International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 11 • Issue 1 pp. 1-6 Sept 2019 - March 2020 www.csjournals.com

Multiple Attribute Authorities in Data Access

Prof. Rakesh Shirsath[1], Mrs. Rohini Tambe[2]
Assistant Professor[1], PG Student[2], Sandip Foundation, Nasik, India

Abstract: Cloud computing is an popular technology that provides different utility to the users where data is stored on the cloud. In open cloud storage system data access limitation is a difficult task's-ABE has been accept as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with truly interested cloud servers. A novel framework is for to avoid the problem of single-point achievement barrier and provide more adequate access control method with an auditing structure. Our framework applies multiple attribute authorities to contribute the load of user authority verification. A CA(Central Authority) is introduced to create secret keys for authenticated users. Each of the authorities in our method guide the whole aspect set personally. We will also offer an auditing system to identify which AA (Attribute Authority) has unauthorized conduct the authentication verification procedure. We propose load balancing and memory management in cloud server.
Keywords: Public Cloud ,CP-ABE Algorithm Central Authority.

Introduction

Cloud storage is really a promising and important service paradigm in cloud computing. Benefits of using cloud repository include greater accessibility, higher reliability, fast delivery and stronger protection, to mention only a few. In contravention of the mentioned benefits, this technique also brings forth new challenges on data access control, which is really a critical issue to make clear data security. Since cloud repository is operated by cloud service providers, that are usually beyond your trusted domain of data owners, the standard access control methods in the Client/Server model aren't suitable in cloud storage environment[1].Cloud Security describes a broad group of guideline, methods, and controls delivered to guard data, applications, and the associated infrastructure of cloud compting. There are Some advanced encryption algorithms that have been applied in to the cloud computing in raise the protection of privacy are CP-ABE,KP-ABE would be the attribute based encryption algorithms [1].In cloud computing, exploring encryption method over outsourced data is a hot research field. Most previous work on encrypted search over outsourced cloud data pursue the design of one size fits all and avoid personal search intention. Moreover, most of them support only particular keyword search, which affects data usability and user experience [2].

Data access limitation is a successful plan to guarantee the data security in the cloud. However, because of data outsourcing and unauthorized cloud servers, the data access limitation becomes a complicated issue in cloud repository systems. previous access control mechanism are not relevant to cloud storage systems ,simply because they either produce multiple encrypted copies of the exact same data or require a completely trusted cloud server. To control the data access of encrypted data cipher text-policy attribute-based encryption (CP-ABE) is used. It needs a reliable authority manages most of the attributes and distributes keys in the system. In cloud storage systems, you can find one or more authorities coexisting and each authority has the capacity to argue attributes individually. For multi-authority cloud storage system existing CP-ABE schemes can't be directly placed on data access due to the inefficiency of decryption and revocation [3].The demand of outsourcing data has increased To satisfy the necessity for data storage and good performance computation, most of cloud computing service providers have visible, such as for example Amazon Simple Storage Service (Amazon S3),Google App Engine, Microsoft Azure, Drop box and so on. You will find two major issues privacy and security of group data sharing in public cloud computing. The cloud provider cant be treated as a reliable alternative party due to its semi trust nature, and thus the standard security models cant be straightforwardly generalized into cloud based group sharing frameworks. So that they propose group sharing framework [4].

Content allocation environments such as for instance social networking are extremely changing when it comes to the amount of on-line users, storage demand, network bandwidth computational capability, applications and platforms; its challenging for service supplier to allocate resources. As cloud computing gives application developers and users an hypothetical view of services that bury a lot of the system functions and internal process, its more and much very famous in Content allocation environments. Access control may be the vital security system to provide information sharing in a limited situation [5].various works and analysis are concentrating on finding methods to the data access limitation in cloud storage model with respective types of works, schemes predicted on Cipher text-Policy Attribute-Based Encryption (CP-ABE) primitive have focus broad consideration because of its capacity to permit data owners fine-grained hold on these data. Intuitively, CP-ABE is usually recommend as a realization to implement role-based access control, where in the actuality the users attributes match to the long-term roles. In certain, a users access authority is not just defined by his/her inherent roles but also depends on his/her environmental situations such as location [6].cloud computing has move attentions from both academia and industry, because it is really a assuring computing paradigm where

computing resources are supplied as services via the Internet. the data sharing in cloud computing via cellular devices has be much more popular. However, data confidence and online computational cost still avail practical thing to the delivery of data sharing in cloud computing for mobile devices. previous data sharing rules in cloud computing either cannot support the flexible sharing style for the encrypted data, or have a problems with big online computational cost that scales with the complexity of the access policy [7].

