International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

ROBUST AND AUDITABLE ACCESS CONTROL WITH MULTIPLE ATTRIBUTE AUTHORITIES FOR PUBLIC CLOUD STORAGE

Pavan Kumar CS
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
pavansharmxa@gmail.com

Ashok BP
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
ashokbpmca@gmail.com

ABSTRACT

Keeping our data safe on the cloud is key but hard, more so when we need to make sure it's easy and safe to get to In traditional systems where a single group has control over everything, what happens is that there are slow systems and one breakdown spoils the whole thing. This is not good when only a single group checks the Applicants and issues keys. These issues cause things to work Irregular and delay services, particularly when many individuals utilize the cloud. To address this our project has a new and improved way of managing who enters data using a blended group of bosses according to Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In this arrangement, multiple Attribute Authorities (AAs) verify who the users are and what they can do, whereas a Central Authority (CA) simply creates and distributes secret keys if users passes the inspection. Breaking these tasks into multiple AAs prevents the Obstacles we experienced earlier when all the bosses were doing everything.

Keywords: *CP-ABE(Ciphertext-Policy Attribute-Based Encryption), Access Control, Attribute Authority(AA), Auditing Mechanism, Cloud data Security, Key distribution*.

INTRODUCTION

Cloud computing has become central to the education and operations of the data storage and management, research, and instruction and that individuals and teams can access any time. It allows individuals to utilize such things as storage, linking points, and applications across the web reducing strain on local configurations and making things function more smoothly and accommodate things easily. But as increasing amounts of data personal information migrate these to cloud locations safeguarding this data and keeping it in line has become a significant challenge. to break down when dealing with the constantly changing the spread of the cloud, which creates concerns about unauthorized access, information leaks, and sluggish service. A top way to make cloud storage safer is with Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which tweaks access based on user traits. Though CP-ABE is bendy,

these systems often slow down because they count on just one spot for checking users and giving out keys. This not only makes things less smooth but increases the risk of system crashes and slowed-down service. To fix these problems, a strong and proven way to handle access is key The proposed system leverages a combined of many Attribute Authorities (AAs) and a Central Authority (CA) who all have responsibilities to verify and generate keys.

LITERATURE SURVEY

The rapid adoption of cloud technology has made analysts to come up with ways of securing data efficiently and securely. The major areas of focus include encryptions in data sets that are searched. The general word search techniques that normally are utilized can frequently be referred to as a same-to-all procedure that constrains the ability of how individualized they can be and the majority of the time is not what the user desires to identify. Studies like those by Fu and Ren show that while word search lets users look into encoded data, it usually misses the deeper meaning and link to the context, causing a bad user time. To fix this, search models that are more personal and ranked have been put out, using understanding frameworks and user past to give back better results.

At the same time, attribute-based encoding (ABE) has caught a lot of eyes for putting detailed access control in cloud stores. Ciphertext-Policy Attribute-Based Encoding (CP-ABE) lets data owners set access plans based on features not who they are, making it more flexible and safe. Yet, single-authority CP-ABE setups face issues like not being able to grow and one place for all checks, where one main hand makes and checks secret keys. It fails to work fruitfully and will be hazardous should that dominating hand happen to break or fall under the danger of being damaged. Recently, configurations with many main hands and large numbers of controling feature sets have been considered. It improves independence on a single unit but on the other hand it has issues of coordination and efficiency. Newer efforts, like Multi-message Cryptography Regulation Attribute-Based solutions attempt to add the benefits of great encoding to the desirable flexibility when meshing up with cell devices with limited assets.

Most texts have a growing need to employ different and authenticated access models, which balance speed, security, and user time in cloud public storage.

EXISTING WORK

In the next generation of cloud storage, it is not easy to regulate sharing of information between the recipients since one cannot be assured that the cloud handlers will take care of the information. A way of acquiring this kind of management is known as Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which provides the encryption to data owners to ensure they only give access to the potential recipients of their data. Only those persons with the proper attributes can observe information in CP-ABE since it is encrypted under attributes. This is a more

flexible and secure method than the legacy server-client access. However, these CP-ABE systems, despite their large advantages, have tremendous issues. Single authority systems have a single group checking the rights of users, and generating secret keys. It is a hazardous situation as in the event of anything going wrong with this group or people becoming online the entire system can collapse. It can as well get slow, when people sit back and wait on their keys. Attributes ended up being divided excessively between many-licensed authorities, and they made games to correct it. This slows things down and makes it difficult to grow and things doesn't work together which is not good for large, public clouds. These systems also fail to monitor bad actions by officials then the wrong individuals may enter the system. With more and more industries adopting the cloud these defects indicate we actually need a bigger, stronger, and clearer system to manage the access.

PROPOSE SYSTEM

The new scheme, Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage, is designed to address the insecure, and congested problems observed in typical Ciphertext-Policy Attribute-Based Encryption (CP-ABE) solutions. While CP-ABE offers detailed access rules and flexibility, it relies too much on just one authority or split multi-authority setups, which aren't good for big public cloud setupsTo address these problems, this system applies a blended design dividing the responsibilities of user check and key making.

