International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 6, June-2018

Improving Key Generation Performance on Public Cloud Storage Along with User Legitimacy Verification

[1]POOJA WILSON, [2]CH.RAMESH

[1]M. Tech Student, Department of Computer Networks And Information Security,
G. Narayanamma Institute of Technology and Science (GNITS), Shaikpet, Hyderabad,
[2]Assistant Professor, Department Of Information Technology,
G. Narayanamma Institute of Technology and Science (GNITS), Shaikpet, Hyderabad, India

ABSTRACT— ***in the cloud storage systems, data management is very difficult to the service providers as well as data owners. To manage the stored data, we used Ciphertext-Policy Attribute-Based Encryption (CP-ABE) & it has been followed as a promising method to offer flexible, fine-grained & secure records get entry to manipulate for cloud storage with honest-but-curious cloud servers. However, inside the present CP-ABE schemes, the single attribute authority ought to execute the time-consuming consumer legitimacy verification and secret key distribution, and therefore it outcomes in a single-factor overall performance bottleneck when a CP-ABE scheme is adopted in a big-scale cloud storage device. In this paper, we recommend a novel heterogeneous framework to do away with the problem of single-factor performance bottleneck and offer an extra efficient get entry to manipulate scheme with an auditing mechanism. The proposed scheme can not only eliminate the single-point performance bottleneck but also be able to present a robust, high-efficient, & secure access control for public cloud storage.***

Keywords: Cloud Computing, Cloud Storage, CP-ABE, Auditing

1. INTRODUCTION

As Cloud Computing turns into usual, increasingly touchy records are being centralized into the cloud, together with emails, personal health statistics, business enterprise finance data, and authorities files, and so on. The fact that information owners and cloud server are not in the identical trusted domain may additionally put the outsourced unencrypted statistics at chance: the cloud server may also leak statistics information to unauthorized entities or maybe be hacked. It follows that sensitive data needs to be encrypted previous to outsourcing for statistics privateness and fighting unsolicited accesses. However, data encryption makes effective statistics usage a completely hard project given that there can be a big quantity of outsourced data documents. Besides, in Cloud Computing, statistics owners may share their outsourced data with a large quantity of customers, who would possibly need to simplest retrieve sure particular statistics files they are interested in for the duration of a given consultation. One of the most popular methods to do so is thru key-word-based totally seek. Such key-word search technique lets in users to selectively retrieve documents of hobby and has been widely applied in plaintext seek situations. Unfortunately, data encryption, which restricts consumer's ability to perform key-word search and in addition demands the safety of keyword privacy, makes the conventional plaintext seek techniques fail for encrypted cloud statistics.

Attribute-based encryption (ABE) is a promising cryptographic method that achieves an exceptional-grained statistics get admission to control. It provides a manner of defining access guidelines primarily based on distinct attributes of the requester, environment, or the information item. Especially, CP-ABE allows to encrypt or to describe the function set over a universe of attributes that a decrypt or desires to possess that lets in you to decrypt the cipher text, and put in force it at the contents. Thus, each user with a distinctive set of attributes is allowed to decrypt one of kind portions of data in keeping with the security policy. This efficiently gets rid of the want to depend upon the data garage server for stopping unauthorized data get entry to, which is the traditional get right of entry to control approach of including the reference monitor Nevertheless, making use of CP-ABE in the records sharing system has several challenges.

In CP-ABE, the important Key Generation Center (KGC) generates private keys of users by means of applying the KGC's master secret keys to customers' associated set of attributes. Thus, the fundamental advantage of this method is to largely reduce the need for processing and storing public key certificate under conventional Public Key Infrastructure (PKI). However, the gain of the CP-ABE comes with a main drawback which is called a key escrow trouble. The KGC can decrypt cipher textual content addressed to particular customers by way of producing their attribute keys. This might be a potential danger to the data confidentiality or privacy in the information sharing systems. Another undertaking is the important thing revocation. Since some users may additionally trade their companion attributes at some time, or some personal keys might be compromised, key revocation or replace for every attribute is necessary with the intention to make structures at ease.

In single-authority schemes, the handiest authority should verify the legitimacy of customers' attributes earlier than producing secret keys for them. As the get admission to manipulate device is associated with data protection, and the simplest credential a person possess is his/her secret key associated with his/her attributes, the procedure of key issuing need to be cautious. However, in the actual world, the attributes are various. For example, to verify whether a person is capable of pressure can also need an authority to give him/her a take a look at to show that he/she will be able to power. Thus he/she will get an attribute key related to driving capacity. To address the verification of numerous attributes, the person may be required to be present to affirm them. Furthermore, the system to verify/assign attributes to users is generally tough so that it normally employs administrators to manually manage the verification.