At a specialized stage, the key aim that people must gain is collusion-resistance: If one or more users collude, they need to have the ability to decrypt a cipher text if a minimum of one of users could decrypt it on self. Specifically, acknowledge back once again to the example right from the start with this formal description, suppose that an FBI dept that works in the terrorism once in San Francisco colludes with a buddy who works in the general public corruption once in New York. We do not require these colluders have the capacity to decrypt the trick memo by collect their attributes. This kind of security could be the sine qua non of access control within our setting[8].A key-policy attribute-based encryption (ABE) system for threshold policies by which a sender can encrypt a message indicating an attribute set and a number, just a recipient with at the very least of the given at attributes can decrypt the message. However, the delivery conclusion of these methods may possibly not be real, in so it consider the presence of just one authorized party who audits all attributes and matters all decryption keys. we usually have various things in chard of monitoring different attributes of an individual[9].some researchers have suggest a some of effective search method over encrypted cloud data. The overall procedure for search design is divide into five stages: obtaining document features, build a searchable index, create search trapdoor, finding the index depends on the trapdoor and retrieving the search results [10].

The Principle goal of the system is to offer security to the data stored on cloud and to keep up the storage capacity of the cloud server. The data on the cloud is confidential and should be protected against unauthorized access and traitors/abnormal players. The core task is always to generate secret keys for legitimacy verified users and makes great performance improvement on key generation and reduce the strain on server and manage time.

Literature Survey

Kaiping Xue, Yingjie Xue [1] introduced a scheme they remove the issue of single point performance bottleneck by utilizing multiple attribute authority to generally share the strain of user legitimacy verification. it Provide more effective access control scheme by having an auditing mechanism and Used CP-ABE scheme in large scale for cloud storage but users might be stuck in the waiting queue for an extended period to acquire their secrete keys, thereby causing in low efficiency of the system [1].Zhangjie Fu, Kui Ren, Jiangang Shu[2] introduced a scheme by which they study and resolve the issue of personalized multi-keyword ranked searched over encrypted data while(PRSE) keep personalize in cloud computing With the aid of semantic ontology Word Net. They form a person interest model for particular user. Examine users search history. accept a rating system to state user interest smartly. Thorough privacy analysis and performance analysis demonstrates that scheme is practicable [2].Author[3] introduced a brand new various authority CPABE scheme with active decryption and also develop an effective attribute abort method that may gain both forward and backward security. The study and the simulation outcomes reveal that DAC-MACS are highly efficient and secure beneath the security model.

The security Weakness of revoked user damage any AA and some invert users and get key easily and also update key. Kaiping Xue and Peilin Hong [4] introduced a novel secure group sharing framework for public cloud storage. Framework joins proxy signature, enhance TGDH and proxy re-encryption together. It still requires the group members to participate along the way of implementation and receive some others sent messages. Most of the sharing files are secured stored in Cloud Servers and most of the session key is protected in the digital envelopes.

Digital envelopes must be simulated on proxy repeat encryption, which could envoy closely all of computing high load to Cloud Servers without hide out any security measures.Yongdong Wu, Zhuo Wei, and Robert H. Deng [5] introduced CP-ABE and proposed a scheme to guide various authority access limitation to scalable media. Slow decryption, modular exponentiation operation is required. Also how exactly to increase the decryption process at low end devices. Features of MCP ABE permit a data owner to accomplish access control predicted on attributes of data user without externally naming the individual data user.it Support multiprivilege access control to scalable media. Access control method is effective for securely and flexibly arrange media content in large distributed systems. Yingjie Xue, Jianan Hong, Wei Li, Kaiping Xue, Peilin Hong [6] introduced in which they separately incorporate CPABE with location backdoors to make up access rules. no need to any additional revocation scheme to revoke location aware access authority when dynamic user location .LABAC takes little over head to data owner.

