Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Cloud files Storage System with Encryption

Namrata Goundadkar
Msc Computer
Savitribai Phule Pune University

Prof Suyash Patankar
Swaraj College, computer Science Department
Savitribai Phule Pune University

Article History:
Received: 06-08-2025
Revised: 27-09-2025
Accepted: 26-10-2025

Abstract:

Without relying on a third party, attribute-based encryption (ABE) offers safe data storage and sharing to data owners in cloud contexts. The previous ABE schemes only had one authority for end-user verification, resulting in a bottleneck at a single point for performance and security. The guarantee the privacy and verification of various attribute subsets, too many multi-authority approaches are offered. However, single-point bottleneck problems are difficult to resolve in many systems. In this proposed research project, the system presented a secure data transmission in cloud settings by focusing on a multi-authority verification mechanism called Robust Access Control (RAAC), a Role Base Access Control (RAC) component. With RAAC, various authorities, middleware, and other trusted parties may share the master and private keys by taking advantage of (t out of n) threshold secret sharing. An authorized user may create a secret key by working with any public authority on the transaction. The PBEWithMD5AndDES encryption offers the best level of data protection when combined with key with middleware authority and two kinds of cipher text policies. Furthermore, we create a method to verify several users concurrently and provide consistent data to end users by skillfully combining the traditional multi-authority system with RAAC. The experimental study also demonstrates how superior the current techniques to the new ones are.

Keywords—RBAC, PBEWithMD5AndDES encryption scheme; secure user Revocation; Proxy Key Generation, Role Base Access Control (RBAC)

INTRODUCTION

Cloud computing is a new and fast-growing technology. Used in the field of computation and data storage, which provides services for owners to outsource data. In cloud computing, data security is a major obstacle, especially in public cloud storage. So confidentiality, integrity and access of data become more vulnerable in cloud environments. To eliminate the collusion attack in public cloud environment. Implement the access control system for group base as well individual user base. Successfully implement a user revocation and proxy key generation system.

Users' eligibility to use various services is always determined by their roles and titles. The function of such a mechanism is performed by a framework known as role-based access

control (RBC), which explains how access restrictions are implemented between users and services. Users are connected to roles connected to role services when using RBAC. Many businesses and organizations utilize this framework to apply the requirements of their internal access control systems to their computer systems. For instance, if a firm's programmer has access to both the backend and front-end source code, the quality assurance team of that company only has access to the source code mentioned above. It should be emphasized that RBAC is a flexible framework; that is, roles are typically employed in a trans-organizational way. Although this access control is often used inside an organization, it should be noted that RBAC is a varied framework. For instance, students are often allowed to buy books at reduced costs. Users' roles and titles are often used to differentiate between those eligible to use certain services and those not. This kind of mechanism was sculpted because of a framework called role-based access management (RBAC), which outlines the access management connection between users and services. Users are connected to roles inside RBAC, and roles are connected to the services they utilize. Many companies and organizations utilize this architecture in their computer systems to meet their requirements for internal access control. For instance, the programmer can access a business's backend and front-end supply code. However, the quality assurance staff can only access the front-end supply codes.

It should be noted, however, that RBAC may be a flexible framework; that is, roles are frequently employed in a trans-organizational way. Although this access management is commonly used inside a business, it should be noted that RBAC can be a versatile framework. For instance, students can often shop for books at lower prices than the general public.

I. LITERATURE SURVEY

According to [1] Combining coordinate matching with Term Frequency-Inverse Document Frequency (TF-IDF) and enhancing the secure kNN approach allows MRSF to retrieve accurate ciphertext. It is possible because of the improved TF-IDF algorithm. In addition to this, it can effectively narrow the search rights of users via the use of a polynomial-based access approach. A formal security study demonstrates that MRSF is secure regarding the privacy of index and tokens and the confidentiality of data that has been outsourced.

According to [2] a safe Multi-authority CP-ABKS (MABKS) solution is needed to alleviate such restrictions and lessen the computation and storage load placed on cloud-based systems' resource-limited devices. In addition, the MABKS system's functionality has been expanded to include support for malicious attribute authority tracing and attribute updating. According to the detailed findings of our comprehensive security research, the MABKS system has selective security in both the selective matrix and the selective-attribute models.

