CP-ABE with MAACS for Secure Cloud Storage

[1]Mr. Velpula Sundara Ratnam,[2]Ms. G V Rama Gayatri
[1]Associate professor, Dept. of CSE,Malla Reddy Engineering College for women,Misammaguda, Dhulapally,Secundrabad-500100
[2]M. Tech, Dept. of CSE ,Malla Reddy Engineering College for Women,Misammaguda, Dhulapally,Secundrabad-500100

Abstract-In most current CP-ABE schemes there's only one authority liable for attribute management and key distribution. This simplest-one-authority scenario can carry a unmarried-factor bottleneck on both protection and performance. Once the authority is compromised, an adversary can easily attain the most effective-one-authority's grasp key, after which he/she will generate personal keys of any characteristic subset to decrypt the precise encrypted statistics. Moreover, once the best-one-authority is crashed, the system completely can't work nicely. Therefore, those CP-ABE schemes are still some distance from being extensively used for get admission to control in public cloud garage. In this paper, from some other perspective, we conduct a multi-authority access manage scheme for public cloud garage, named MAACS, wherein a couple of government together manage a uniform characteristic set. In MAACS, taking advantage of (AA, U) [AA indicates attribute authority, U indicates users] threshold secret sharing, the master key can be shared among a couple of government, and a prison person can generate his/her secret key with the aid of interacting with characteristic authorities. Security and overall performance analysis results show that MAACS is not best verifiable relaxed when much less than AA authorities are compromised, but also sturdy when no much less than AA authorities are alive in the machine.

Keywords- CP-ABE;secret sharing;multi-authority; public cloud storage;access control

I. INTRODUCTION

Cloud computing is a innovative computing method, by which computing sources are furnished dynamically via Internet and the information garage and computation are outsourced to a person or a few party in a 'cloud'. It significantly attracts interest and interest from both academia and enterprise because of the profitability, but it also has as a minimum 3 challenges that should be treated before coming to our real existence to the nice of our know-how. First of all, facts confidentiality must be guaranteed. The facts private ness is not most effective approximately the data contents. Since the maximum attractive part of the cloud computing is the computation outsourcing, it is a long way past sufficient to simply behavior an get right of entry to manipulate. More possibly, customers need to govern the privileges of facts manipulation over other customers or cloud servers. This is because while sensitive facts or computation is outsourced to the cloud servers or every other user, which is out of users' manipulate in most cases, privateness risks could rise dramatically because the servers would possibly illegally look into customers' statistics and access touchy records, or other users is probably capable to infer touchy records from the outsourced computation. Therefore, no longer best the get entry to but additionally the operation have to be managed. Secondly, personal facts (defined via each user's attributes set) is at threat because one's identification is authenticated primarily based on his statistics for the motive of get admission to control (or privilege control in this paper). As people are getting more worried about their identity privateness in recent times, the identification privacy additionally desires to be covered earlier than the cloud enters our lifestyles. Preferably, any authority or server alone need to not know any consumer's non-public information. Last however not least, the cloud computing gadget have to be resilient within the case of security breach in which some part of the machine is compromised by using attackers.

Various techniques had been proposed to defend the statistics contents privateness through get admission to manipulate. Identity-based encryption (IBE) turned into first delivered by means of Shamir [1], in which the sender of a message can specify an identity such that only a receiver with matching identification can decrypt it. Few years later, Fuzzy Identity-Based Encryption [2] is proposed, which is also referred to as Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a fixed of descriptive attributes, and decryption is feasible if a decrypter's identification has a few overlaps with the only specific within the ciphertext. Soon after, greater preferred tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) [3] and Ciphertext-Policy AttributeBased Encryption (CP-ABE) [4], are presented to explicit more standard condition than easy 'overlap'. They are opposite numbers to every different inside the feel that the choice of encryption policy (who can or can't decrypt the message) is made with the aid of special events. The in advance ABE schemes contain best one authority to keep the whole characteristic set, that could bring

a single-factor bottleneck on each security and performance. Subsequently, a few multi-authority schemes are proposed, in which multiple government one at a time hold disjoint characteristic subsets. However, the single-factor bottleneck trouble remains unsolved. In this paper, we endorse a robust multi-authority CP-ABE get admission to control scheme, named MAACS, to cope with the single-factor bottleneck on both security and performance in maximum existing schemes. In MAACS, a couple of authorities collectively manage the complete attribute set but no person has full manage of any particular characteristic. Since in CP-ABE schemes, there may be always a mystery key (SK) used to generate characteristic non-public keys, we introduce (AA, U) threshold secret sharing [5] into our scheme to share the name of the game key among auth orities. In MAACS, we redefine the secret key within the conventional CP-ABE schemes as master key. The creation of (AA; U) threshold mystery sharing guarantees that the grasp key can not be received by means of any authority alone. To the nice of our understanding, this paper is the primary try and cope with the single point bottleneck on each safety and performance in CP-ABE get right of entry to control schemes in public cloud storage.

