International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

# SECURED ORGANIZATIONAL CLOUD STORAGE USING MESSAGE DIGEST ALGORITHM

**[1]HARISH.M, [2]KENNETH KISHORE KUMAR.E , [3]ABISHEK.R.R , [4]NALINI POORNIMA.S**

[1,2,3,] IV Year B.Tech CSE Students, Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, MADURAVAYOL, CHENNAI-95, TAMIL NADU, INDIA

[4,] Assistant Professor, Dept of Computer Science and Engineering, DR MGR Educational And Research Institute, MADURAVAYOL, CHENNAI-95, TAMIL NADU, INDIA

[1] harishtaker024@gmail.com,[2] kennethkishorekumar@gmail.com,[3] abishek0461@gmail.com

***Abstract*—** The Secure Organizational Cloud Storage System is an advanced cloud storage platform designed specifically for organizations that prioritize data security. The platform provides a similar functionality to Google Drive, but with enhanced security features to ensure that sensitive information remains safe from cyber threats. With the Secure Organizational Cloud Storage System, organizations can store and manage their data in a centralized and secure location. Users can easily upload, share, and collaborate on files and documents, and can access them farom anywhere with an internet connection. Secure cloud storage is indispensable in today's data-driven world, providing the convenience of remote data access while mitigating the risks associated with cyber threats and data breaches. By implementing advanced encryption, access controls, data integrity checks and redundancy strategies, secure cloud storage systems offer a comprehensive solution to protect sensitive information in an increasingly interconnected digital ecosystem. This abstract serves as a concise introduction to the importance and key components of secure cloud storage. Cloud service and storage providers offer valuable IT solutions for businesses of all sizes. Originally thought of as more for personal use, cloud storage for business is following in the footsteps of many personal technologies adapted for business purposes. Cloud storage works by storing data on remote servers, where it can be maintained, managed, backed up and accessed remotely. Data stored in the cloud is accessible by any device at any time, as long as permissions are in place. Despite its accessibility, data stored via the cloud is extremely safe and secure. Many people reap the benefits of the cloud for personal reasons, but most businesses have yet to take the leap. Whether your current on-premises data storage seems sufficient, or you simply haven't taken time to consider cloud storage, reviewing these advantages is a good place to start.

## 1. INTRODUCTION

Secure Organizational Cloud Storage System, organizations can store and manage their data in a centralized and secure location. Users can easily upload, share, and collaborate on files and documents, and can access them from anywhere with an internet connection Cloud storage allows you to save data and files in an off-site location that you access either through the public internet or a dedicated private network connection. Data that you transfer off-site for storage becomes the responsibility of a third-party cloud provider. The provider hosts, secures, manages, and maintains the servers and associated infrastructure and ensures you have access to the data whenever you need it. One of the key features of the Secure Organizational Cloud Storage System is its advanced security protocols. The platform uses industry-leading encryption and authentication methods to ensure that data is protected from unauthorized access. Additionally, the system employs multi-factor authentication to provide an extra layer of security for users. Private cloud storage setups typically replicate the cloud model, but they reside within your network, leveraging a physical server to create instances of virtual servers to increase capacity. You can choose to take full control of an on-premises private cloud or engage a cloud storage provider to build a dedicated private cloud that you can access with a private connection. Organizations that might prefer private cloud storage include banks or retail companies due to the private nature of the data they process and store.

Secured cloud computing environments with high-level security are essential in today's digital landscape, where organizations rely on cloud services to store, process, and manage their data and applications. In this introduction, we'll explore the concept of a secured cloud computing environment and the key principles and technologies that contribute to its high-level security. Cloud computing is a technology paradigm that allows users to access and use computing resources (e.g., servers, storage, databases, networking, software, analytics) over the internet on a pay-as-you-go basis. Major cloud service providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

## 2. RELATED WORKS

Here in this paper the authors "L.S. Ezema, C.K.A. JoeUzuegbu, J. N. Eneh, and I. Amanze" have proposed and implemented a reliable, secure, fast, and efficient system replacing a manual and unreliable system. The system can be implemented in many organizations and institutions. This system will save time, reduce the amount of work the administrator must do and replace the stationery material with an electronic device. Hence, a system with the expected results has been developed but there is still room for improvement.

