Optimized Cloud Storage Framework Utilizing Key Aggregate Searchable Encryption for Collaborative Data Sharing

Dr. R. Ushadevi[1], M. Viswanathan[2]

Department of Computer Science, SriKrishnasamy Arts & Science College, Sattur, Tamil Nadu, India

[1]ushadeviraj15[at]gmail.com
[2]mailforvichu[at]gmail.com

Abstract: ***Distributing encrypted data through cloud storage significantly enhances security in remote communication services. Symmetric-key encryption ensures that only users possessing valid keys can access and decrypt the information. Given the diversity of subscription models, efficient key management is essential for effective access control in broadcast services. The proposed solution utilizes a key tree structure (KTR) to manage key distribution, accommodating complex subscription preferences and user behaviors. This approach supports all subscription operations in wireless broadcast environments. Instead of maintaining separate key sets for each application, users need only a single key set for all their subscribed services. The KTR mechanism determines the minimum number of keys that must be updated to maintain broadcast security while minimizing rekeying overhead.***

Keywords: Searchable encryption, records sharing, facts privateers

1.Introduction

Cloud computing has emerged through the evolution and integration of existing technologies, providing a secure and efficient environment for users. Its primary objective is to enable users to utilize advanced computing resources without requiring deep technical expertise in managing each component. Cloud services aim to reduce costs while allowing businesses to focus on their core functions rather than being constrained by IT infrastructure limitations. A fundamental technology driving cloud computing is virtualization, which enables a physical hardware system to be divided into multiple virtual devices. These virtual devices can be independently managed and used for various computing tasks. Operating system–level virtualization creates a scalable network of independent computing resources, allowing underutilized hardware to be effectively allocated and employed. This flexibility helps speed up IT operations and improves cost efficiency by maximizing infrastructure usage. Furthermore, cloud computing automates resource provisioning, allowing users to request and deploy resources on-demand. Automation not only streamlines workflows but also reduces the need for manual intervention, minimizing human error and labor costs. To address business process challenges, cloud computing integrates concepts from Service-Oriented Architecture (SOA), breaking complex problems into modular services that can be combined to form comprehensive solutions. This approach standardizes and simplifies global access to cloud services (Wikipedia, 2021).

Broadcasting refers to the transmission of signals carrying content, such as television or radio programs, to a broad audience, which may include the general public or targeted groups. Scheduling organizes the sequence in which content is broadcast. Traditionally, broadcasting used radio waves or cable systems to deliver content, often simultaneously. Encryption technologies enable secure subscription-based services, such as pay-per-view channels, by ensuring that only authorized users can access certain broadcasts. Historically, the term “broadcast” originated from agriculture, describing the scattering of seeds over a large area, and was later adopted by radio engineers to describe the wide dissemination of radio signals. Broadcasting plays a crucial role in mass communication, with narrowcasting referring to targeting a specific, limited audience segment. In networking, broadcasting involves transmitting data packets where every device in the network potentially receives the packet, though its reach is typically confined to a local area. With the growing use of smart mobile devices and rapid advances in wireless technologies, there is increasing interest from both industry and academia in enhancing wireless data services. Broadcasting stands out as a highly efficient way to maximize limited Wi-Fi bandwidth, as it enables multiple mobile users to access data simultaneously. Over the years, commercial broadcast services have become widely available on wireless networks, with services like MSN Direct highlighting the feasibility of using broadcast methods for wireless data delivery (Direct MSN Service, 2021).

2.Related Work

Multi-User Searchable Encryption

There is extensive research available on searchable encryption, which includes schemes such as Symmetric Searchable Encryption (SSE) and Public Key Encryption with Keyword Search (PEKS) (Curtmola et al., 2006). In the context of cloud storage, keyword search under a multi-tenant environment is particularly common. In this scenario, a data owner wishes to share a file with multiple authorized users, where each user receives a trapdoor that enables them to perform keyword searches on the shared file. This concept is referred to as Multi-User Searchable Encryption (MUSE) (Chu et al., 2014). Recent research in this field generally applies a single-key approach combined with access control mechanisms to achieve the desired functionality (Yu et al., 2010). Typically, MUSE schemes assign the file's searchable encryption key to authorized users, and broadcast encryption methods are employed for coarse-grained access control. In addition, Attribute-Based Encryption (ABE) is applied to enable fine-grained access control during keyword searches. A major challenge in MUSE systems is effectively managing which users can access specific files while also reducing the number of shared keys and trapdoors required. Key Aggregate Searchable Encryption (KASE) provides an efficient solution by enabling scalable and practical multi-user searchable encryption that addresses these challenges (Boneh et al., 2004).