2. RELATED WORK

It is unrealistic to expect there is a single authority that could display each single attribute of all users. Multi-authority attribute-based totally encryption enables a more practical deployment of attribute-based get entry to manage, such that exclusive government are liable for issuing one of a kind sets of attributes. The authentic answer by way of Chase employs a trusted imperative authority and the usage of a international identifier for every person, because of this the confidentiality, depends critically on the safety of the vital authority and the user-privacy depends on the honest conduct of the attribute-government. M. Chase and S. S. Chow proposed an attribute-based encryption scheme without the depended on authority, and an anonymous key issuing protocol which fits for both present schemes and for our new construction. Their paintings accomplished a more exercise-oriented attribute primarily based encryption gadget.

J. Hur and D. K. Noh made a survey on the effective records get entry to control scheme built for multi-authority cloud garage systems. Nowadays, there may be an emerging fashion that increasingly customers are beginning to apply the public cloud garage for online records storing and sharing; the safety in cloud is fundamental issue. The multi-authority CP-ABE reduces Decryption overhead for customers in step with attributes. This cozy attribute based cryptographic method for strong information safety that's being shared within the cloud .This multi-authority CP-ABE scheme proved that it's far comfortable and verifiable. The revocable multi-authority CPABE is an effective technique, which can be appropriate in any remote garage structures and on line social networks etc.

Building at the notion for multi-authority primarily based attribute based totally encryption, H. Lin, Z. Cao, X. Liang, and J. Shao constructed a scheme wherein the valuable authority is now not able to decrypting arbitrary cipher texts created in the device. In addition to supplying protection within the selective ID model, the proposed gadget can tolerate a honest-but-curious principal authority. Since both Chase's scheme and the proposed scheme depend on the identical hardness assumption, and have a comparable complexity, the new scheme appears a feasible opportunity to Chase's production. However, for the reason that handiest the proposed method is capable of coping with a curious yet honest important authority, the proposed scheme is recommended in programs where protection against this kind of central authority is required.

3. FRAMEWORK

A. Overview of the Proposed System

We suggest a sturdy and auditable get right of entry to manipulate scheme (named RAAC) for public cloud storage to sell the overall performance at the same time as maintaining the power and excellent granularity capabilities of the prevailing CP-ABE schemes. In our scheme, we separate the method of user legitimacy verification from the secret key era, and assign these two sub-methods to 2 one-of-a-kind varieties of authorities. There are a couple of government (named attribute government, AAs), each of which is in charge of the entire attribute set and may behavior user legitimacy verification independently. Meanwhile, there is handiest one international trusted authority (referred as Central Authority, CA) in charge of mystery key generation and distribution. Before appearing a secret key generation and distribution method, one of the AAs is selected to confirm the legitimacy of the consumer's attributes and then it generates an intermediate key to ship to CA. CA generates the secret key for the user on the premise of the acquired intermediate key, and not using a need of any extra verification. In this manner, more than one AAs can paintings in parallel to proportion the load of the time-consuming legitimacy verification and standby for each different so that you can get rid of the single-point bottleneck on overall performance. Meanwhile, the selected AA doesn't take the obligation of generating final secret keys to users. Instead, it generates intermediate keys that accomplice with customers' attributes and implicitly accomplice with its own identification, and sends them to CA. With the assist of intermediate keys, CA is capable of not most effective generate secret keys for legitimacy demonstrated customers more correctly but additionally hint an AA's mistake or malicious behavior to decorate the safety.

In our one-CA/more than one-AAs production, CA participates inside the key era and distribution for safety motives: To expand auditability of corrupted AAs, one AA can't attain the gadget's grasp secret key in case it could optionally generate secret keys with none supervision. Meanwhile, the advent of CA for key generation and distribution is suitable, on account that for a big-scale device, the maximum time-ingesting workload of legitimacy verification is offloaded and shared a few of the more than one AAs, and the computation workload for key technology may be very light. The manner of key technology and distribution could be more efficient than other present schemes. To trace an AA's misbehavior in the process of user legitimacy verification, we first locate the suspected data patron based on bizarre behavior detection, that's much like the mechanisms used present. For a suspected person, our scheme can trace the authorized AA who has falsely validated this user's attributes and illegitimately assigned secret keys to him/her.

