AN EFFICIENT PRIVACY FOR OUTSOURCING DATA IN UN-TRUSTING CLOUD USING MODIFIED- CP-ABE TECHNIQUE

Amritesh Kumar[1], SaloniSinha[2], Pooja Paul [3], Shubhangee D Anant [4],
[1,2,3,4] *UG student,*
Department of Computer Science Engineering,
SRM University, Ramapuram, Chennai – 89.
[1]*amriteshmishra.6june@gmail.com,* [2]*salonisinha1102@gmail.com,*
[3]*poojapaul36@gmail.com,* [4]*shubhangeedanant@gmail.com*

Ms.Adlene Ebenezer[5]
Assistant Professor[5],
Department of Computer Science Engineering,
SRM University, Ramapuram, Chennai – 89.

Abstract— Cloud computing is going to be very famous technology in IT enterprises. For an enterprise, the data stored is huge and it is very precious. All tasks are performed through networks. Hence, it becomes very important to have the secured use of data. In cloud computing, the most important concerns of security are data security and privacy. And also flexible and scalable, fine grained access control must be maintained in the cloud systems. For access control, being one of the classic research topics, many schemes have been proposed and implemented. There are policy based schemes have been proposed. In this paper, we are going to explore various schemes for encryption that consist of Attribute based encryption (ABE) and its types CP-ABE. Further discussion consists of improvement in CP-ABE to CP-ASBE and to HASBE. A comparison table has been included for comparative study of these techniques. In this project, we propose a framework for efficient and privacy-preserving outsourced cloud using CP-ABE technique. Our proposed technique is designed to allow users to outsource their own data to cloud server for secure processing. Using CP-ABE, a user can securely outsource the storing and processing of data to a cloud server without compromising the security of the (original) data and the computed results. More specifically, we present a cipher policy attribute based encryption with RSA key distribution, the core cryptographic primitive, to reduce the private key exposure risk in data processing.

Keywords—Access control, Attribute based encryption, Key policy, cipher text policy, hierarchical-ASBE.

1. Introduction

Recent development of the network and computing technology facilitate many people to easily share their data with others using online external storages. Along with the development of the Internet and the distributed computing technology, there is a developing

demand for data sharing and processing in an accessible distributed computing environment. Cloud computing is an alternative to information technology as a result of its resource-sharing and low-maintenance characteristics. Among the recent adoption and diffusion of the data sharing paradigm in spread systemssuch as online social networks or cloud computing, there have been growing demands and firm for distributed data security. Immediately as people enjoy the advantages of these new technologies and services, their firm about data safety and access control also begin. Public would like to make their acute or private data only reachable to the authorized people with credentials they described. Here are various other issues such as risks of privacy exposure, scalability in key management, supple access and efficient user revocation. Toward achieve fine grained and scalable data access control for any records stored in semi trusted servers, influence attribute based encryption (ABE) techniques[1] is a promising cryptographic approach to encrypt record file. ABE is envisioned as an significant tool for addressing the problem of secure and fine-grained data sharing and access control. During an ABE system, a user is identified by a set of attributes.

Sudden case that in un-trusted storage data servers are neither can be expect to accomplish data access policies nor allowed to learn contents of susceptible data. So pursuing best practice, data owner encrypts the data before outsourcing it on storage server. This helps to sustain data confidentiality. The user who holds decryption key[2][3] is acknowledged to get access to encrypted data. There are few claiming pertained to this type of access control mechanism.

We summarize them as below:

Exquisite access control vs. scalability:

Fine-grained access control is required whenever acute data needs to be revealed. Traditionally access control is accomplished by ACL-based connection control[4], capability-based connection control and role-based connection control. Making use of ACL based, and capability-based cryptographic method, ahead towards the scalability problem. When ACL's are used as cryptographic method, complicated for each data object in terms of data encryption operation or cipher text size is continuous to the number of system users. This results in few scalable system. Thus the Capability-based access control do have the same system scalability issue. In role-based access control, remembering the authorized users list is not expected as access to data is granted on the basis of user's role. Several contempo work in the areas of "access control of outsourced data" and "shared cryptographic file systems" do address the data access control problems with accepted symmetric and asymmetric cryptography. To overcome this issue, ABE have been security problem needs to be addressed before ABE is adapted in practical systems.

User Dynamics:

In the real time systems, user may join or leave system at any time. So acknowledge and recall use access advantages, there should be accomplished user management in place. In cryptography, user key repeal is always a matter of field. User key repeal in ABE is found challenge problem. Efficient repeal scheme for IBE that also applies to ABE is arranged.

User liability:

In cryptographic-based data access control, user who hold right decryption key, is allowed to access encrypted data. But sometime this leads to distribution of decryption key to unauthorized user by the authorized user. Copyright accurate application can be harmed more by such attack. A unique solution is needed to ignore key abuse attack

Privacysecurity:

It is good practice to open as less user privacy information to un-trusted servers. Even data owner would always adopt not to open his access policy information to server. It is mandatory to bring new construction to ABE than the existing one that takes care of privacy preservation policy.