According to [3] they have a structure allowing safe data exchange in the smart grid. IPE stands for "inner product encryption," which is the method used by the scheme. In this particular architecture, the access policy and the attribute set are rendered ambiguous by being converted into two vectors. Users can only receive the shared data correctly when the two vectors are orthogonal. In addition, our system allows the threshold access policy to include attribute name indexes. Sensitive attribute value information is not included in the shared data, ensuring that the attributes' privacy is maintained. In addition, to make our method more effective, we have included a testing stage. They help us only do operations that are essential before retrieving data. In conclusion, our performance study and trials have shown the advantages of the suggested architecture.

According to [4] The author suggests the first revocable large universe decentralized MA-ABE that does not involve key abuse and is based on prime order bilinear groups. The strategy that has been provided makes it possible to dynamically expand the capacity of qualities, users, and authorities. It provides static security in the random Oracle model while operating under the premise of q-DPBDHE2 and protects against key abuse attacks that any party may initiate. The ciphertext can only be successfully decrypted using the secret key if it is owned by the person who has the secret key. Using their legal key, the data user cannot construct a key distinct from their legal key to access the access key. Even though the access policy is met by the characteristics it controls, neither the CSP nor the authority can produce the accessible decryption key or decode the ciphertext by using the keys they possess. It is the case even if they both hold the keys. A user-attribute revocation method that is both effective and efficient is provided, and the suggested technique requires just a small number of processes to perform decryption.

According to [5] when installing such a system, many implementation difficulties must be addressed and proposed solutions for, such as data encryption and decryption, key storage, and key distribution. The implementation issues and possible solutions include encrypting and decrypting data and storing and distributing keys. In response to these problems, we have proposed a variety of potential remedies, each of which comes with its own set of benefits and drawbacks. These insights might be used by a system designer to better tailor the system to the requirements of the application being developed.

According to [6] a technique known as LW-C-CP-ARBE, which stands for lightweight collaborative ciphertext policy attribute role-based encryption, was developed to offer fine-grained and lightweight access control for mobile cloud environments. We adopt the CP-ABE technique as the primary cryptographic access control and provide a novel proxy re-encryption (PRE) protocol to lessen the burden of data re-encryption and decryption on mobile users. The achieve this goal, the overhead involved in conducting the cryptographic process on the end-user device is kept to a minimum.

According to [7] There is also a technique known as linear secret sharing, which has the potential to improve access policy significantly. In addition, two components make up each attribute, namely the name of the attribute and its definition. The possibility of covering essential judgments of traits is the aspect of this context's freedom that stands out as the clearest. And about PHR, it will provide high levels of security to customers. In the proposed system, the size of the public parameters is similar, and the cost of decryption is simply two pairing operations, which progressively reduces it to zero. In the long run, we establish that the solution provided by using the dual system encryption strategy in the regular model under static assumptions offers total security. It is just a mechanism for partially masking information, which the suggested plan accomplishes. The problem, which involves rapid encryption that will be left as a chore for the future, is intriguing and finishes off a covert objective.

According to [8] Enhance the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) framework by integrating two supplementary modules. These added components are aimed at strengthening fine-grained access control mechanisms while simultaneously preserving the confidentiality and integrity of the protected data. It makes encryption and hashing systems easier to implement. We compared the newly suggested framework to previously established frameworks using the CP-ABE approach. It demonstrates that the SecHS provides superior characteristics to protect the data of healthcare services. In an ideal scenario, the requirements for data security, including privacy, integrity, and fine-grained access control, must be

satisfactorily addressed to properly ensure data sharing in an environment that operates under cloud computing.

According to [9] There will be a presentation of a PHR-tiered CPABE system with numerous authorities. The hierarchical PHR is encrypted using a protocol that merges many distinct access structures. This structure is the basis for the encryption. On the other hand, it does not have a single or central authority that can be trusted among numerous authorities. In addition, the suggested method is immune to the collusion assault brought on by (N1) compromised authorities out of a total of N authorities. Because the conventional decisional bilinear Diffie–Hellman issue cannot be solved, the security of this protocol is semantically safe. [citation needed.