One location server will only affect the data along with this location, while other data still private. When a consumer encrypts sensitive data, its imperative that she set up a specific access control policy on who is able to decrypt this data [7]. As an example, guess that the FBI public corruption offices in Knoxville and San

Francisco are investigating an allegation of bribery involving a San Francisco lobbyist and a Tennessee congressman. The top FBI agent might want to encrypt a delicate memo to ensure that only personnel which have certain credentials or attributes can access it. It could be preferable to truly have a evidence of security that reduces the issue of breaking our scheme to a well-studied complexity-theoretic problem. Such reductions will only going to exist for more complicated schemes compared to the one we give here.
Each authority is in charge of different attributes, we should allow them to issue decryption keys independently [8], and never having to keep in touch with one another. in order to avoid collusion in this setting, we want some consistent notion of identity. We review the motivation behind the utilization of the CA, and show how to prevent it. Enables an even more realistic deployment of attribute-based access control, in a way that different authorities are accountable for issuing different sets of attributes. Our work provides a more practice-oriented attribute based encryption system. A concept ranking is build on the basis of the approach relate to familiarity with the dataset. Secondly, two index vectors for every single document of the dataset are create on the basis of the key concepts of the document and the idea hierarchy [9],[10]. Finally, the searchable index is constructed with all the current index vectors.

System Architecture

Cloud computing is an popular technology that provides different utility to the users where data is stored on the cloud. CP-ABE has been accept as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with truly interested cloud servers. a novel framework is for to avoid the problem of single-point achievement barrier and provide more adequate access control method with an auditing structure.In our proposed system we use CP-ABE scheme multiple attribute authority for security in data access. We will also propose an auditing mechanism to detect which attribute authority has incorrectly or maliciously performed the legitimacy verification procedure.

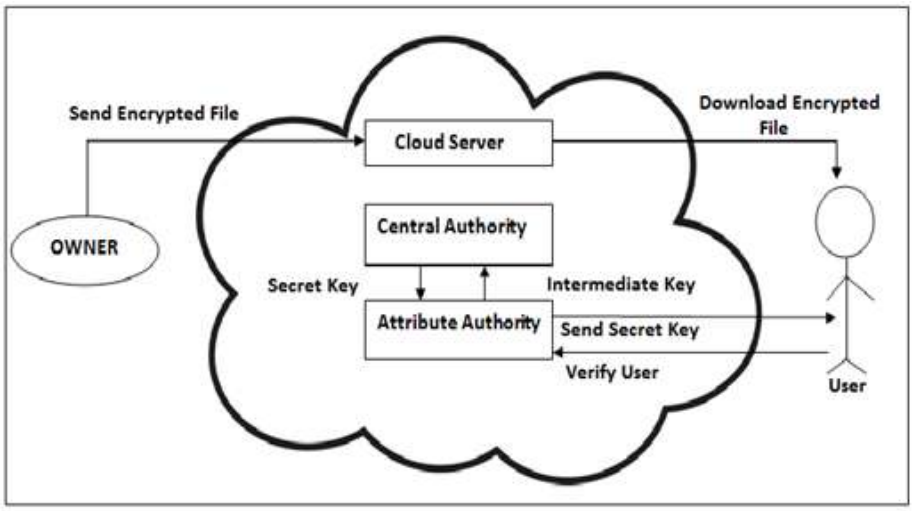

Figure 1: System Architecture

The system can be utilized to security purpose. It'll support both stand alone and also networking environment. In this technique we could share data from sender to receiver in light weighted format. We could send link from PC to mobile, mobile to mobile and other devices. All the data will soon be within an optimized database on then central server. These details could be accessed by the users. The next steps show the flow of system:-

1) Admin have access of upload document in encrypted Format.
2) Uploaded document will soon be stored that link to database.
3) Link is likely to be sending to server.
4) User log in to system.
5) User can select that link then OTP Is generated on user registered mobile.
6) Verification of OTP.
7) Then user can download this document in decrypt format.