The authors Alomari, H. M., & Othman, Z. A. (2018). Secure Organizational Cloud Storage System for Small and Medium Enterprises. Journal of Engineering and Applied Sciences introduces such a solution called SFSData, which secures data and information stored locally or through some cloud facility.

The authors Liu, S., & Wang, X. have proposed Secure Data Storage Techniques in Cloud Computing. International Journal of Advanced Computer Science and Applications. proposed system improves the security in cloud storage framework using different encryption algorithms like AES algorithm with S- box and Feistel Algorithm. The structure utilizes the information-transferring, cutting, ordering, encryption, merging, unscrambling and recovery cycle to make sure about the enormous information put away in the multi cloud. Cryptographic algorithms are mostly used for sending data over a network in a secure manner and to store data in a system in non-human readable form.

Here in this paper the authors Gao, Y., Li, M., & Li, M. (2020). Secure Data Storage in Cloud Computing is described as a project that allows users to store data on remote servers. It can be a good option for protecting data from cyberattacks because it's often backed up regularly and stored off-site. The efficiency and functionality of SED improves the usability in client-side. Finally, the comparing results show that the performance of our scheme is superior to that of the existing schemes.

## 3. SYSTEM METHODOLOGY

In our proposed system, we have given access control and the authentication level of security by using two authentication techniques; At any instant of time, these users cannot use all the services provided by the cloud. As a result, by taking the needs of the users and cost-effective benefits into consideration, pay per service would be a viable solution for the cloud computing scenario. Users only pay for those services which they use for a particular duration. Individual users and organizations benefit from cloud computing services, which allow permanent online storage of files. The problem occurs when companies store highly confidential documents on cloud servers. Therefore, this paper aims to introduce a backbone structure for a cloud storage system where the security and personal privacy is highly maximized. It is obvious that cloud computing servers are highly protected against unauthorized access, but in some cases these files stored can be accessible by the maintenance staff. Full protection is needed to ensure that the files stored in the server are only accessible to owners.

## 4.OVERVIEW

Secured cloud storage is a dynamic framework determined by the rigorous implementation of advanced safety techniques and procedures that ensure the safety of data within cloud-based storage services. This new framework, known for its scalability and ease meets the different needs of individuals and companies seeking efficient data management over the enormous surface of the internet. However, the imperatives of strengthening the security architecture become paramount, given the underlying hazards connected with illegal access, potential data breaches, and a wide variety of security threats. In combination with encryption, the use of strong hashing and digesting message algorithms offers

an extra degree of protection. Hashing algorithms serve an important role in converting data into a fixed-length string of characters known as a hash. These irreversible alterations maintain data integrity, as even little changes to the original materials result in a drastically distinct hash value. At the same time, message digest algorithms deliver a unique fixed-size production, termed for its digest or hash, which serves as a digital signature for data. The integration of these cryptographic approaches strengthens the overall security posture by ensuring data integrity and authenticity.

## 5. SYSTEM ARCHITECTURE

### 5.1 DATA ACCESS MODULE:

This is the framework responsible for accessing, mainting, updating data. It typically consists of an Admin Login, processing unit, and storage for data to be stored. When an individual enters the credentials their access level will be synced with the account on the module, it reads the username which can be any social media accounts and processes it to extract unique features that can be used for accessing data for storing, viewing, sharing and verification.

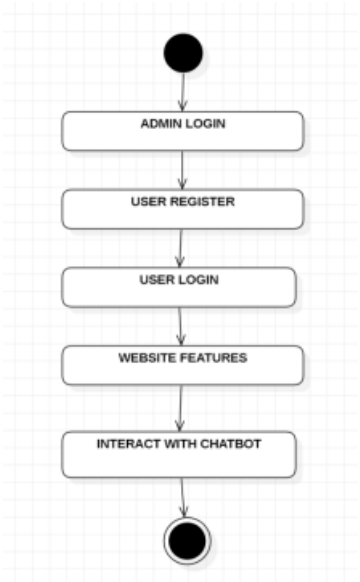


*Figure 4. Architecture of the proposed system*

### 5.2 MSQL:

The MYSQL acts as the database that interfaces with the registration module. It reads data from the login module, processes it, and then communicates with external services. These tools are often used fortheir connectivity and processing capabilities.