According to [10] A brand new technique known as linear secret sharing with multiple values has the potential to enhance the presentation of access policy significantly. In addition, each attribute has two components: the attribute name and the value associated with that attribute. The ability to conceal potentially sensitive attribute values is. As a result, the most evident benefit of the approach that has been offered. And it can do a good job of protecting users' privacy in PHR. Using the static assumptions from the standard model, we can eventually demonstrate that the suggested scheme has a high level of security thanks to the dual-system encryption approach.

II. PROPOSED METHODOLOGY

Figure 1 below illustrates the architecture of the proposed system, outlining its various phases and operational flow. The system incorporates Attribute-Based Encryption (ABE) along with cloud storage integration. Attribute authorities are utilized to handle user authentication and revocation processes. In existing models, multiple certificate authorities are typically needed for user verification, which can be time-consuming. However, the proposed approach eliminates this dependency by introducing a Trusted Third Party (TTP) to streamline verification.

A. Architecture

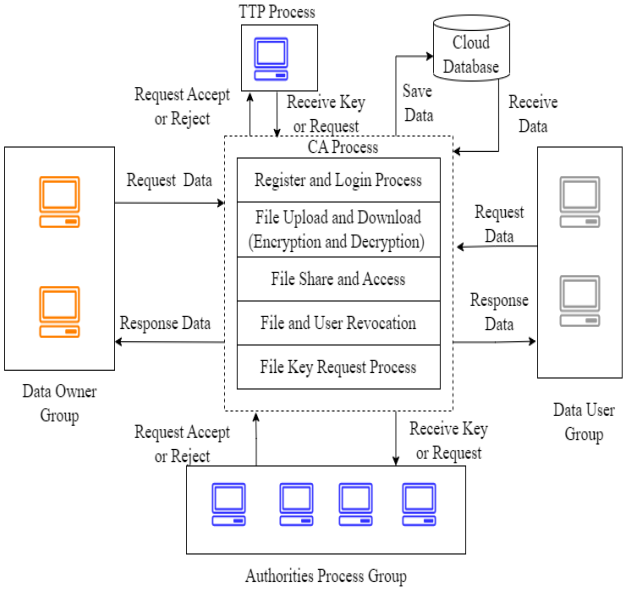

Figure1. System Architecture

B. Methodology

Registration and Authentication: In that phase all entities can register. Data owner, AA's, TTP and user can create own profile.

Data Uploading: In first phase once data owner uploads the file. In that module data encryption done using PBEWithMD5AndDES encryption scheme and the same time keys send to EC2 Cloud. Data Owner will upload file for his backup and can allow the file to be accessed by friend user. He will be able to access the uploaded file by entering proper credentials sent to his registered email id. Files uploaded by user will get scan by algorithm and if similar contents are there in old and current new file then previous file will get stored. Common files in which all contents are exactly similar if gets uploaded on the system by multiple users will get registered as the first owners file and others can access it as friend user which will avoid duplication of file at server.

Data Sharing: In that phase data sharing done by data owner, he can any file to any user in cloud group. Friend user can access the shared file to him by data owner by following the login process and proper credentials send to him for that particular file.

Access Control and revocation: In access control any user can view or access the file shared by user to him. In revocation data owner can revoke the file access to specific user. The common files uploaded by multiple users can't be deleted will get deleted according to maximum requirement time specified by out of multiple users.

Cloud Storage Service Provider (CSP): The provider of cloud storage services provides database services. It makes it possible for the data owner to store any information. The user is also given the ability to design their user-defined database schema while using CSP.

C. Algorithms

Algorithms 1 : Encryption and Decryption

Key Create Phase

Step 1: Initialize a character array R_data with 5 randomly generated characters using the char.random method.

Step 2: Convert the character array R_data into a string and store it in the variable Key_data.

Step 3: Return Key data

Encryption

Input: plain text data p, and key k

Output; cipher text C

Step 1: Establish a new instance of PBEWithMD5AndDES.