The central authority (CA)

CA could be the administrator of the whole system. It generates the general public key for every single attributes, it assigns each user a distinctive Uid and each attribute authority a distinctive Aid. It generates secrete keys for users.CA trace AA incorrectly or maliciously verified a user.

The attribute authorities (AAs)

AA performs user legitimacy verification and generating intermediate keys for legitimacy verified users.

The data owner (Owner)

Owner can obtain access to each file and encrypts the file under defined policy. Data Owner assigns the unreadable data and encrypted symmetric key to the cloud server to be stored in the cloud.

The data consumer (User)

Global Uid assigned by CA.The user possesses group of attributes with it could possibly get any favor encrypted data from the cloud server but user can decode that file only if when attribute set amuse the access policy of encrypted data.

The cloud server

Provides the general public platform for owners to store and share encoded data. Cloud server doesn't handling data access control for owners. Encrypted data may be downloaded by any user freely. You can find two operations in access control that need effective processing, namely decode and revocation. We propose a hierarchical framework with single CA and multiple AAs to eliminate the issue of single-point Performance bottleneck and enhance the system efficiency to attain an active and adequate access control for public cloud storage.

Mathematical Model

The System can be mathematically defined as a collection of three tuples.
S can be written as :

1. I= Input (set of users).
2. O= Output (set of efficient access control with an auditing mechanism).
3. A= set of Procedures.

Input:

X= users{x1, x2, x3, …, x_n}

Output:

Y= efficient access control with auditing {y1, y2, y3,…, y_n}

System Initialization

1. i = set of user.
2. Sk = CA also randomly generates public keys.
3. Dr = handling AAs and users registration.
4. r1 = generates a pair of keys to sign and verify

Encryption

1. Input Si = performed by the data owner and chooses a random number.
2. Output = encrypts the plaintext message.
3. k є GT
4. The encrypted data can be denoted as Ek(M)

Key Generate

1. Input Si = the given user, a selected AA and CA.
2. Output = user legitimacy verification.
3. UJ = AAi
4. AAi = CA

Decryption

1. Input = the given user.
2. Output = download any interested encrypted data from the public cloud storage.
3. let MU be a sub-matrix of M,
4. AAi = CA

Auditing

1. Input Si = the given user.
2. Output = download any interested encrypted data from the public cloud storage.

Performance Analysis

The size and capacity requirements are also important. Our system can be efficiently run on Intel core i3 system with minimum 4 GB RAM.

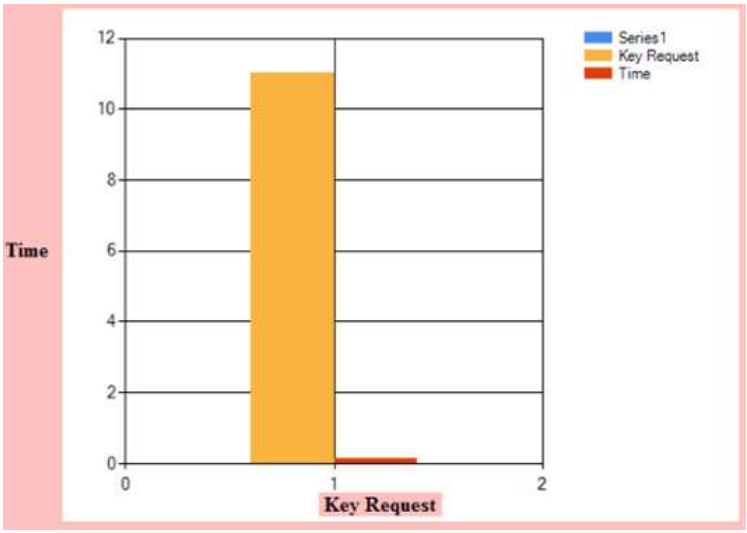

Figure 2: The time for key request in RAAC

Fig.2 shows the average waiting time versus the arrival rate and the number of AAs. We can see that the average waiting time increases rapidly with the increase of arrival rate when the arrival rates are low.

