Privacy-Preserving Data Access with Key-Aggregate Encryption

T. Ramya[1], Dr. Bhuvaneswari.M[2]
Department of Computer Applications
[1]PG Student, Dr. M.G.R. Educational and Research Institute, Chennai - 95.
[2]Associate professor, Dr. M.G.R. Educational and Research Institute, Chennai - 95.

Abstract- *Secure Cloud Storage is an online platform for storing user data with sharing facilities among other users. The data is optionally encrypted before storing and decrypted on download by the system and the process is transparent to the end user. The platform also provides marking data private or public such that all public data are visible to end user and can perform search or download request to the owner. The data owner or user can audit all such request and grant download access to individual or multiple files accordingly. Each file on our system is encrypted using different AES key and the real challenge come when multiple file needs to be shared between users.*

Keywords: *Aggregate Key, Individual Keys, Fine-grained Access Control, Efficient Data Sharing, Privacy Preservation, Cloud Storage, Healthcare.*

I. INTRODUCTION

Electricity is essential to modern civilization. However, power outages occur from time to time in various parts of the world, causing significant economic damage and social impacts. For example, in 2019, the Guri hydroelectric plant, which produces 80 percent of Venezuela's electricity, was maliciously attacked, resulting in blackouts in 21 out of 23 states [1].

In the same year, a widespread blackout also occurred in South America, affecting more than 40 million people in Argentina, Brazil, Uruguay and Chile. When such an accident occurred, traffic lights stopped working and all public transport was stopped, throwing the affected cities into chaos [2].

It is generally accepted that smart grids are the basic infrastructure for renewable energy. Smart meters are essential devices for implementing two-way communication in smart networks, so they are vulnerable targets for attackers. Therefore, it is worth investigating methods that securely transmit information in smart grids and build a flexible smart grid architecture[3].

It is necessary to build an information security model that meets the security requirements of the smart grid. To solve this problem, various privacy-preserving data fusion schemes have been proposed in the literature. In addition, these works can be divided into two main categories: one protects users' energy consumption data, and the other protects users' identity[4].

In a hierarchical way, a new encryption system is proposed that supports homomorphic re-encryption, where ciphertexts can either be decrypted or re-encrypted, both of which require the decentralized work of two parties. However, most existing data collection solutions require a trusted third party[5].

II.LITERATURE SURVEY

According toYun Wang.et al.,2023 The continuous development of cloud technology requires technologies that protect user privacy even from cloud service providers themselves, such as multi-user searchable encryption. It allows data owners to optionally allow users to perform keyword searches against encrypted data stored in the cloud[6].

According toNingning Wang.et al.,2019 The integration of portable wireless devices and cloud computing into electronic health systems has greatly improved their efficiency and availability. Patients can upload their personal health information (PHI) to the cloud, where healthcare providers (HSPs) can get the information they need to determine their health status[7].

According toBakkiam David Deebak.et al.,2022 The integration of sensor technologies and cloud computing covers design aspects of electronic health systems. It has its own application area that can be used to upload clinical data of patients and medical procedures to the cloud server in IOT[8].
According toJoonYoung Lee.et al.,2022 Cloud server and fog computing have been used to manage huge amounts of data with low service delivery time in the Internet of Things (IoT) environment. However, unreliable connections between network entities and the cloud server cause many security problems[9].

According toHuang Minmin.et al.,2023 With its promising security and decentralized features, blockchain offers a significant opportunity to break through privacy protection issues in the edge computing paradigm. However, when edge actors send security tasks to the domains of the decentralized blockchain network, they can expose their privacy and local privacy[10].

III.PROPOSED SYSTEM

The proposed system aims to elevate the existing platform's capabilities by integrating advanced features and functionalities designed to improve user experience, security, and efficiency. By leveraging the power of Key-Aggregate Encryption (KAE) and other cutting-edge technologies, the proposed system will provide a secure, user-friendly, and robust platform for privacy-preserving data access and management.

ARCHITECTURE DIAGRAM:

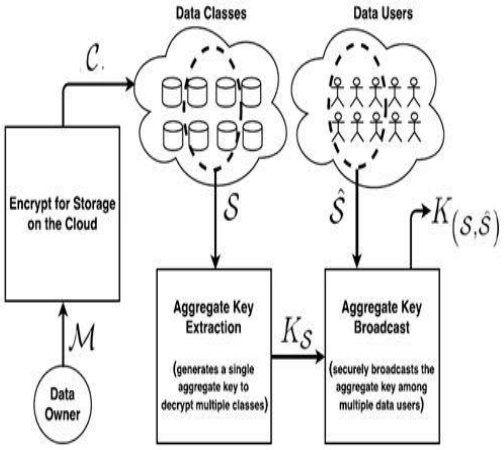

Fig. 1: A Desirable Online Data Sharing Scheme

Explanation:
Data Owner: The entity that possesses the data and wants to share it securely while maintaining privacy.