Main contributions of this work can be summarized as follows:

A. In existing access control systems for public cloud storage, there brings a single-point bottleneck on both security and performance against the single authority for any specific attribute. To the best of our knowledge, we are the first to design multi-authority access control architecture to deal with the problem.

B. By introducing the combining of (AA; U) threshold secret sharing and multi-authority CP-ABE scheme, we propose and realize a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set.

C. Furthermore, by efficiently combining the traditional multi-authority scheme with ours, we construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

II. RELATED WORK

In the KP-ABE [6], a ciphertext is associated with a set of attributes, and a personal secret is related to a monotonic get right of entry to shape like a tree, which describes this person's identity (e.G. IIT AND (Ph.D OR Master)). A user can decrypt the ciphertext if and simplest if the get entry to tree in his personal key is happy via the attributes within the ciphertext. However, the encryption policy is defined within the keys, so the encrypter does now not have complete manage over the encryption policy. He has to believe that the key mills problem keys with accurate structures to accurate customers. Furthermore, when a re-encryption takes place, all the customers within the same gadget ought to have their personal keys re-issued with a view to advantage get entry to to the re-encrypted documents, and this procedure reasons enormous troubles in implementation.

In [7] and [8], a multi-authority gadget is provided in which each person has an ID and they can interact with each key generator (authority) the use of one of a kind pseudonyms. One consumer's one-of-a-kind pseudonyms are tied to his non-public key, but key mills by no means recognise approximately the private keys, and as a consequence they're not capable of link more than one pseudonyms belonging to the identical consumer. Also, the whole attributes set is split into N disjoint sets and managed via N attributes authorities. In this putting, each authority knows most effective part of any consumer's attributes, which are not enough to figure out the user's identity. However, the scheme proposed by way of Chase et al. [8] considered the simple threshold-primarily based KP-ABE, which lacks generality in the encryption coverage expression. Many characteristic primarily based encryption schemes having multiple government were proposed afterwards [9] however they both additionally rent a threshold-based ABE [9], or have a semi-honest critical authority [10], or cannot tolerate arbitrarily many customers' collusion assault [9].

Ciphertext-Policy Attribute-primarily based Encryption (CP-ABE) [11] is seemed as one of the maximum appropriate technologies for information get admission to manage in cloud garage structures, because it gives the facts owner more direct manipulate on get entry to guidelines. In CP-ABE scheme, there is an authority this is responsible for characteristic control and key distribution. This simplest-one-authority scenario can bring a unmarried-factor bottleneck on each protection and overall performance. Once the authority is compromised, an adversary can without difficulty gain the handiest-one-authority's master key, and then he/she can generate non-public keys of any characteristic subset to decrypt the particular encrypted facts. Moreover, as soon as the most effective-one-authority is crashed, the machine completely cannot work well. Therefore, those CP-ABE schemes are nevertheless a ways from being widely used for get admission to manipulate in public cloud garage.

III. IMPLEMENTATION OF MAACS

3.1 System Model

In robust multi-authority public cloud storage systems, there exist five entities: a global certificate authority (CA), multiple attribute authorities (AAs), data owners (Owners), data consumers (Users), and the cloud server.

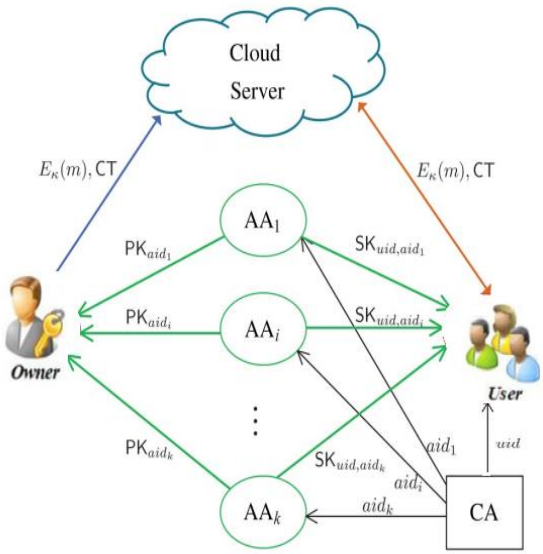

Fig.1:System Architecture

Certificate Authority (CA):

The certificate authority is a international depended on entity within the system this is responsible for the improvement of the device with the aid of using installing tool parameters and characteristic public key (PK) of every attribute inside the complete function set. CA accepts clients and AAs' registration requests with the aid of way of assigning a unique uid for each jail patron and a completely particular useful resource for every AA. CA additionally comes to a selection the parameter t approximately the edge of AAs which is probably concerned in customers' secret key era for each time. However, CA isn't worried in AAs' grasp key sharing and customers' mystery key era.

