purpose of the Study

The purpose of the study on cloud storage represents a transformative paradigm in information technology, offering scalable, flexible, and cost-effective solutions for organizations to store, access, and manage their data. This project aims to design a secure storage mechanism that leverages data dispersion and encryption techniques to safeguard the confidentiality and data integrity. By dispersing data across multiple locations and applying robust encryption protocols, the study seeks to mitigate the risks associated with unauthorized access and data breaches, ensuring the protection of user information.

©IJRASET: All Rights are Reserved

B. Objective

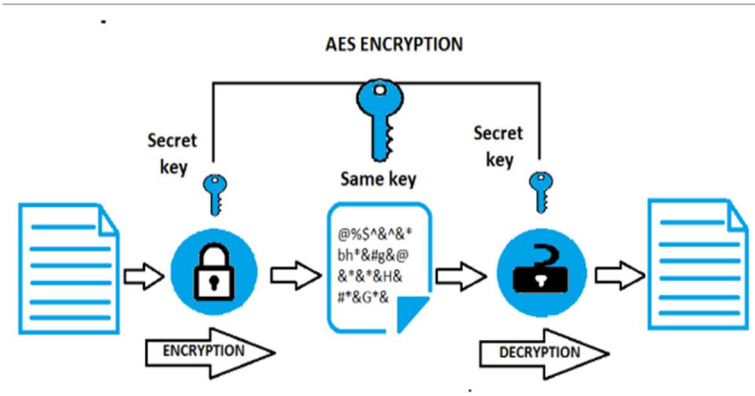
1) The proposed *Cloud Secure Storage Mechanism* is an application that provide data integrity, data privacy and compliance for the cloud user.
2) Cloud storage provides easy and convenient access to data from anywhere with an internet connection. This accessibility is particularly useful for remote work, collaboration, and data sharing.
3) Cloud storage maintain history of user data can be stored in a secure and cost-effective manner. This data can be retrieved when needed for reference or compliance purposes, even if it is not accessed frequently.

III. METHODOLOGY

1) *User Login/Register Module:* The cloud user can register and login to the application to store the datas in cloud.
2) *User Cloud Operations Module:* User cloud operations constitute the interactions and activities that users perform within the cloud storage environment. This module focuses on providing a seamless and secure experience for end-users. Users can perform operations such as uploading, downloading, updating and managing files, with the assurance that their data is subjected to the prescribed dispersion and encryption protocols. The user cloud operations module also includes features like access control mechanisms, ensuring that only authorized users can retrieve or modify specific data.
3) *Cloud Service Provider Module/Admin Module:* A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing Systems. The Admin Module serves as a crucial component within the cloud service provider's infrastructure. This module is designed to facilitate the efficient and secure management of the cloud storage environment. Administrators can utilize the admin module to oversee user access permissions, monitor system performance, and manage data dispersion strategies.
4) *Third Party Auditing Module:* The Third-Party Auditing Module is integrated to provide an additional layer of transparency and accountability. PA will verify the data before storing it on the cloud. There are large number of users of cloud computing who are accessing and modifying the data and they need the reliable service provider who can provide complete security for their data, So the TPA will audit the data and check data integrity of client data.

IV. ALGORITHM

In the Cloud Secure Storage Mechanism, the Advanced Encryption Standard (AES) algorithm plays a pivotal role in fortifying the security of stored data. Utilizing AES, a symmetric key encryption algorithm, enhances the confidentiality aspect of the project's security measures. AES operates by employing a secret key to encrypt and decrypt data, ensuring that only authorized parties with the correct key can access the information. In the context of data dispersion and encryption, AES serves as a cornerstone in the encryption process, ensuring that each fragment of dispersed data is securely encoded. The strength of AES lies in its widespread adoption, proven security, and efficiency, making it a well-established choice for safeguarding sensitive information in cloud storage environments. The encrypted data, when dispersed across multiple locations, further enhances security by reducing the risk of a single point of compromise. This combination of data dispersion and AES encryption not only addresses the confidentiality concerns associated with cloud storage but also aligns with contemporary best practices for ensuring the robust protection of data in transit and at rest within the cloud infrastructure.