### 5.3 FIREBASE:

Firebase is a popular mobile and web application development platform offered by Google. It includes various services, including a real-time database, authentication, and cloud functions. Firebase can be used to securely store and manage stored data in real-time, making it accessible to applications and users.

Firebase includes a real-time SQL database where confidential data can be stored. This database is accessible from various platforms, and it ensures data synchronization in real-time. Firebase also provides data security and user authentication features.

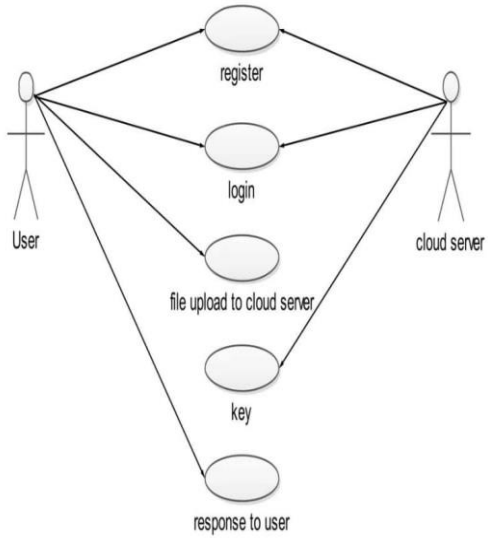


*Figure 5. Process of storing and connection to server.*

## 6. RESULT AND DISCUSSION

Obtain the necessary software components like database, web service provider and other required sensors or devices. Set up software tools, including XAMPP, and Firebase for cloud-based storage and development environment for the application. Connect all the modules to the system, install and ensure proper connection and communication between the two components. Develop the interface code to capture and

process encryption of data, allowing for functions like enrollment and identity verification. Implement code on the data access for processing data, implement logic for user data tracking, including identifying unique and confidential data to the firebase, and enable MQTT connection to facilitate communication with other components. Create a red storage account, set up a new account, and obtain the necessary credentials. Create accounts to interact with Firebase real-time database, defining the structure for storing data and user information.We develop local host websites for user-facing applications. Develop the application code, enabling users (clients, administration) to interact with data, generate reports, and manage and analyze and set access control for information.Conduct unit tests for each component to ensure they function correctly. Perform system integration testing to verify seamless working cloud and fast responsive storage algorithm. Install the system component in the educational institution. Provide training for end-users on how to use the system effectively. Implementing these data sophisticated security measures will shield your organization's cloud-stored data from an enormous number of potential threats. Visualize that information as virtual protected by strong encryption methods, multiple levels of authentication, and strict access limits. The implementation of network traffic reduction algorithms ensures that the data path between your device and cloud servers is streamlined and efficient, reducing needless transmission volumes. This not only speeds up data transport but also helps to make cloud computing more cost-effective.Hashing algorithms such as MD5 as well as SHA serve as digital personal information, adding an extra degree of security. They serve like sentinels, constantly ensuring the authenticity of your data.

## 7. CONCLUSION

In Conclusion, secure cloud storage has become a critical component of modern data management, providing the convenience of remote access while addressing the ever-present concerns of data security, privacy, and reliability. The rapid evolution of technology and the continuous emergence of new threats have driven the development of robust security measures and innovative solutions in the realm of cloud storage.Secure cloud storage systems have made significant strides in safeguarding data, with advancements in encryption, access control, data integrity verification, and redundancy strategies. These measures collectively work to protect data both at rest and in transit, ensuring its confidentiality, integrity, and availability.

The functionalities of the system can be further enhanced through the following recommendations:

- Zero-Knowledge Encryption: Zero-knowledge encryption, also known as client-side encryption, allows data to be encrypted and decrypted only on the user's device. Cloud providers cannot access or decrypt the data. Future enhancements may include making zero-knowledge encryption more user-friendly and accessible.

- Homomorphic Encryption: This is a form of encryption that allows computation on encrypted data without decrypting it. It enables secure processing of data in the cloud without exposing sensitive information.