Here, a lot of Attribute Authorities (AAs) are configured to verify if users exist. Attributes are inspected independently by each AA and a middle key is generated upon verification. The middle keys are then delivered securely to a Confidence Authority (CA) that only generates final keys. This division of labor keeps in good condition checks and key creation without overwhelming the single authority. By enabling numerous AAs to run in parallel, the system removes the single-point slow down and thus reaches more scale and faster responses.

A key new feature in this system is the provision of a check mechanism. The use of AA has been used in the past, and all middle keys can be traced to unique identifications that connect the check with the authority power. This enables the CA to identify misdeeds, carelessness, or collusion fraud between AAs, which makes them truly accountable and induces trust. This alternative offers transparent access control and it protects the system against evil insiders which in most cases traditional designs ignore. The RAAC scheme also preserves the fine-grained access rules of CP-ABE, allowing data owners to define attribute-based rules that dictate who may access locked files. Data owners lock files using simple keys before uploading, and the keys are concealed by attribute-based locking. The cloud server only stores the locked data, ensuring that even the server cannot access the data beneath it. Data users, in consequence, earn the right to open files only when their attributes conform

to the established rules, ensuring security and data privacy. In addition to improved speed and respondability, the system is designed to scale for production applications. As more users and requests increase, the shared work among numerous AAs keeps the system fast. Its check power also ensures its reliability, which is why it is a good option in groups that handle sensitive information within the public cloud. In general, the new system delivers a stable, verifiable, and positive access control structure.

METHODOLOGY

The plan of the RAAC system is established to ensure that it operates effectively, can scale, and manage access control to public cloud storage.

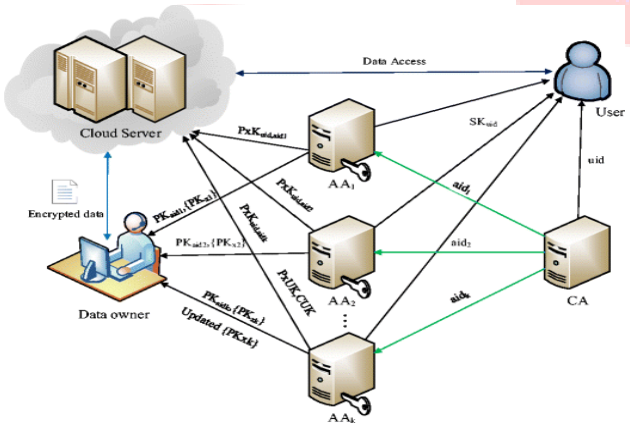

Fig 1. Block Diagram

It begins with the owner of the data, who encrypts files with a universal code mechanism. The key code is then stored securely by CP-ABE, defined by access policies based on attributes. The data is then uploaded to the cloud server, which has been encrypted. This makes it impossible for the cloud host to see the data contents and that only those users with the required attributes can use it.

To access a file a data user may require, an AA checks this. The AA tries whether the attributes of the user are accurate or not and it forms a middle-way key. This mechanism authenticates users in accordance with access rules. To build confidence and faith, there is also a check device in the plan. All mid way keys will have marks that can be used to reveal the AA who checked it. The wrong act by the AA can be recognized and recorded by the CA provided the AA misbehaves or checks users incorrectly.

Task	Task Name	Status
1	Requirement Analysis & Feasibility Study	Done
2	Design of System Architecture & UML Diagrams	Done
3	Development of Data Owner & Data User Modules	Done
4	Integration of File Encryption & Key Management using CP-ABE	Done
5	Cloud Server Setup & Secure File Storage	Done

EXPERIMENTAL RESULTS

The new system, built and checked for safe, big, and clear access control in cloud storage, underwent tests to see how well it worked. The tests that were carried out were meant to measure performance of various subsystems of the system in order to check whether they are effective and efficient. They also examined the reliability and trustworthiness of the encryption schemes, key administration and testing and confirmation and approval procedures. They used the system to test the log in and sign up components. There were designated areas of log in to separate people such as Data Owner, Data User, Attribute Authority (AA), Central Authority (CA), and the Cloud Server. This kept the functions different and prevented unidentified accessibility. Any sign-ups were entered into the database creating a method of access control down the line. The Data Owner component allowed users to send files locked through a one-key mechanism. Pictures revealed that once a file was uploaded, its name, the size and the date were stored on the cloud server. The files remained secured so that the cloud server could not view what was in them without permission. In the Data User section, users were requested to access locked files. The AAs received these asks and verified user information and generated start keys. The Central Authority converted start keys into final keys and allowed appropriately authorized users to open files. The improper users would not get access and this demonstrated that the system checked access properly.