2. Literature Survey

During 2009, M. Chase and S.S.M. Chow offered a distributed KP-ABE scheme that solves the key escrow difficulty in a multi-authority system. Within this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a dispersed way such that they cannot pool their data and link numerous attribute sets belonging to the same user. Individual disadvantage of this kind of fully distributed approach is the concert degradation. Seeing as there is no centralized authority with master secret information, all attribute authorities should speak with the other authorities in the system to produce a user's secret key. Here results is message overhead on the system setup phase and on any rekeying phase, and requires each user to store additional support key components besides the attributes keys, where N is the number of authorities in the system . Here 2009, Recently, S.S.M. Chow projected an anonymous private key generation protocol in identity-based writing such that the KGC can matter a private key to an authenticated user without knowing the list of users' identities. It seems that this unsigned private key generation protocol works properly in ABE systems when we indulgence an attribute as an identity in this creation. Though, establish that this cannot be modified to ABE systems due to mostly two reasons. Primary, in Chow's protocol, identities of users are not community anymore, at least to the KGC, since the KGC can make users' secret keys or else. Following the given collusion attack between users is the main security threat in ABE. Within 2008, Bettencourt, V. Kumar and Boldyreva planned first key revocation mechanisms in CP-ABE and KP-ABE settings, respectively. KP-ABE scheme consists of the following four algorithms:

1Setup: Here this algorithm takes as contribution a security parameter κ and proceeds the public key PK and a system master secret key MK. PK is used by significance senders for encryption. MK is used to produce user secret keys and is known only to the authority.

2. Encryption: Here this algorithm takes a communication M, the public key PK, and a set of attributes as input. It outputs the cipher text E.

3. Key Generation: In this algorithm takes as key an access structure T and the master secret key MK. It then outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.

4. Decryption: Here it takes as input the user's secret key SK for admittance structure T and the cipher text E, which was encrypted under the attribute set. Here this algorithm outputs the message M if along with only if the attribute set satisfies the user's admission structure T. Boundaries of KP-ABE:-Encryptor cannot make a decision that can decrypt the encrypted data. Here it can only prefer expressive attributes for the data, and has no option but to faith the key issuer. KPABE is not logically suitable to certain applications. For example, complicated transmit encryption, where users are described by a variety of attributes and in this, the one whose attributes competition a policy connected with a cipher text, it can decrypt the cipher text. KP-ABE scheme supports user secret key accountability. Here it is only if well grained access but has no longer with suppleness with scalability.

Expressive Key Policy Attribute Based Encryption:-
During KP-ABE [5], enables senders to encrypt messages with a set of attributes and secret keys are associated with access tree structure. Right to use tree structure specifies which all the cipher texts the key controller is permitted to decrypt. Expressive key-policy attribute-based encryption (KPABE) schemes permit for non-monotonic access structures. With the non-monotonic access tree structures are those may have negated attributes and with stable cipher-text size. Hence this is well-organized than KP-ABE.

Cipher text Policy Attribute-Set Based Encryption (CPASBE):-Since compared to CP-ABE[1] plan in which the decryption keys only bear user attributes that are prepared reasonably as a particular set, so users can only use all possible combinations of attributes in a distinct set issued in their keys to assure policies. Toward answer this problem, cipher text-policy attribute-set based encryption (CP-ASBE or ASBE for short) is introduced by Bobba, Waters et al. ASBE is a complete form of CPABE which organizes user attributes into a recursive set structure. Cipher text Policy Attribute Set Based Encryption (CP-ASBE) is a customized form of CP-ABE. It differs from accessible CP-ABE schemes that symbolize user attributes as a monolithic place in keys. Here it organizes user attributes into a recursive set based structure and allows users to oblige dynamic constraints on how those attributes may be collective to convince a policy. CP-ASBE consists of recursive set of attributes. The attractive attribute and the recursive key structure is implemented by four algorithms, Setup, Key Gen, Encrypt, and Decrypt

1. Setup: The depth of key structure take as input a depth parameter'. It outputs a communal key PK and master secret key MK.

2. Key-gen: It takes as input the master secret key MK, the individuality of user u, and a key structure A . It outputs a secret key SK for user u.

3. Encrypt: It takes as input the public key PK, a message M, and an right of entry tree T . It outputs a cipher text CT.

4. Decrypt: Take as input a cipher text CT and a secret key SK for user u. It outputs a significance m.

Stipulation the key structure a linked with the secret key SK, satisfies the access tree T, linked with the cipher text CT, then m is the unique correct message M. Otherwise, m is null. Purposely CP-ASBE allows User attributes are prepared into a recursive family of sets and Allowing attributes to join from multiple sets. Therefore, by grouping user attributes into sets and no constraint on how they can be mutual, CP-ASBE can hold composite attributes. More suppleness and well grained access is provided by AP-ASBE. Likewise, multiple arithmetical assignments for a given attribute can be supported by insertion each assignment in a divide set as well as placing it into a single set.