Group Data Sharing System Evaluation

To improve existing systems, implementing a caching-based strategy offers a more efficient way to conduct keyword searches. In this method, a single aggregate trapdoor is provided, allowing the cloud server to process keyword searches using the KASE framework (Liu et al., 2013). Notably, the computational cost of the key adjustment algorithm grows linearly with the number of documents, ensuring predictable and manageable performance as the system scales.

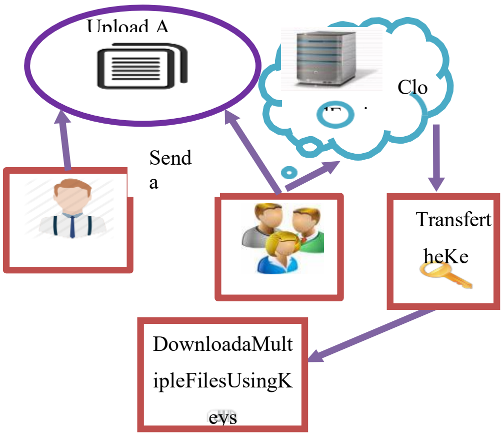

Figure 1: Architecture

3.Methodology Proposed System

The original concept of Key Aggregate Searchable Encryption (KASE) is introduced through the design of a practical KASE system. The architecture, as illustrated in Fig. 2, demonstrates an efficient structure composed of multiple interconnected modules to implement the KASE framework.

In this system, the data owner uploads files to a secure cloud storage platform. When an authorized user needs to access a file, they send a request to the data owner, who then provides an encrypted unique key, enabling the user to retrieve the required file securely.

The proposed KASE model is compatible with any cloud storage system that supports searchable data sharing functionalities. This allows a user to share a specific set of documents with a group of designated users, enabling them to perform keyword searches across the shared documents without compromising security. The overall framework consists of seven key algorithms that collectively support the system's operations: security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing. These algorithms work in harmony to provide secure, efficient, and flexible keyword search capabilities in a multi-user cloud environment.

Process Flow:

1. Setup Phase (DATA USER)
2. Encrypt Phase
3. Key Gen Phase
4. Key Aggregator
5. Decrypt Phase
6. Digital signature

Setup Phase (data user)

The setup algorithm takes no contribution aside from the implicit protection parameter. It outputs the community parameters PK and a grasp key MK.**3.2**

Encrypt Phase

Encrypt (PK, M, A). The encryption algorithm takes as enter the public parameters PK, a message M, and an admittance shape A above the creation of attributes.