B. Proposed System Working

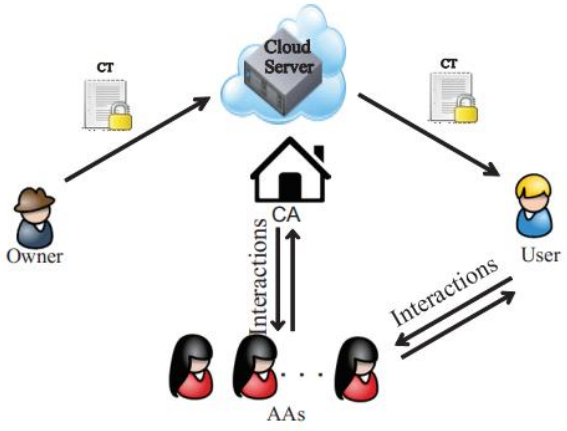

Fig1. Proposed System workflow

From the Fig1 the proposed model contains 6 entities, the Central Authority (CA) is the administrator of the entire device. It is liable for the system production by way of setting up the system parameters and producing public key for each attribute of the prevalent attribute set. In the device initialization segment, it assigns each person a completely unique U_{id} and each attribute authority a unique A_{id}. For a key request from a user, CA is responsible for producing secret keys for the user on the premise of the received intermediate key associated with the user's valid attributes tested via an AA. As an administrator of the complete machine, CA has the capability to trace which AA has incorrectly or maliciously confirmed a person and has granted illegitimate attribute units.

The Attribute Authority (AA) is answerable for acting patron legitimacy verification and producing intermediate keys for legitimacy tested clients. Unlike maximum of the triumphing multi-authority schemes in which each AA manages a disjoint characteristic set respectively, our proposed scheme involves a couple of authorities to percentage the obligation of person legitimacy verification and each AA can carry out this system for any user independently. When an AA is selected, it will confirm the customers' valid attributes by using guide hard work or authentication protocols, and generate an intermediate key related to the attributes that it has legitimacy-proven. Intermediate secret's a state-of-the-art idea to help CA to generate keys.

The Data Owner (Owner) defines the get entry to coverage approximately who can get admission to every document, and encrypts the document below the defined coverage. First of all, each owner encrypts his/her records with a symmetric encryption algorithm. Then, the owner formulates get right of entry to policy over a attribute set and encrypts the symmetric key under the policy in step with public keys obtained from CA. After that, the proprietor sends the entire encrypted statistics and the encrypted symmetric key (denoted as cipher textual content CT) to the cloud server to be saved within the cloud.

The Data User (User) is assigned a worldwide consumer identity U_{id} by CA. The consumer possesses a fixed of attributes and is equipped with a secret key associated with his/her attribute set. The person can freely get any interested encrypted information from the cloud server. However, the person can decrypt the encrypted data if and only if his/her attribute set satisfies the access coverage embedded within the encrypted records.

The cloud server gives a public platform for owners to save and share their encrypted information. The cloud server doesn't conduct data get entry to control for owners. The encrypted records saved within the cloud server may be downloaded freely via any consumer.

C. Auditing Mechanism

Each AA may also generate an intermediate key for any attribute set related to a selected person, after which CA can generate the name of the game key for this consumer with none more verification. However, AAs can be compromised and can't be fully depended on. Meanwhile, the person legitimacy verification is carried out by way of guide hard work, and consequently AAs may additionally maliciously or incorrectly generate an intermediate key for an unverified attribute set. A malicious person will seek any feasible means to gain the name of the game key related to the unique attribute set to acquire the records get admission to permission. Under this assumption, the person could regularly display extraordinary behaviors. Usually, we want to keep the duty of AAs to prevent the compromised or misbehaved ones from freely generating secret keys for malicious customers. Like consumer responsibility addressed, we anticipate that we've got appropriate techniques to detect customers' bizarre behaviors. The method of Auditing is periodically accomplished or occasion-prompted by using CA to mandatorily ask a suspected consumer to securely publish key of a given attribute, timestamp in his/her gained mystery key. In order to continue to gain records, customers must cooperate to perform the process correctly. However, which will mislead CA, a suspected user nevertheless has the motivation to publish a mystery key aspect that doesn't belong to him/her. Thus, to put into effect a powerful tracing, CA needs to affirm the received secret key components without a doubt belong to the given consumer.

4. CONCLUSION

The end of this paper is to eliminate the single-point overall performance bottleneck of the existing CP-ABE schemes; we proposed a new framework, named RAAC. Our proposed scheme gives a high-quality-grained, strong and efficient access control with one-CA/multi-AAs for public cloud storage. Our scheme employs multiple AAs to proportion the burden of the time-consuming legitimacy verification and standby for serving new arrivals of customers' requests. We also proposed an auditing method to trace an attribute authority's capacity misbehavior.

REFERENCES

[1] Kaiping Xue, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, David S.L. Wei, and Peilin Hong, "RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage", DOI 10.1109/TIFS.2016.2647222, IEEE Transactions on Information Forensics and Security

[2] 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. 1214–1221, 2011

[3] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.

[4] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proceedings of the 16th ACM conference on Computer and Communications Security (CCS 2009). ACM, 2009, pp. 121–130.

[5] 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.

[6] 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.

[7] 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

[8] J. Hur, "Improving security and efficiency in attributebased data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271–2282, 2013.

[9] 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, 2014, pp. 3782–3787

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in International Workshop on Public Key Cryptography. Springer, 2011, pp. 53–70