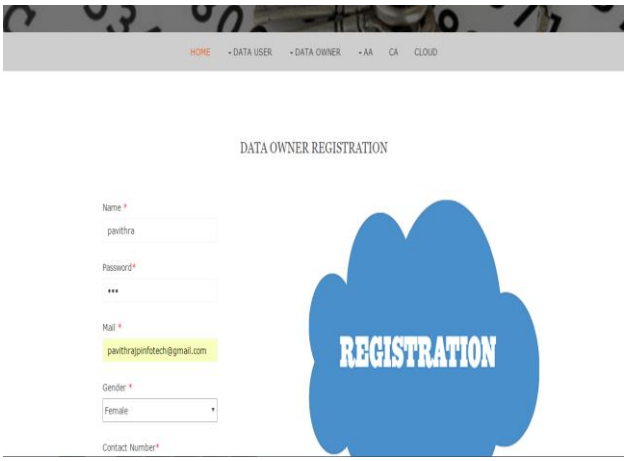

Fig 2. Data Owner Registration

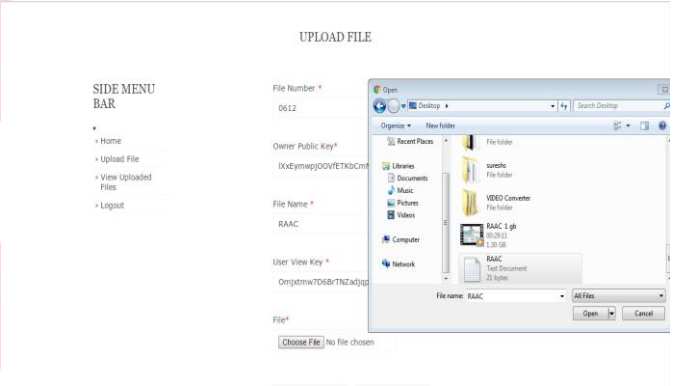

Fig 3. Uploading files to the Cloud

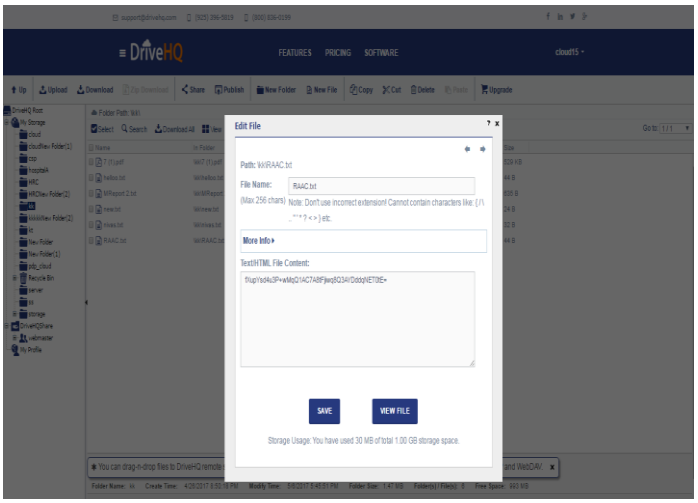

Fig 4. Decrypted file in the Cloud

CONCLUSION

The project called Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage has got past the big flaws in the normal Ciphertext-Policy Attribute-Based Encryption (CP-ABE) systems. The usual systems with one person in charge often run into issues like slowdowns and risiks of break down, while those with many people in charge and no tie between them are not smooth or well-coordinated By using a mixed setup that splits checking who gets in and making secret keys, this work shows a scalable and safe way to keep cloud data safe.

The system has a lot of Attribute Authorities (AAs) to verify tasks, distributing the load and making it quicker, which facilitates performance. As soon as the user traits are satisfactory, the Central Authority (CA) secretly generates the final secret keys thus eliminating the time consuming and smooth secret key issuance process. This type of job split prevents the problem at the point of identification and preserves CP-ABE fine-grained access control. Testing has proven that the new system is very useful in protecting the integrity of files, it effectively controls access, and it executes checks with sobriety, all this done in a user-friendliness to the advantage of users.

Encrypted files are going to be confidential even when they may be in servers that are not necessarily very safe and that safety is going to be available to the people who have been authorized depending on the rules which are going to be established.

REFERENCES

[1] Kaiping Xue, et al. "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage." IEEE Transactions on Information Forensics and Security 12.4 (2017): 953-967.

[2] Xue, K., Xue, Y., Hong, J., Li, W., Yue, H., Wei, D. S., & Hong, P. (2017). RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), 953-967.

[3] Xue, Kaiping, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, David SL Wei, and Peilin Hong. "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage." IEEE Transactions on Information Forensics and Security 12, no. 4 (2017): 953-967.

[4] Xue, K., Xue, Y., Hong, J., Li, W., Yue, H., Wei, D.S. and Hong, P., 2017. RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), pp.953-967.

[5] Xue K, Xue Y, Hong J, Li W, Yue H, Wei DS, Hong P. RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage. IEEE Transactions on Information Forensics and Security. 2017 Jan 2;12(4):953-67.