Step 2: Set the cipher instance to operate in encryption mode.

Step 3: Assign the original plain byte array to a new plaintext byte array.

Step 4: Encrypt the plaintext using the cipher and key 'k'

Step 5: Encode the encrypted byte array to a Base64 string

Step 6: return Encstring

Decryption

Input:

C: The ciphertext to be decrypted

k: The decryption key

Output:

p: The resulting plaintext after decryption

Step 1: The key k must be used to perform decryption.

Step 2: Configure the cipher instance to work in decryption mode.

Step 3: Decode the value of c using Base64 to obtain byte[] ks.

Step 4: Apply the decryption method on ks using the key k to get a byte[ ] utf.

Step 5: Convert the utf byte array into a string using the String class.

Step 6: Return the resulting plain text string.

Algorithms 2: Role Based Access Control Algorithms:

Input:

Email-ID: The user's email address used as an identifying attribute**.**

File Data: The actual content or payload of the file to be processed.

File key_data: The associated encryption/decryption key or metadata linked to the file.

Output: Rules are defined either as policy guidelines or as signature-based patterns**..**

Step 1: Initialize a data array named S_list[] to store the required elements.

Step 2: Set the initial values of variables Fa and Uk to 0, and retrieve the user's Email-ID.

Step 3: Load or read the contents of the FileData and the associated FileKey.

Fa← {file_key list [i . . . . . n]}

Uk← {User_ Email-ID List [i . . . . . n]}

Step 3: Iterate through each entry by reading Fa into the S_list.

if (key_data.equals(Fa) && userEmail.equals(Uk))

Then User File Share information show

Else

Display a message indicating that the user's file is not shared or accessible.

End for

Step 4: End Procedure

D. Objectives

- To study and analysis various cloud data security approaches in multi cloud environment
- To design and implementation of PBEWithMD5AndDES encryption scheme in proposed system architecture.

- To design and develop a new verification as well as authentication protocol between authorities and trusted third party.
- To explore and validate the proposed system results with various existing systems

E. Problem Statement

To design and implement a system for Robust Access Control (RAAC) which is the part of Role Base Access Control (RAC). The system need to eliminate the single point bottleneck problem in multi cloud environment.

III. RESULT AND DISCUSSIONS

Accurate matrices measurement is necessary for the evaluation of process efficiency. The app is installed on an Amazon EC2 public cloud console with an Intel 2.8 GHz i3 processor, a Java 3-tier architecture platform, and 4 GB of RAM. For system evaluation, we build two physical network devices with Wi-Fi and ten virtual machines on Amazon EC2 as a public cloud platform. After putting portions of the system into place, we successfully increased the system's production to a level that met our expectations. Table 1 displays the outcomes of applying the proposed PBEWithMD5AndDES algorithm to convert encrypted text to plain text and decrypt encrypted material.

Table 1: System Performance

File Data Size in KB	Encryption time (Milliseconds)		Decryption time (Milliseconds)	
	Existing	Proposed	Existing	Proposed
5	495	425	624	612
10	620	526	745	733
15	840	720	954	810
20	995	895	975	890

In the second phase of experimentation, the assessment was performed utilizing two widely recognized approaches: KP-ABE [11] and DAC-MAC [12]. Within the current framework, four key steps essential for authentication were identified. The resulting performance metrics, derived under multiple configuration settings using these established techniques, are depicted in Figure 3 below.