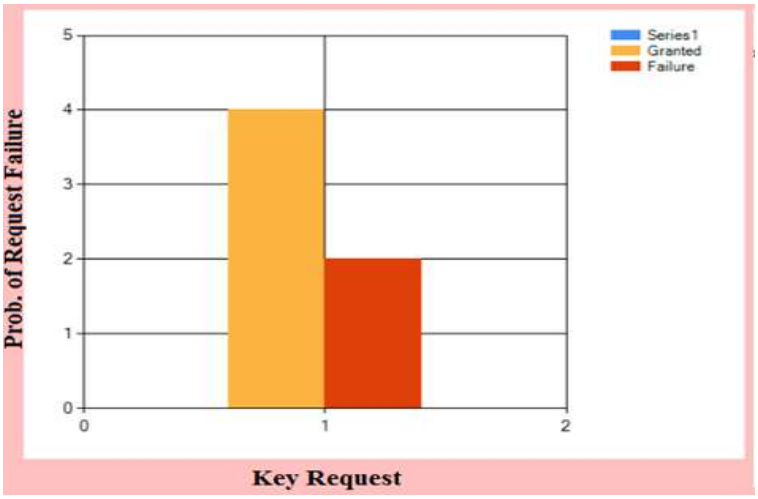

Figure 3: Number of key request /failure time in RAAC

The performance analysis in terms of the common failure rate and also the average granted time is shown in Fig.3 shows the failure rate versus the arrival rate and also the variety of AAs. The system will greatly increase its service capability with the support of a larger arrival rate at the lowest failure rate.

Conclusion

A new framework named RAAC that's used to remove the single-point performance bottleneck of the present CP-ABE schemes. By effectively reformulating CPABE cryptographic technique. Provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. We also proposed an auditing method to trace an attribute authority's potential misbehavior. For public cloud storage reveal security and performance analysis is going to be evaluate to verify that our scheme is secure and efficient and also performance analysis of our scheme will check over the traditional CP-ABE based access control schemes.

References

[1]. Kaiping Xue, Senior Member, IEEE, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, 'RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage.", , IEEE,2016,PP.15.2016.

[2]. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement",vol. 27, no. 9, pp. 25462559, 2016..

[3]. K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing,"IEEE Transactions Cloud Computing, vol. 2, no. 4, pp. 459470, 2014.

[4]. Y. Wu, Z. Wei, and H. Deng, K. Li, Z. Li, and W. Qu, "Attributebased access to scalable media in cloud-assisted content sharing,",IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778788, 2013.

[5]. LNCS Homepage, \url{http://www.springer.com/lncs}. Last accessed 4 Oct 2017.

[6]. J. Hur, "Improving security and efficiency in attributebased data sharing,",IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 22712282, 2013.

[7]. J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems,",IEEE Transactions on Parallel and Distributed Systems,vol. 22, no. 7, pp. 12141221, 2011.

[8]. J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on timesensitive data in public cloud,",in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, pp. 16 , 2015.

[9]. Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attribute-based access control scheme for cloud storage,",in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016).IEEE, pp. 16, 2016.

[10]. A. Lewko and B. Waters, "Decentralizing attribute-based encryption,",in Advances in CryptologyEUROCRYPT 2011. Springer, pp. 568588 , 2011.

[11]. K. Yang, X. Jia, K. Ren, and B. Zhang, "DMACS:Effective data access control for multi-authority cloud,",in Proceedings of 2013 IEEE Conference on Computer Communications (INFOCOM 2013).IEEE, pp. 28952903, 2013.

[12]. J. Chen and H. Ma, "Efficient decentralized attributebased access control for cloud storage with user revocation,",in Proceedings of 2014 IEEE International Conference on Communications (ICC 2014). IEEE, pp. 37823787 ,2014.