IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 31-35
www.iosrjournals.org

Protected and Verifiable Policy Update for Big Data Access Control in the Cloud

Vishnu R. Lembhe[1], Ravi A. Mule [2], Pratik R.Ponde[3], Tejas S. Yerguntla[4]
R.G.Raut5
[1,2,3,4](IT Department, P.D.V.V.P.C.O.E,SPPU(MS), India)

***Abstract*:** *In computing environment, the storage of big data is major problem. So to overcome this store the big data in cloud because it has capabilities of storing largeamount of data and processing a high volume of user access requests. Cloud computinguse the Attribute Based Encryption (ABE) [3] for providing the end to end security forbig data in a cloud. Using this ABE policy, updating has been a challenging issue in the previous implementations, firstly data owners have to retrieve the data and thenre-encrypt the new access policy and send back to the cloud .Due to this, high communication and computational burden was on the data owners. Soto overcome this problem of existing system here proposed a new system that dynamicallyupdates a policy for big data in the cloud. Data owners have to just check whether cipher text has been updated correctly or* not.

I. Introduction

A storage platform which provides a high velocity and various information which needs a new processing for enabling advanced decision making and optimization process is referred as big data. On cloud they have an efficient way to store a large amount of data Because of its features that stores a big data and user access requests are high in volume. When analyzing big data in the cloud, data security is serious problem because a dataowner does not have trust on cloud servers. Attribute Based Encryption (ABE) [3] has Come to an existence for a promising technique to provide the end to end data security in cloud storage system. By this, access policies can be define by the data owners in such way where only users who has attributes which satisfies their policy can decrypt thedata. When a huge amount of people or any organization outsources the data into thecloud, [4] policy updating is significant issue because data access policies can be changeddynamically by data owners.

The policy updating is a difficult thing in attribute based access [1] because when dataowner stores data into the cloud, it does not have a copy of it in local systems. If any particular data ownerwants to change the data he has to transfer data back to hislocal site from the cloud, encrypt it again and move back to the server. Due to this,There is a high communication between them which puts lot of burden on data owners. For this have to develop a new method in which data can be edited on the cloudIt and does not need to download it just to check whether a cipher text has been updatedsuccessfully. In the policy updating method, they were provide requirementssuch as correctness, completeness and security that have been described in key structurepolicy and cipher text structure policy. Focus on secure and verifiable policy updating method for ABE systems and propose a novel scheme. Our contributions in this include a new method for outsourcing data in the server, efficient data access control and dynamic policy updating.

II. Existing System

In [3] ABE(Attribute Based Encryption) is providing a security over a cloud but other problem are created, credential of user's may change and third party will get access of it or third party may store the cipher text by revocation our valuable credential's in trouble or attack a attacker by doing revoking can easily get credential's suppose user has stored his valuable credential's over a storage of cloud and one employee whose name is Ramesh for misbehaving Ramesh is red in to an organization or a company he has old key by using that key he can invoke and access credentials mostly this are a common attack on user's information (credential's) to handle such a problem our scheme allows a storage server or other kind of server to update the stored encrypted data or a cipher text to prevent and disqualify revoked so here key update can dynamically revoke selected user's.

To solve this attack, A user who is not trusted with key information and he is processed for a cipher text or a encrypted data stop him to revoking a decrypting data who is encrypted in the past. tool is a new procedure called cipher text delegation that can help to a cipher text to "re-encrypted" and become a strong policy and it is restrictive only to a public information. here we first provide strong secure construction by modifying an ABC scheme also we prove that here is a strong security, Also to add some efficient algorithm in

to a ABE system which make it more perfect than previous. Policy which is a big headache for a owner means there is need to a change the policy then it retrieve in to a local system and make changes and again send it back to a server which take lot of time, cost and hard work also a need of a big storage system which is not available In previous system, so we propose a new system which fulfill all previous defects.

III. Drawbacks Of Previous System

1 Previous system faced the problem of collusion resistant also this system cannot handle the complex policies and this system requires the coordination between authorities.
2 In previous system attacker can easily access the credentials of a user by revoking. Here data is encrypted only once that cans an open invitation for a attacker.
3 In previous system user has to encrypt his data before it send back to a server with policy and if any changes need to made later then he have to again retain data and made changes.
4 ABE system is efficiently working but it fails to minimize the load of a owner. Owner has to spend high cost for management also takes to much time for a operation.
5 Revoking is a big issue in a previous system that causes user to lost is information and also minimize the security

There is also not any effective key combination that can prevent revocation mostly it happen in a company which is provide a security to a data.