Data Users: Entities or users who are authorized to access the encrypted data.

Key Generation: The data owner generates a unique encryption key for each user and keeps a record of these keys.

Encryption: The owner of the data encrypts the data using unique encryption keys for each user. This ensures that each user can extract only a portion of their data.

Key-Aggregate Encryption: This is the core technique where a single aggregate key is generated by combining the individual encryption keys of authorized users. This aggregate key allows authorized users to collectively decrypt the data without the need for the data owner to distribute multiple keys.

Key Distribution: The owner of the data securely distributes the master key to authorized users.

Decryption:Authorized users use the master key to decrypt data. Each user has access to only part of the data encrypted with his own key.

Access Control:The owner of the data can control access by managing the master key. Users can be added or removed by updating the build key accordingly.

Security: Appropriate security measures such as authentication, secure communication channels and key management policies are implemented to protect keys and data from unauthorized access.

Logging and Monitoring: logging and monitoring mechanisms can be implemented to control use of encrypted data and detect unauthorized attempts.

IV.RESULT AND DISCUSSION

Fig1.HOMEPAGE ADMIN LOGIN PAGE

a)HOMEPAGE:It offers a user-friendly gateway to explore our platform's services and features. Designed for clarity and engagement, it guides visitors effectively, highlighting our commitment to revolutionizing privacy-preserving data access through Key-Aggregate Encryption.

b)ADMIN LOGIN PAGE:The Admin Login page provides secure access for authorized administrators to manage our platform's backend. Built with robust security features, it ensures only authorized personnel can access sensitive data, reflecting our commitment to maintaining a secure environment using advanced encryption techniques.

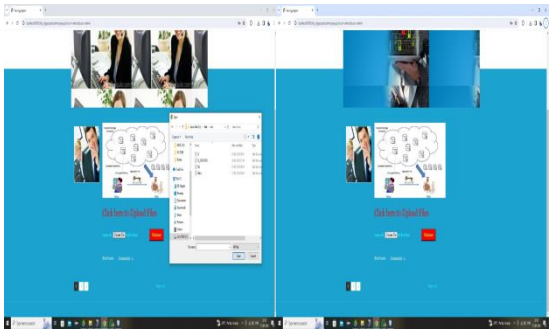

Fig2. FILE UPLOAD PAGE CHOOSE FILE UPLOAD

a) FILE UPLOAD PAGE:Our File Upload page offers a secure and user-friendly interface for seamless file uploading. With advanced encryption like Key-Aggregate Encryption, we prioritize data confidentiality and integrity, ensuring a smooth and trustworthy experience for users.

b) CHOOSE FILE UPLOAD:The "Choose File" feature simplifies file selection, enhancing user experience. Combined with robust security measures, users can upload files confidently, knowing their data is protected within our platform.

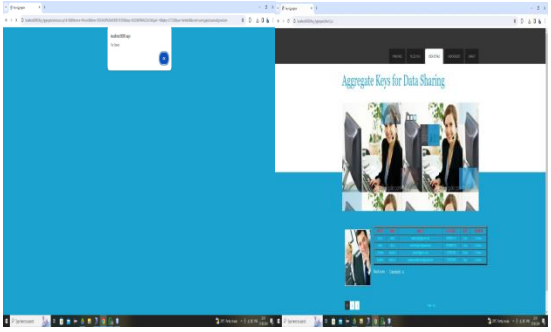

Fig 3. SHARE FILE VIEW ALL USER

a)SHARE FILE:Our Share File feature offers secure and intuitive file sharing. With advanced encryption like Key-Aggregate Encryption, we prioritize secure and controlled access for shared files, ensuring a seamless sharing experience.

b)VIEW ALL USER:The View All User feature simplifies user management for administrators. Designed with security in mind, it provides an overview of registered users while maintaining the integrity and confidentiality of user information within our secure platform.

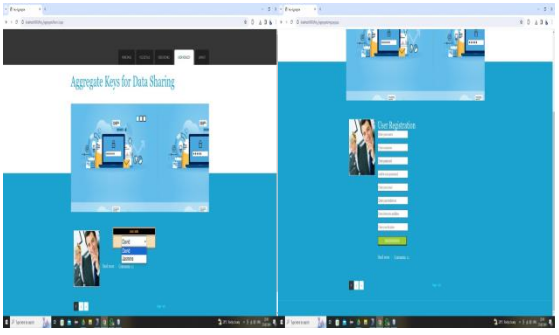

Fig4.USER REQUEST PAGE USER REGISTER PAGE

a)USER REQUEST PAGE: Our User Request page offers a streamlined and secure platform for users to submit access or permission requests. With robust security measures, we prioritize the confidentiality and integrity of user requests, ensuring a trustworthy experience.

b)USER REGISTER: The User Register feature provides a secure and user-friendly registration process. Designed for simplicity and security, it ensures the confidentiality and protection of user information using advanced encryption techniques within our platform.

