International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

A Novel Approach for User-Cloud Interaction using RAAC

Shwetha Balaji[1], Sriraksha[2], Vaishnavi M[3], Wasim Akram[4], Mrs. Geetha Rani[5]

Final year B.E Students (UG) ,Department of Information Science & Engineering, The Oxford College of Engineering, Bangalore,India[1,2,3,4]

Assistant Professor, Department of Information Science & Engineering, The Oxford College of Engineering, Bangalore, India[5]

ABSTRACT: Data access and security control is the challenging issue faced with regards to public cloud systems. Ciphertext-Policy Based Encryption (CP-ABE) has been adopted in order to provide flexibility, fine-grained and secure data access control with secure access to various cloud servers. In the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Although multiauthority access control schemes have been proposed, these schemes still cannot overcome the drawbacks of single-point bottleneck and low efficiency, due to the fact that each of the authorities still independently manages a disjoint attribute set. RAAC removes the problem of single-point performance bottleneck and provides a more efficient access control scheme with an auditing mechanism. It employs multiple attribute authorities to share the load of user legitimacy verification. Meanwhile, RAAC consists of a CA (Central Authority) to generate secret keys for legitimacy verified users. Unlike other multiauthority access control schemes, each of the authorities programmed in by RAAC manages one whole attribute set individually. RAAC enhanced security by including an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure. The goal of this project is to guarantee the security requirements needed for accessing data stored remotely as well as improving the user-system interaction performance by making use of key generation techniques.

KEYWORDS: Cloud storage, Access control, Auditing, CPABE

I. INTRODUCTION

To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labelled with his/her own attributes. Only if the attributes associated with the user's secret key satisfy the access structure, can the user decrypt the corresponding ciphertext to obtain the plaintext. RAAC not only employs a single CA but multiple RAs as well and thus proposes a robust and auditable access control scheme (named RAAC) for public cloud storage to promote the performance while keeping the flexibility and fine granularity features of the existing CP-ABE schemes. CA generates the secret key for the user on the basis of the received intermediate key, with no need of any more verification. In this way, multiple AAs can work in parallel to share the load of the time-consuming legitimacy verification and standby for each other so as to remove the single-point bottleneck on performance. With the help of intermediate keys, CA is able to not only generate secret keys for legitimacy verified users more efficiently but also trace an AA's mistake or malicious behaviour to enhance the security. The main contributions of this work can be summarized as follows:1) To address the single-point performance bottleneck of key distribution existed in the existing schemes, a robust and efficient heterogeneous framework with single CA (Central Authority) and multiple AAs (Attribute Authorities) for public cloud storage is implemented. 2) It includes an auditing mechanism that helps the system trace an AA's misbehaviour on user's legitimacy verification.

II. LITERATURE REVIEW

In cloud computing, searchable encryption scheme over outsourced data is a hot research field. However, most existing works on encrypted search over outsourced cloud data follow the model of "one size fits all" and ignore personalized search intention.[1]

With the increasing adoption of cloud computing, a growing number of users outsource their datasets into cloud. The datasets usually are encrypted before outsourcing to preserve the privacy.[2]

With the popularity of group data sharing in public cloud computing, the privacy andsecurity of group sharing data have become two major issues. The cloud provider cannot be treated as a trusted third party.[3]

A novel Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE) technique is presented, and employs the MCP-ABE. The scheme is efficient and flexible.[4]

The recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social networks or cloud computing, there have been increasing demands and concerns for distributed data security. Ciphertext policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue.[5]

III. PROBLEM STATEMENT

The main problem with the existing system is the presence of only one authority which is in charge of all the attributes in single authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set. The inefficiency of the authority's service results in single-point performance bottleneck, which will cause system congestion such that users often cannot obtain their secret keys quickly, and have to wait in the system queue. On the other hand, if there is only one authority that issues secret keys for some particular attributes, single-point performance bottleneck problem arises affecting the efficiency of secret key generation service and immensely degrades the utility of the existing schemes to conduct access control in large cloud storage systems.

IV. EXISTING SYSTEM

To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labelled with his/her own attributes.

V. PROPOSED SYSTEM

Inspired by the heterogeneous architecture with single CA and multiple RAs, we propose a robust and auditable access control scheme (named RAAC) for public cloud storage to promote the performance while keeping the flexibility and fine granularity features of the existing CP-ABE schemes.In this scheme, the procedure of user legitimacy verification from the secret key generation, and assign these two sub-procedures to two different kinds of authorities was separated. There are multiple authorities (named attribute authorities, AAs), each of which is in charge of the whole attribute set and can conduct user legitimacy verification independently. Meanwhile, there is only one global trusted authority (referred as Central Authority, CA) in charge of secret key generation and distribution. Before performing a secret key generation and distribution process, one of the AAs is selected to verify the legitimacy of the user's attributes and then it generates an intermediate key to send to CA. CA generates the secret key for the user on the basis of the received intermediate key, with no need of any more verification. In this way, multiple AAs can work in parallel to share the load of the time-consuming legitimacy verification and standby for each other so as to remove the single-point bottleneck on performance.Meanwhile, the selected AA doesn't take the responsibility of generating final secret keys to users. Instead, it generates intermediate keys that associate with users' attributes and implicitly associate with itsown identity, and sends them to CA. With the help of intermediate keys, CA is able to not only generate secret keys for

legitimacy verified users more efficiently but also trace an AA's mistake or malicious behaviour to enhance the security.