- Quantum-Resistant Cryptography: With the advent of quantum computing, traditional encryption methods may become vulnerable. Future cloud storage systems may incorporate quantum-resistant cryptographic algorithms to protect data.

- Multi-Factor Authentication (MFA): Expanding the use of MFA, including biometric authentication, for accessing cloud storage accounts will enhance security. Future enhancements may include more seamless and user-friendly MFA methods.

- Secure Access Control: Advanced access control mechanisms will be developed to ensure that only authorized users and devices can access cloud-stored data. This might involve continuous monitoring and adaptive access controls.

- Data Residency and Privacy Regulations: As data privacy regulations evolve, cloud storage providers will need to offer more granular control over data residency and compliance with various international data protection laws.

- Blockchain for Data Provenance: Blockchain technology can be used to track and verify the origin and changes to data stored in the cloud, enhancing data integrity and auditability.

- Machine Learning for Anomaly Detection: Machine learning algorithms can be used to detect anomalies and potential security breaches in real-time. Future cloud storage systems may incorporate advanced AI and ML for threat detection.

- Immutable Storage: Immutable storage ensures that once data is written, it cannot be modified or deleted, making it resistant to data tampering and ransomware attacks.

- Data Classification and Tagging: Automated data classification and tagging can help identify sensitive data and apply appropriate security controls based on data sensitivity.

- Data De-Identification: Techniques for de-identifying sensitive data while preserving its utility will become more important to meet privacy requirements.

- Advanced Threat Intelligence: Integration with threat intelligence services and sharing of threat information among cloud providers will become more common to proactively protect against emerging threats.

- End-to-End Encryption for Collaboration Tools: Secure cloud collaboration tools will offer end-to-end encryption to protect data shared between users.

- Incident Response and Recovery: Advanced incident response and disaster recovery capabilities will be integrated into cloud storage services to minimize downtime and data loss in the event of a security incident.

- User Education and Awareness: Increasing user education and awareness about best practices for secure cloud storage will remain a critical aspect of security enhancements.

- Regulatory Compliance Automation: Automating compliance checks and reporting to meet regulatory requirements will be a focus to reduce the burden on organizations.

- Red Teaming and Penetration Testing: Continuous red teaming and penetration testing will help identify vulnerabilities and weaknesses in cloud storage systems.

## REFERENCES

[1] Al-Kasasbeh, R., & Al-Ani, A. (2019). Cloud Storage Security: Challenges, Solutions and Future Directions. Journal of Cloud Computing: Advances, Systems and Applications, 8(1), 1-17.
[2] Alomari, H. M., & Othman, Z. A. (2018). Secure Organizational Cloud Storage System for Small and Medium Enterprises. Journal of Engineering and Applied Sciences, 13(11), 4165-4172.
[3] Arshad, N., & Sohail, S. (2018). Secure Data Storage Techniques in Cloud Computing. International Journal of Advanced Computer Science and Applications, 9(3), 225-231.
[4]Chaudhary, S., & Kaur, P. (2019). Cloud Storage Security: A Review of Techniques and Challenges. International Journal of Computer Science and Mobile Computing, 8(8), 91-96.
[5] Fang, W., Zeng, L., & Wang, L. (2019). Secure and Efficient Data Storage in Cloud Computing. International Journal of Distributed Sensor Networks, 15(6), 1-12.
[6]Gao, Y., Li, M., & Li, M. (2020). Secure Data Storage in Cloud Computing: A Review of Techniques and Challenges. IEEE Access, 8, 2813-2823.
[7]Liu, S., & Wang, X. (2018). Research on Secure Cloud Storage System Based on Blockchain. Journal of Physics: Conference Series, 1067(4), 042005.
[8]Lu, Y., Jiang, L., & Li, G. (2018). A Secure Cloud Storage System Based on Cryptography and Access Control. IEEE Access, 6, 11349-11359
[9]Al-Sabbagh, M. (2018). Secure and Efficient Cloud Storage: A Review of Cloud Storage Services and Techniques Journal of Cloud Computing: Advances, Systems and Applications, 7(1), 1-21.