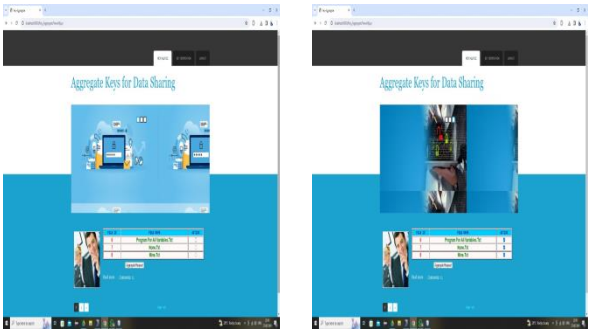

Fig5.VIEW ALL FILE AGGREGATE REQUEST

a)VIEW ALL FILE: The View All File feature provides administrators with a clear overview of uploaded files, enhancing file management. With robust security measures, we prioritize the confidentiality and integrity of stored data within our platform.

b)AGGREGATE REQUEST: The Aggregate Request feature allows users to efficiently request aggregated data from stored files. Designed for user-friendliness and security, it ensures privacy and controlled access to aggregated insights using advanced encryption techniques like Key-Aggregate Encryption.

V.CONCLUSION

Key-Aggregate Encryption (KAE) introduces a transformative approach to privacy-preserving data handling, providing a robust and efficient mechanism for secure data sharing. Using a master key, aggregate key, and individual keys, KAE enables fine-grained access control, allowing data owners to define and control access policies at a granular level. It facilitates secure and efficient sharing of encrypted data across industries, including cloud storage, healthcare and IoT applications. While KAE offers significant benefits in terms of privacy preservation and data security, it also involves challenges such as key management, performance overhead, and potential security risks. Careful implementation, management and continuous monitoring are necessary to reduce these risks and ensure the reliability and effectiveness of the encryption system. In conclusion, key pooled encryption is a powerful tool in the field of privacy protection technologies, paving the way for secure, efficient and privacy-friendly data exchange solutions. As organizations and

industries continue to prioritize data privacy and security, KAE plays a key role in shaping the future of secure data handling and sharing.

REFERENCES

[1] Fang, L.; Huang, L.; Zhao, Q. Discussion on megalopolis power grid safety from the perspective of Venezuelan blackout. Power Energy 2019, 40, 674–677.

[2] Gao, K.; Han, F.; Dong, P.; Xiong, N.; Du, R. Connected vehicle as a mobile sensor for real time queue length at signalized intersections. Sensors 2019, 19,

[3] Sheha, M.; Mohammadi, K.; Powell, K. Solving the duck curve in a smart grid environment using a non-cooperative game theory and dynamic pricing profiles. Energy Convers.Manag. 2020, 220, 113102

[4] Zhang, J.; Zhao, Y.; Wu, J.; Chen, B. LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT. IEEE Internet Things J. 2020, 7, 4016–4027.

[5] Zhang, M.; Chen, Y.; Lin, J. A privacy-preserving optimization of neighborhood-based recommendation for medical-aided diagnosis and treatment. IEEE Internet Things J. 2021, 8, 10830–10842.

[6] Yun Wang, Dimitrios Papadopoulos 2023,Multi-user collusion-resistant searchable encryption for cloud storage, IEEE Transactions on Cloud Computing.

[7] Chang Xu, Ningning Wang, Liehuang Zhu, Kashif Sharif, Chuan Zhang 2019, Achieving searchable and privacy-preserving data sharing for cloud-assisted E-healthcare system, IEEE Internet of Things Journal 6 (5), 8345-8356, 2019

[8] Bakkiam David Deebak, Fida Hussain Memon, Kapal Dev, Sunder Ali Khowaja, Nawab Muhammad Faseeh Qureshi 2022,AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT, Ad Hoc Networks 125, 102740.

[9] Jihyeon Oh, JoonYoung Lee, MyeongHyun Kim, Youngho Park, KiSung Park, SungKee Noh 2022, ieeexplore.ieee.org A secure data sharing based on key aggregate searchable encryption in fog-enabled IoT environment, IEEE Transactions on Network Science and Engineering 9 (6), 4468-4481.

[10] Huang Minmin, Yuan Lingyun, Pan Xue, Zhou Chuan 2023, Trusted edge and cross-domain privacy enhancement model under multi-blockchain, Computer Networks 234, 109881.