Advanced Encryption Standard Algorithm

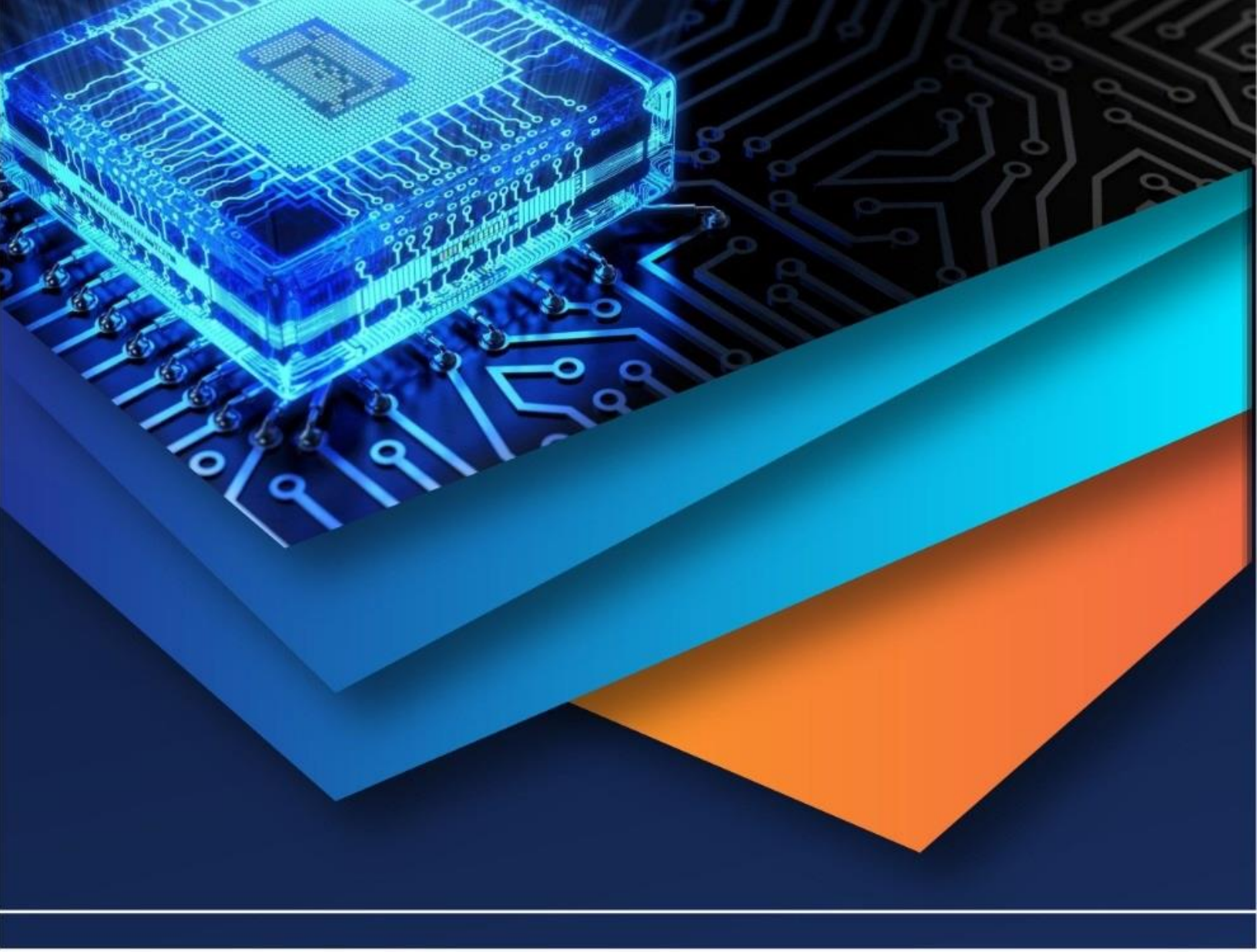
V. CONCLUSION

This project aims to develop a secure cloud storage mechanism that leverages data dispersion and encryption to address the challenges of data security and privacy. By dispersing data across multiple nodes and employing encryption, we enhance data security, mitigate the impact of potential breaches, and protect the confidentiality of stored information. This mechanism has the potential to provide individuals and organizations with a trustworthy and secure cloud storage solution for future reference and the protection of their valuable data.

REFERENCES

[1] https://aws.amazon.com/cloud-computing
[2] https://www.techtarget.com/searchcloudcomputing/tip/cloud-computing
[3] https://cloud.google.com/learn/what-is-cloud-computing
[4] https://www.geeksforgeeks.org/cloud-computing/
[5] https://www.javatpoint.com/cloud-computing
[6] Behavior-based attacks recognition in IoT-oriented industrial control systems,'' IEEE Access, vol. 8, pp.104956–104966, 2020
[7] Secure attribute-based data sharing for resource limited users in cloud computing,'' Comput. Secur., vol. 72, pp. 1–12, Jan. 2018.
[8] The OpenStack Project. Possible Glance Image Exposure Via Swift. Accessed: Feb. 23, 2015. https://wiki.openstack.org/wiki/OSSN/OSSN-0025
[9] Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: Aug. 8, 2018. https://downloads. cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloudcomputing-deep-dive.pdf
[10] Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation, Comput. J., vol. 60, no. 8, pp. 1210–1222, Feb. 2017.
[11] Securing cryptographic keys in the IaaS cloud model, in Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Comput. (UCC), Limassol, Cyprus, Dec. 2015, pp. 397–401.
[12] Securing cryptographic keys in the cloud: A survey, IEEE Cloud Comput., vol. 3, no. 4, pp. 42–56, Jul. 2016.
[13] Verifiable privacy preserving single-layer perceptron training scheme in cloud computing, Soft Comput., vol. 22, no. 23, pp. 7719–7732, Dec. 2018.
[14] Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: Aug. 8, 2018, https://downloads. cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloudcomputing-deep-dive.pdf
[15] Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing, Inf. Sci., vol. 379, pp. 42–61, Feb. 2017

©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)