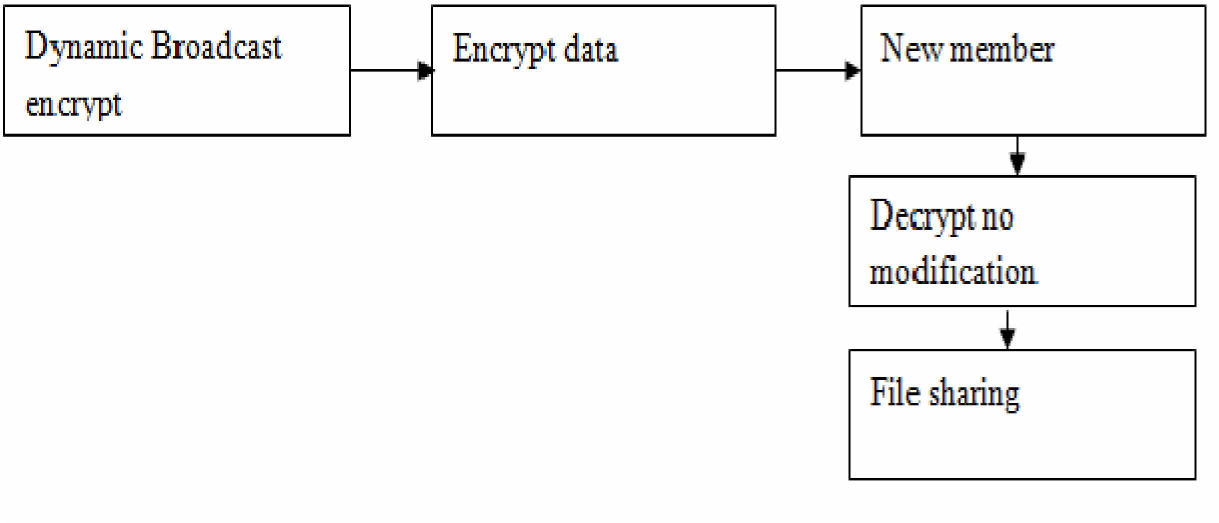

Figure 2: Encrypt Phase

The algorithm will encrypt M and build a cipher textCT such that simply a user that possesses a set of attributes that satisfies the access arrangement will be able to decrypt the significance. We will suppose that the cipher text implicitly contains A. The Figure 2 shows the procedure of encrypt phase and give the secure surroundings to admission the required file.

KEY GEN PHASE

The enter era set of rules takes as enter the master key MK and a placed of attributes S that specify the key. It outputs a non-public key SK.

Key Aggregator

The data owner sets up the system by generating public system parameters through the Setup process and creates a public/master-secret key pair using the Key Generation (KeyGen) algorithm. Anyone can encrypt messages using the Encrypt algorithm, specifying the type of ciphertext associated with the plaintext that needs encryption. The data owner can then use the master secret key to derive an aggregate decryption key for a defined set of ciphertext classes via the Extract function. These aggregate keys can be securely distributed to authorized users, either through secure emails or trusted devices. Subsequently, any user possessing the aggregate key can decrypt specific ciphertexts, as long as the ciphertext class is included within the scope defined by the aggregate key, using the Decrypt algorithm.

Decrypt Phase

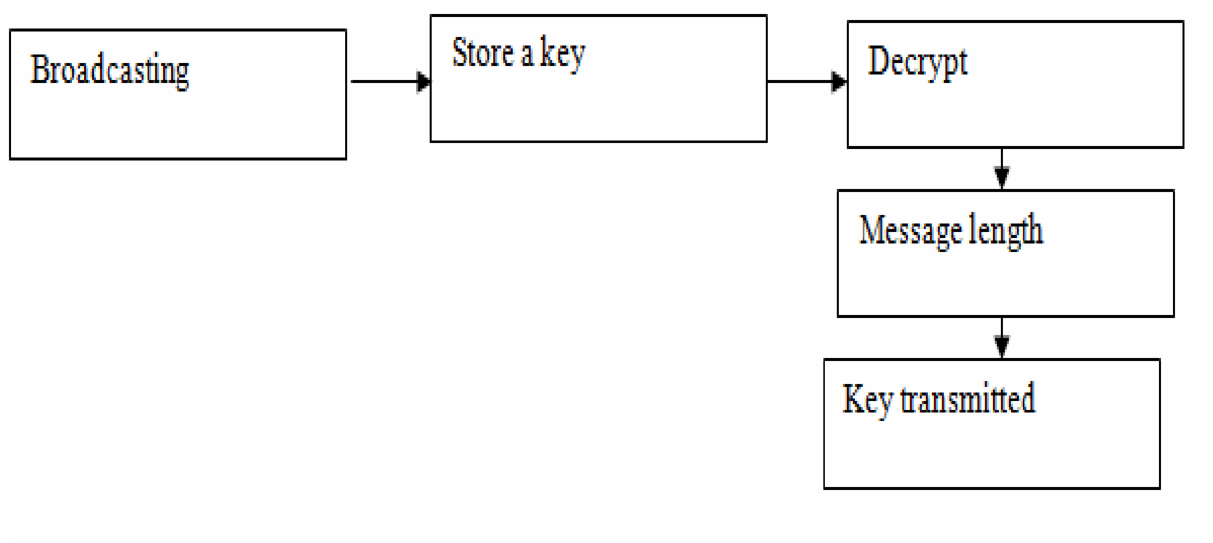

Figure 3: DecryptPhase

The decryption algorithm takes as input the public system parameters (PK), a ciphertext (CT) that includes an access policy, and a private key (SK) associated with a set of attributes S. If the attribute set S satisfies the access policy A embedded in the ciphertext, the algorithm proceeds to decrypt the ciphertext and returns the original message M.

Digital Signatures

A digital mark, which should not be mistaken for a digital certificate, is a numerical technique used to confirm the ig 4henticity and integrity of messages, software, or digital documents. Digital signatures provide an additional layer of assurance by verifying the origin, uniqueness, and validity of an electronic document, message, or business transaction, while also indicating the signer's informed consent.