A.SYSTEM ARCHITECTURE

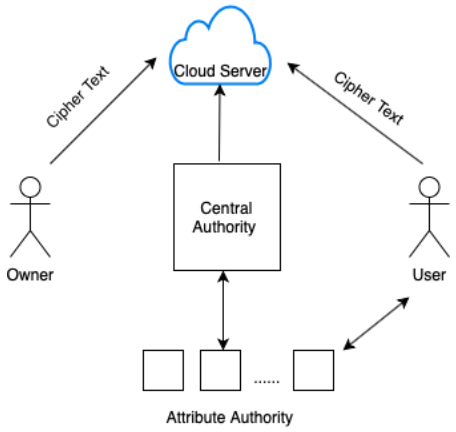

Fig 1: System Architecture

1. **Data Owner/User**: Data owner can upload files to the cloud and possesses the authority to decide who can access the files uploaded by him. Whereas the user can only view/download the files.
2. **Attribute Authorities**:Does all the user legitimacy verification and generates the intermediate key for the user.
3.**Central Authority**: Central Authority is the administrator of the entire system.For a key request from a user, *CA* is responsible for generating secret keys for the user on the basis of the received intermediate key associated with the user's legitimate attributes verified by an *AA*. Once the user is authenticated, he shall be given access to the files.
4.**Cloud Server**: Cloud Server provides a public platform for owners to store and share their encrypted data. The cloud server doesn't conduct data access control for owners. The encrypted data stored in the cloud server can be downloaded freely by any user.