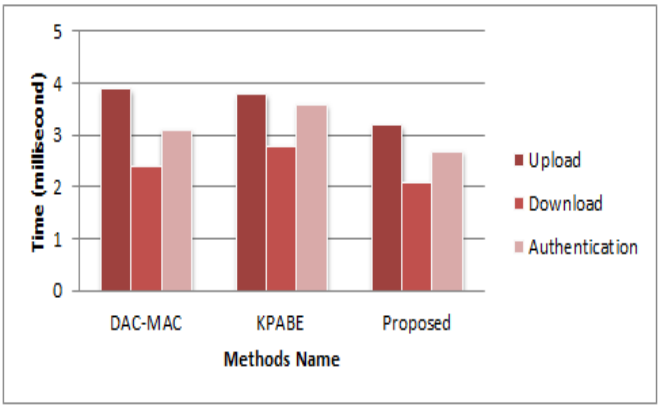

Fig. 3. Performance Analysis of the Proposed System

IV. CONCLUSIONS

In this study, the system proposes a safe method of data sharing using Role Base Access Control (RBAC) for use in untrusted environments such as those found in the cloud. The users of our system can get their master and private keys from the middleware authorities providers, and safe communication may be established between many parties thanks to this system. In addition to this, our method can enable safe revocation for users who cannot be trusted. Additionally, the production of proxy keys has been suggested in this study. When the data owner withdraws access rights from a specific user, the system promptly invalidates any existing keys and generates fresh ones for the remaining authorized users. This mechanism ensures optimal security and privacy levels at all times. Designed as a decentralized access control framework, the system supports efficient attribute revocation within multi-authority cloud storage environments. Importantly, it features a revocation capability, allowing dynamic control over data accessibility. It eliminates the burden of decryption that users have to bear according to characteristics. A secure attribute-based encryption scheme was introduced to ensure robust data privacy for cloud-based information sharing. This revocable, multi-authority access control mechanism incorporates verifiable outsourced decryption and also supports outsourced encryption. The approach is versatile and can be effectively applied to remote storage platforms, online social media, and similar environments. While the current system demonstrates strong security performance, it occasionally demands significant resource utilization. Allocating numerous resources can lead to increased interdependencies within the system. The next update should focus on minimizing resource use while maintaining maximum system flexibility in power, virtual machines (VMs), networks, and memory.

REFERENCES

[1]Li, Jiayi, et al. ”Practical multi-keyword ranked search with access control over encrypted cloud data.” IEEE Transactions on Cloud Computing 10.3 (2020): 2005-2019.

[2]Miao, Yinbin, et al. ”Multi-authority attribute-based keyword search over encrypted cloud data.” IEEE Transactions on Dependable and Secure Computing 18.4 (2019): 1667-1680.

[3]Zhang, Leyou, et al. ”Privacy-preserving multi-authority attribute-based data sharing framework for smart grid.” IEEE Access 8 (2020): 23294-23307.

[4]Huang, Kaiqing. ”Revocable Large Universe Decentralized Multi-Authority Attribute-

Based Encryption Without Key Abuse for Cloud-Aided IoT.” IEEE Access 9 (2021): 151713-151728.

[5] Phillips, Tyler, et al. ”Design and implementation of privacy-preserving, flexible and scalable role-based hierarchical access control.” 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). IEEE, 2019.

[6] Fugkeaw, Somchart. ”A fine-grained and lightweight data access control model for mobile cloud computing.” IEEE Access 9 (2020): 836-848.

[7] Rao, Reddy Veeramohana, et al. ”Attribute based Encrypted and Secured Cloud based Personal Health Record System.” European Journal of Molecular Clinical Medicine 8.2 (2021): 1501-1507.

[8] Satar, Siti Dhalila Mohd, et al. ”Cloud-Based Secure Healthcare Framework by using Enhanced Ciphertext Policy Attribute-Based Encryption Scheme.” Int. J. Adv. Comput. Sci. Appl 12 (2021): 393-399.

[9] Guo, Rui, et al. ”An attribute-based encryption scheme with multiple authorities on hierarchical personal health record in cloud.” The Journal of Supercomputing 76.7 (2020): 4884-4903.

[10] Zhang, Leyou, et al. ”Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system.” IEEE Access 7 (2019): 33202- 33213.

[11] Rajput, Amitesh Singh, and Balasubramanian Raman. "Privacy-Preserving Smart Surveillance Using Local Color Correction and Optimized ElGamal Cryptosystem over Cloud." 2019 IEEE 12th International Conference on Cloud Computing (CLOUD). IEEE, 2019.

[12] Sukmana, Muhammad IH, et al. "Unified Cloud Access Control Model for Cloud Storage Broker." 2019 International Conference on Information Networking (ICOIN). IEEE, 2019