IV. Problem Statements

Dynamic policy updating is a big problem now a day's owner has to retain his data into our local system and made changes this will take huge time and large burden on aowner hence policy updating is difficult on owners point of view also there is one another problem here owner has to maintain security when retaining data . First upon encrypt it under the policy when at the retaining time it has to decrypt and again encrypt it under new policy and upload on to a server, in this scenario first upon user has to prove his identity on to a server. Here policy updating is has been a challenging issue when ABE [3] is used to construct access and control schemes. A trivial implementation is to let data owners retrieve the data and re-encrypt it under the new policy and send back it to the cloud. This method however incurs high overhead and heavy computation burden on a data owners.

Suppose as an example Ramesh is an owner and he need to update his policy for some reason to update his policy first upon he need to bring our retrieve his data on to a local system from a server then Ramesh decrypt which is in a encrypted format after decrypting then he will make changes in to a system and after that using a new accesspolicy he will again encrypt or make a simple text / Plain text in to a Cipher text which is in a encoded format user cant read it directly he need to again decrypt it using key orsomething then Sure will updating it on to a server in this whole operation there was a lot of Bur-don on a Ramesh that the bring the data in to a local system and then againsend it back to a server in this a high overhead and a heavy communication Bur-don on a Ramesh also a time which is take more and more time to complete this operation means simply a time consuming process also make a lot of changes in which policy is include where policy update because at the time where retrieve data then again they changes in to a old policy and make it on a new policy. [1] ABE which is provide a security on a cloud here policy updating is big issue where they can't update the policy dynamically they have to bring it in to a local system.

V. Proposed System

In this project they propose a policy which can be dynamically update and a scheme that has access control which is enabled themselves with updating a dynamic policy for big data in the cloud our aim is to developed policy updating by outsource for a ABE [3] system in a project they minimize the owner's computation work . To do this need to use previous old access policy and encrypted data which is encrypted previously, also in this project they are proposing algorithm's which are related policy updating for different kinds of access policies. they are proposing a method which enable data owner's to check correctness of cipher text updating they are also focusing effectiveness in terms of correctness, completeness, security and performance.

They proposed a scheme where data owner is just send a query about a policy then server will update the policy dynamically and investigate the correctness of a policy which is dynamically updated by a server. ABE method which provide a security on a cloud is interrupt for a new policy updating by dynamically so here focus on our new scheme and control algorithm's that can control and manage different types of access policy.

VI. System Analyses And Proposed Architecture

In this project proposed a policy which can be dynamically update and a scheme that has access control which is enabled themselves with updating a dynamic policy for big data in the cloud our aim is to developed policy updating by outsource for aABE system in there project they minimize the owner's computation work and avoid encrypted data transmission. to do this they need to use previous old access policy and encrypted data which is encrypted previously, also in this project they are proposing algorithm's policy updating for different kinds of access policies. They proposed a method which enable data owner's to check correctness of cipher text updating they are also focus on various other scheme in term of correctness, completeness, security andperformance. they proposed a scheme where data owner's is a send a query about a policy then server will update the policy dynamically and investigate the correctness of a policy which is dynamically update by a server. ABE method which provide a security and a cloud is interrupt for a new policy updating by dynamically so here focus on our new scheme and control algorithm's that can control andmanage different types of access policy.[4]

There are three attributes in which Administrator (Data Owner) , Users (Data Consumers) and Finally Cloud (Cloud Server) which are shown in fig 1 here multiple authorities they consider for a cloud storage will see it one by one.Cloud Server Which is a cloud server and has capability to maintain all to store data and maintain the data. Large amount of data stored inthecloud server. Cloud Serverstores data of a data owner and give access of this data to users also provide services to them, The main project aim is carried out on a server, Server is responsible for aupdating cipher text from old policies in to new policies. Server dynamically updates thepolicy which takes query from a owner and as per his requirement server will update the policy.

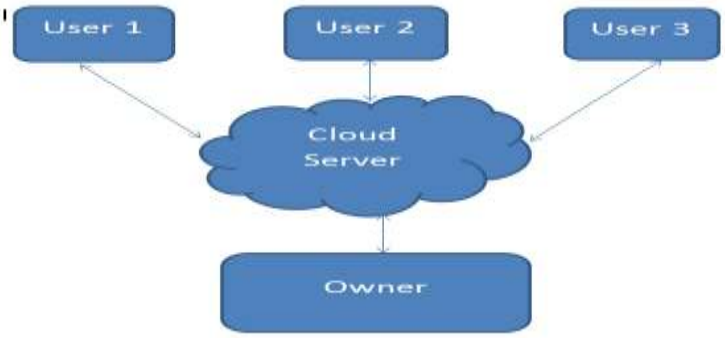

Fig 1 Proposed Architecture

Administrator - Administrator is responsible for a defining a Policy, data ownerdene access policy and encrypt information or a data under this policies he did thisoperation before hosting them in the cloud. If any query to a owner about the policy hegive his query to the server and ask server to the update the policies and then server willautomatically update the old policy in to the new policy also the cipher text is updateddynamically. After updating the policy owner will Check whether the server has updated the policy Correctly or not if it is not then again owner will send query.