Attribute Authorities (AA):

The function government attention on the venture of function manipulate and key era. Besides, AAs take part of the responsibility to assemble the machine, and that they may be the directors or the managers of the software program gadget. Different from different existing multi-authority CP-ABE systems, all AAs together control the entire characteristic set, but, any character of AAs cannot assign customers' thriller keys on my own for the hold close secrets and techniques shared by way of the use of all AAs. All AAs cooperate with every different to proportion the grasp key. By this indicates, each AA can benefit a chunk of grasp key share as its non-public key, then each AA sends its corresponding public key to CA to generate one of the machine public keys. When it comes to generate users' mystery key, every AA great need to generate its corresponding secret key independently. That is to mention, no communication among AAs is needed in the segment of customers' mystery key technology.

Data Owner (Owner):

The information owner (Owner) encrypts his/her report and defines get entry to coverage approximately who can access his/her records. First of all, each proprietor encrypts his/her facts with a symmetric encryption set of regulations like AES and DES. Then the proprietor formulates get proper of entry to coverage over an characteristic set and encrypts the symmetric key underneath the insurance constant with attribute public keys gained from CA. Here, the symmetric key's the vital aspect used within the former technique of symmetric encryption. After that, the owner sends the whole encrypted facts and the encrypted symmetric key to store within the cloud server. However, the owner doesn't depend upon the cloud server to conduct statistics get entry to govern. Data stored in the cloud server can be won with the useful resource of any statistics patron. Despite all this, no information purchaser can benefit the plaintext without the feature set enjoyable the get entry to coverage.

User:

The information client (User) is assigned with a global individual identification uid from CA, and applies for his/her thriller keys from AAs collectively along with his/her identification. The purchaser can freely get the ciphertexts that he/she is interested in from the cloud server. He/she could be able to decrypt the encrypted records if and most effective if his/her function set satisfies the get entry to insurance hidden inside the encrypted records.

Cloud Server:

The cloud server does no longer something however offer a platform for proprietors storing and sharing their encrypted information. The cloud server doesn't behavior records get proper of entry to govern for proprietors. The encrypted facts saved inside the cloud server may be downloaded freely with the aid of any records customer.

3.2 (AA, U) Threshold Secret Sharing:

Secret sharing [12] is a manner used to proportion a mystery among a set of members, every of whom is allocated partial records approximately the secret, which is referred to as a share of the call of the sport. The thriller may be reconstructed simplest when a enough wide sort of partial stocks are combined together. Individual stocks are of little want on their private. There are several forms of mystery sharing schemes, among which, the most fundamental sorts are the so-referred to as (t; n) threshold schemes.

IV. CP-ABE with MAACS:

The framework of data access control scheme for multi-authority cloud storage systems contains the following phases: CASetup(μ) → (GMK,GPP , (GPKuid , GPK0uid) , (GSKuid, GSK0uid), Certificate(uid)).

The CA setup set of rules is run by using the CA. It takes no enter apart from the implicit security parameter μ. It generates the worldwide grasp key GMK of the gadget and the global

public parameters GPP. For every consumer uid, it generates the consumer's international public keys (GPKuid; GPK0uid) the consumer's international mystery keys (GSKuid; GSK0uid) and a certificate Certificate (uid) of the user.

AASetup (Uaid) → (SKaid, PKaid, {VKxaid,PKxaid} xaid € Uaid).

The attribute authority setup set of rules is run by each characteristic authority. It takes the characteristic universe Uaid controlled by means of the AAaid as input. It outputs a secret and public key pair (SKaid; PKaid) of the AAaid and a set of model keys and public characteristic keys VKxaid;PKxaid xaid € Uaid for all the attributes managed via the AAaid.

SKeyGen(GPP , GPKuid , GPK0uid , GSKuid , SKaid, Suid,aid, {VKxaid,PKxaid} xaid € Suid,aid) → SKuid,aid.

The secret key era algorithm is run by means of every AA. It akes as inputs the global public parameters GPP, the worldwide public keys (GPKuid,GPK0uid) and one worldwide mystery key GSKuid of the person uid, the secret key SKaid of the AAaid, a fixed of attributes Suid,useful resource that describes the person uid from the AAaid and its corresponding version keys fVKxaidg and public attribute keys PKxaid. It outputs a mystery key SKuid,useful resource

Encrypt (GPP, {PKaidk}, K, A) → CT.