Enhanced ID Entity Based Encryption Algorithm

Authentication and Signature Generation:

Alice authenticates with the Secure Key Generator (SKG) and receives her confidential key, EIDAliceEID_{Alice}EIDAlice. Using this key, Alice generates a signature σ\sigmaσ for a message MMM and sends it to Bob, possibly along with an encrypted supplementary message CCC.

Signature Verification:

Upon receiving MMM and σ\sigmaσ, Bob verifies whether σ\sigmaσ is a valid signature for MMM using Alice's identity IDIDID and the SKG's public key skSKGsk_{SKG}skSKG.

Acceptance or Rejection:

If the verification succeeds, Bob accepts the message. Otherwise, he rejects it. Importantly, Bob does not need to maintain any prior record for Alice.

Enhanced Identity-Based Systems (EIBS):

Enhanced Identity-Based Systems allow a user to derive a public key directly from a known identity value, such as an ASCII string. A trusted third party, the SKG, generates the corresponding private keys.

To set up the system, the SKG publishes a master public key while securely retaining the master private key (also called the master key).

Anyone can compute a public key corresponding to a given identity by combining the master public key with the identity value.

To obtain the matching private key, the user authorized for a specific identity contacts the SKG, which uses the master private key to generate the corresponding private key.

This approach allows users to encrypt messages or verify signatures without prior key distribution among parties, which is particularly useful in scenarios where pre-distribution is impractical. However, to decrypt or sign messages, the user must obtain the appropriate private key from the SKG. Therefore, the SKG must be partially trusted, as it can generate any user's private key and potentially decrypt or sign messages without authorization.

4.Performance Analysis

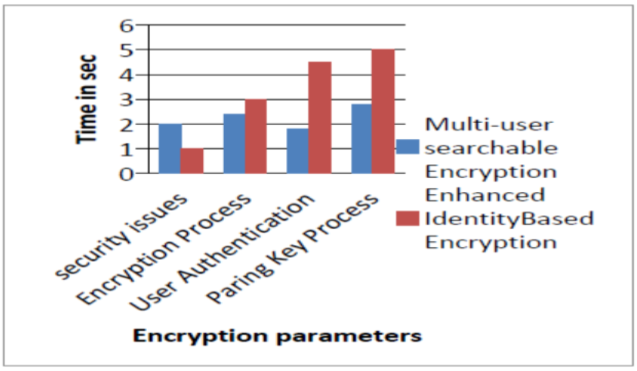

Figure 4: Performance analysis

Based on fig 4, the proposed Key-Aggregate Searchable Encryption (KASE) approach demonstrates more effective results in building practical data-sharing systems on public cloud storage compared to existing methods, particularly in terms of security, encryption, and the allocation of unique keys to authorized users.

5.Conclusion

Searchable encryption is an important cryptographic technique that has gained significant attention due to the widespread use of cloud storage services such as Dropbox, Microsoft OneDrive, Apple iCloud, and public cloud platforms like Amazon S3 and Microsoft Azure Storage. A practical searchable symmetric encryption (SSE) scheme should satisfy several key properties, including sub-linear (ideally optimal) search efficiency, adaptive security, compact storage, and the capability to support dynamic operations such as adding or deleting files and folders.

References

[1] Boneh, D., Goh, E.-J., Ostrovsky, R., & Persiano, G. (2004). *Public Key Encryption with Keyword Search.* EUROCRYPT 2004, pp. 506–522.

[2] Chu, C., Chow, S., Tzeng, W., et al. (2014). *Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.* IEEE Transactions on Parallel and Distributed Systems, 25(2), 468–477.

[3] Chu, C., Chow, S., Tzeng, W., et al. (2014). *Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.* IEEE Transactions on Parallel and Distributed Systems, 25(2), 468–477.

[4] Curtmola, R., Garay, J., Kamara, S., & Ostrovsky, R. (2006). *Searchable symmetric encryption: improved definitions and efficient constructions.* Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 79–88.

[5] Liu, X., Zhang, Y., Wang, B., & Yan, J. (2013). *Mona: secure multiowner data sharing for dynamic groups in the cloud.* IEEE Transactions on Parallel and Distributed Systems, 24(6), 1182–1191.

[6] Yu, S., Wang, C., Ren, K., & Lou, W. (2010). *Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing.* Proc. IEEE INFOCOM, pp. 534–542