Users - Users is responsible for a access of data on to a server But first upon user has to prove his identity on to a server, Each user has assigned a global user identity and byproving his assigned identity he can freely get the encrypted data or a cipher text from the server. User has capability to decrypt the encoded data or a cipher text but whenits attributes satisfy the access policy which is defined in the cipher text by owner usingserver.

Authority - Here authority is defined and every authority is not dependent with each other authority, It is responsible for managing attributes of users in its domain. Forhigher security it generates a secret or private key pair for each attribute in its domainbecause only dependent upon a public key is open invitation for a attacker and mostlyattack is happened on to a server that's why here private or secret key pair is assignedto each attribute in its domain. Here also a secret key is generated for each user butaccording to his or her attributes.

We have a following Algorithm for a dynamic policy access control scheme.

6.1 GlobalSetup(l)-GP.

The global setup algorithm takes no input other than the implicit security parameter l. It outputs the global parameter GP for the system.

6.2 AuthoritySetup(GP;AID) - (SK;PK).

The authority setup algorithm is run by each authority AID with GP and the authority identity AID as inputs and its secret/public key pair (SKAID;PKAID) as outputs.

6.3 S-KeyGen(GID;GP;SGID;AID;SKAID) - SKGID;AID.

Each authority AID runs the secret key generation algorithm to generate a secret key SKGID;AID for user GID. It takes as inputs the global identity GID, the global parameter GP, a set of attributes SGID;AID issued by this authority AID and the secret key SKAID of this authority. It outputs a secret key SKGID;AID for this user GID.

6.4 Encrypt(fPKg;GP;m;A) ! CT.

The encryption algorithm takes as inputs a set of public keys fPKg of relevantauthorities, the global parameter GP, the message m and an access policy A. It outputs a cipher-text CT.

6.5 Decrypt(CT;GP;fSKGID;AIDg)!m.

The decryption algorithm takes as inputs the cipher-text, the global parameterGP and a collection of secret keys from relevant authorities for user GID. It outputs the message m when the user's attributes satisfy the access policy associated with the ciphertext. Otherwise, the decryption fails.

6.6 UKeyGen(fPKg;EnInfo(m);A;A0) - UKm.

The update key generation algorithm is run by the data owner. It takes as inputs the relevant public keys, the encryption information EnInfo(m) of the message m, the previous access policy A and the new access policy A0. It outputs the update key UKmof m used to update the ciphertext CT from the previous access policy to the new one.

6.7 CTUpdate(CT;UKm) - CT0.

The ciphertext updating algorithm is run by cloud server. It takes as inputs the previous ciphertext CT and the update key UKm. It outputs a new ciphertext CT0 corresponding to the new access policy A0.

VII. Related Work

In cloud storage system Attribute Based Encryption (ABE) [3] is used and it is known as one of the most suitable technologies, it has two forms ABE (KP-ABE) and Cipher text policy ABE both are effective for a ABE. Policies are building into user's secret keys in a KP-ABE. While in other form means in CP-ABE attributes are used to describe the user's attribute and the access policies over there attributes are attached to the encrypted are attached to the encrypted data. In fine-grained access control of encrypted data process key policy based encryption and also discussed how to change policies on keys. In Dynamic credentials & cipher text delegation for attribute-based encryption's author proposed a cipher text delegation method which is used to update the policies of cipher text. In" "Privacy preserving cloud data access with multi-authorities," author proposed any valid user's can cipher text re-encrypted by decrypting it first, thus a new outsourced policy updating method is desired for ABE system's.

VIII. Conclusion

In this project, they have audited the policy updating Problem in big data and going to invent some challenging requirements of problems that have been occurred. They aredeveloping an efficient method to store data in the cloud server in such a. way that it satisfiesall the requirements. They were also using a expressive method for cloud to store big data i.e. attribute based access control scheme and designing various policy updating algorithms. In this project, they proposed a method which enables data owners to check the correctness of cipher text updating. They also focus on various other schemes in terms of correctness, completeness, security and performance. Although, a design has been based on different schemes our methods for policy updating can also be able for otherABE systems.

References

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in CCS06. ACM, 2006, pp. 8998.
[2] A. Sahai, H. Seyalioglu, and B. Waters, Dynamic credentials and ciphertext delegation for attribute-based encryption, in CRYPTO12. Springer, 2012, pp. 199217.
[3] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption,"

in EUROCRYPT'11. Springer, 2011, pp. 568–588.

[4] T. Jung, X.-Y.Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in INFOCOM'13. IEEE, 2013, pp. 2625–2633.