The encryption set of rules is run via the information owner to encrypt the content material keys. It takes as inputs the worldwide public parameters GPP, a set of public keys PKaidk for all of the AAs in the encryption set the content key K and an get admission to policy A. The set of rules encrypts K in keeping with the get admission to policy and outputs a ciphertext CT. We will count on that the ciphertext implicitly contains the get right of entry to policy A.

Decrypt (CT, GPKuid, GSK0uid, {SKuid, aidk})→ K.

The decryption set of rules is run by way of customers to decrypt the ciphertext. It takes as inputs the ciphertext CT which contains an get right of entry to coverage A, a worldwide public key GPKuid and a global secret key GSK0uid of the person uid, and a hard and fast of mystery keys SKuid, aidk from all the concerned AAs. If the attributes SKuid, aidk of the user uid satisfy the get admission to coverage A, the set of rules will decrypt the ciphertext and go back the content material key K.

V. SECURITY PERFORMANCE ANALYSIS

This section numerically evaluates the performance of MAACS in terms of storage, communication, and computation overhead.

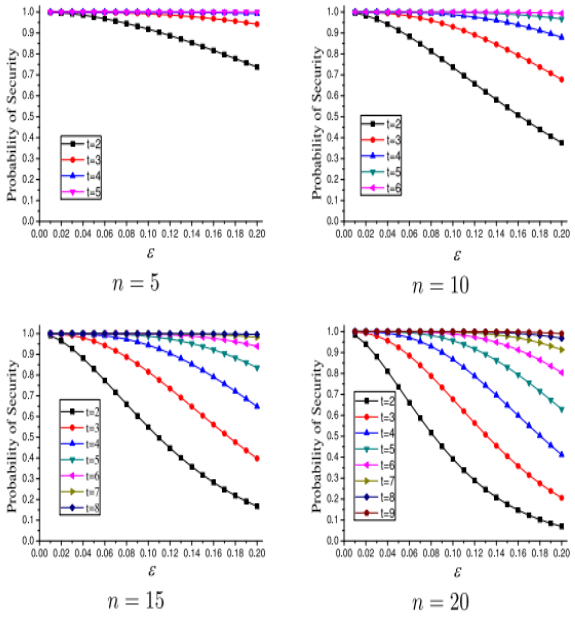

Fig.2:Probability of security against AA compromise.

To have an intuitive knowledge for the safety of MAACS towards this attack, we draw the opportunity map in Fig. 2, which indicates the possibility of device safety as opposed to the quantity of AAs n and the possibility ". From the discern, we will see that for any range of authorities, we can growth the cost of t to make MAACS at ease in opposition to the above assault as an excessive possibility. But we can also observe that the overlarge price of t will simplest bring more overhead in preference to boom the safety successfully. For example, the machine may be comfy with chance near 1, whilst we set the cost of t simplest same to 5 in place of a larger fee in a system with 10 authorities, even the adversary can tool the authority as a high opportunity 0.2. We can say, MAACS can be secure against the above attack with the best threshold price t.

VI. CONCLUSION

In this paper, we recommend a brand new multi-authority CP-ABE get entry to manipulate scheme, named MAACS, in public cloud garage, in which all AAs at the same time manage the whole characteristic set and proportion the grasp key a. Taking benefit of (AA, U) threshold mystery sharing, by way of interacting with all AAs, a prison user can generate his/her mystery key. Thus, MAACS avoids any person AA being a unmarried-point bottleneck on both security and performance. The analysis results display that our access manage scheme is strong and comfy.

VII. REFERENCES

[1]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[4]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[5]. T. Pedersen, "A threshold cryptosystem without a trusted party," in Proc. 10th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 1991, pp. 522–526.

[6]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[7]. M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[8]. M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

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

[10]. V. Božovi´ c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[11]. J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321-334.

[12]. A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

Authors Profile

Mr. Velpula Sundara Ratnam Obtained his B.Tech from JNTUCEH, Kukatpally and received M-Tech in the stream of Computer Science and Engineering at JNTUCEH, Kukatpally, He has 13 years of Experience teaching for both under graduate and post graduate students .He published 11 technical papers in both the National and International Journals and conferences .He is now working as Associate professor at Malla Reddy Engineering College for women JNTUH.

Ms. G V Rama Gayatri obtained her B Tech from Malla Reddy College of Engineering for Women JNTUH, with First Class Distinction. She is currently pursuing M. Tech from Malla Reddy Engineering College for Women JNTUH.