B.WORKING

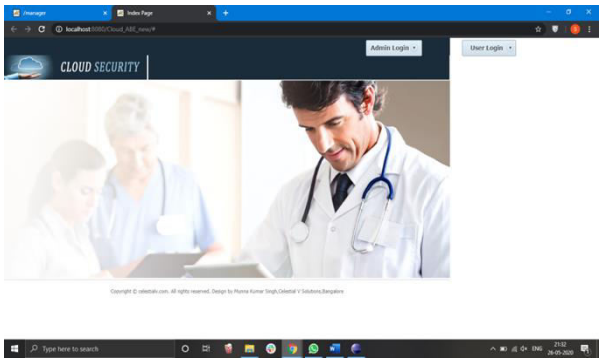

Figure 2:Home page

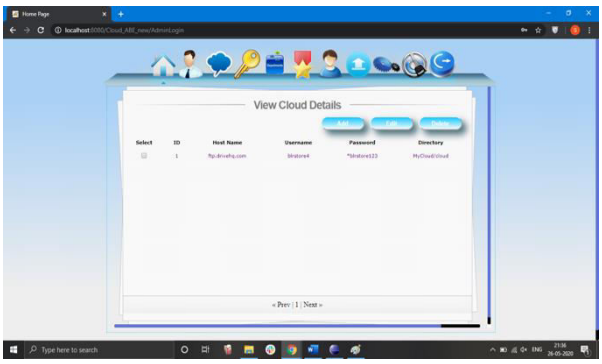

Figure 3: Cloud Details

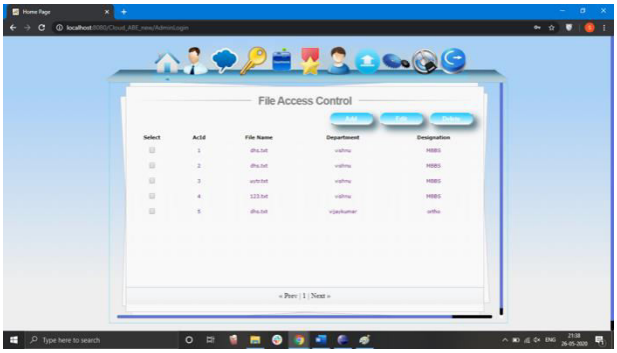

Figure 4: File access control

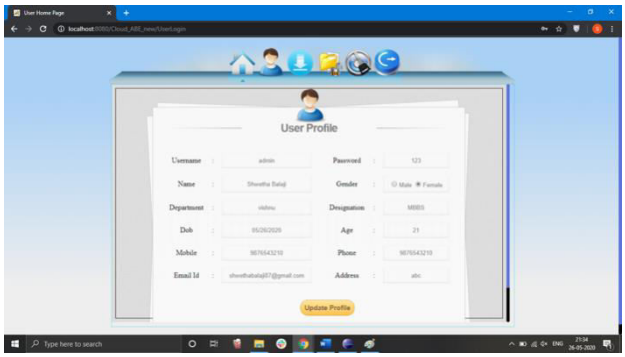

Figure 5: User Profile

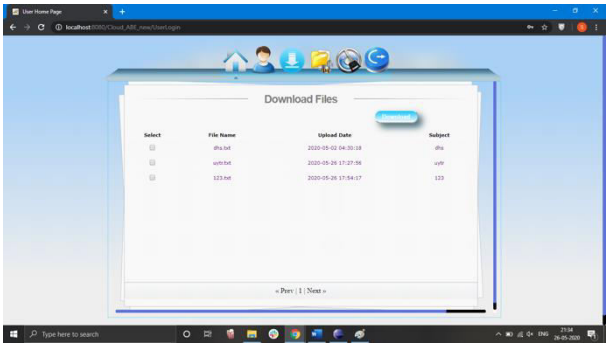

Figure 6: Files in cloud

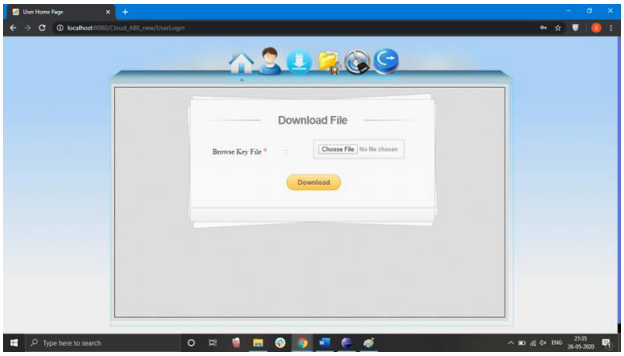

Figure 7: Downloading Files

The following is the implementation of the system based on the images shown in the above figure.The figures above shows the working of the project. The Home page contains the link to both Admin and user panel where they can log in to their respective accounts.The admin, after logging into his account, can upload new files to the cloud. The admin can also view the list of users requesting access to his files. He can grant access permissions to any of the new users. The Admin also has the power to modify the access given to any existing user for any of his files in the cloud. The user after being authenticated should upload the private key he possesses in order to view or download the file.

VI. RESULTS

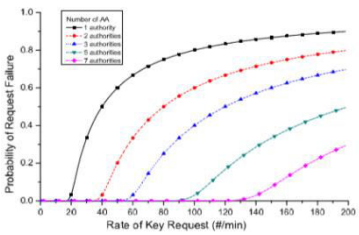

Figure 8

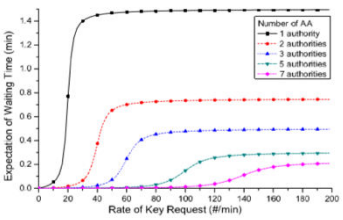

Figure 9

When multi AAs is filled with N users, it means that K users are waiting in the queue and all AAs are occupied, the newly arriving users are rejected.We analyse the probability of failure to show how to lower this failure rate with more AAs. Based on the emulation of the scheme, the average time of generating a secret key for an attribute is about 35ms. Furthermore, we assume that users possess 10 attributes on average and the verification takes tenfold amount of time of that of the key generation. The performance analysis in terms of the average failure rate and the average waiting time is

shown in below graphs.The first graph shows the failure rate versus the arrival rate and the number of AAs.The second graph shows that the average waiting time increases rapidly with the increase of arrival rate when the arrival rates are low.

VII. CONCLUSION AND FUTURE WORK

The goal of this research is to eliminate the single-point performance bottleneck of the existing CP-ABE schemes proposed. By effectively reformulating CP-ABE cryptographic technique along with RAAC to provide a fine-grained, robust and efficient access control with one CA/multi-AAs for public cloud storage. RAAC employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of user's requests. It was also confirmed that the auditing method to trace an attribute authority's potential misbehaviour would be included, along with a detailed security and performance analysis to verify that RAAC is secure and efficiency is confirmed. The security analysis shows that RAAC could effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers.The security analysis shows that RAACcould effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers. Besides, with the proposed auditing & tracing scheme, no *AA* could deny its misbehaved key distribution. Further performance analysis based on queuing theory showed the superiority of RAACover the traditional CP-ABE based access control schemes for public cloud storage.

REFERENCES

[1]Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel & Distributed Systems*, vol. 27, no. 9, pp. 2546–2559, 2016.
[2]Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in *in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016)*. IEEE, 2016, pp. 1–9.
[3]K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 459–470, 2014.
[4]Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," *IEEE Transactions on Multimedia*, vol. 15, no. 4, pp. 778–788, 2013.
[5]J. Hur, "Improving security and efficiency in attribute- based data sharing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271–2282, 2013.