Limitations: - Challenge in constructing a CP-ASBE method is in selectively allowing users to merge attributes from various sets within a given key. Here is challenge for preventing users from combining attributes from many keys.

3. Existing Method

One application of cloud is IoT (or Cloud of Things) where computationally limited devices, such as body sensors (used to monitor patient's heart rate, blood pressure and glucose levels, etc), can send data to the cloud for processing.

In the body sensor example, it is important to ensure the security and privacy of patient's health and other personally identifiable information (PII), such as health status. The accuracy of the collected data is also crucial in applications, such as healthcare. In healthcare, most data (e.g. blood glucose, insulin, and C-peptide levels) are non-integer.

Traditional cryptosystems are generally designed to protect only integer values. Therefore, this will affect the accuracy of the data and consequence, decision making and in the worst case scenario, resulting in the wrong diagnosis of a patient.

4. Proposed Method

This paper has 5 main modules and three main algorithms for working the desired modules and getting the correct result. The main architecture of our module is given below. It will be the best way of explanation of our work that to go through module by module and for the better understanding it have some diagrams which is can make us understand it better. And it will be very easy to make someone understandabout the views of our work that have

been done with help of some different references which made our work easy as well as efficient with things that have been added to the modules are best of efforts. Inside these modules you find the liability and the transpierce of the work and the things have been made easy to understand and normally we can get the prospective of the propose system, where the new facilities are introduced and made easy to proceed further future work.

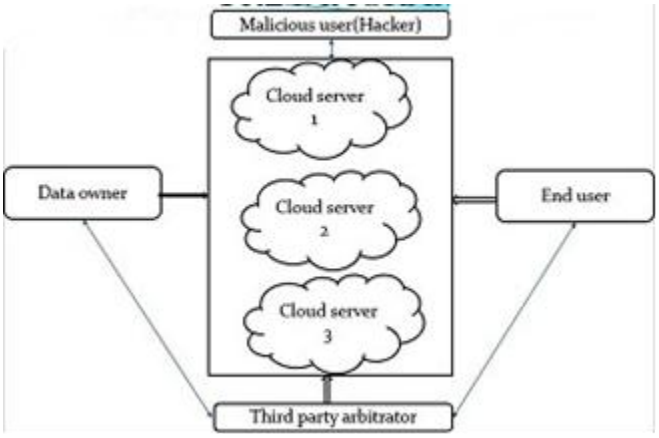

Figure 1: System Architecture of our Model.

Each of our model has one specific functionality with which each of them function at the front end and the backend. Each of which are dependent on each other. The modules are:

- Data owner
- End user
- Cloud server
- Third party arbitrator
- Attacker

Each of the model functionality along with its work flow is explained detailed below.

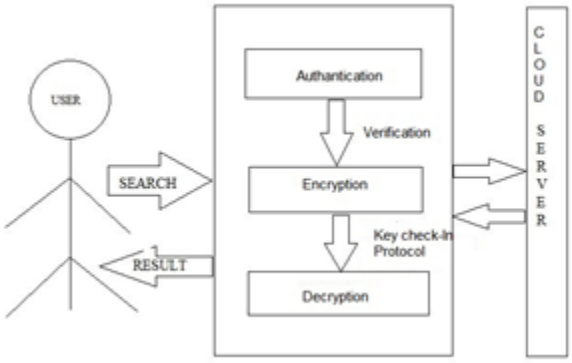

Figure 2: Dataflow Diagram of Our Work

This explains the detailed workflow of how our model works. In our module first you have to register yourself as a data owner with the appropriate cloud server and then you can start the end user process where you have to consider about the cloud server that means, both the module data owner as well as end user should be registered with the same cloud provider .Here after the all registration will done you can be able to upload the data to the cloud in data owner side where the file will be encrypted and the an activation code will be generated for the end user which will be sent through the mail id and parallely the meta data will be sent to the third party arbitrator for the verification if the file is safe then the final upload can be done otherwise the file will be rejected by data owner, After the encryption have been done the end user have to login to the domain with its login ID and the password, he has to send the request of the file to cloud server for the download, then the clod server will check the authentication of the user then it will approve the request, once the approval have done then the end user will get the file download link where he has to put the activation key and the mac address. We have the other module called Attackers who will try to change the file data with some inappropriate information that may can cause the data theft so for that he have the give the activation code will be sent to the authorized user only once you will be blocked by the modules then you have to get the authentication by data owner to proceed further. We have another module called rank search which will allocate the files that have been frequently searched it will make a stack of the file in search order by the users.

5.Experiment Results

A. Data Owner

The module helps the owner to register those details and also include login details. It helps the owner to upload his file with encryption using RSA algorithm. It ensures the files to be protected from unauthorized user. It will send the Meta data to the third party arbitrator to check the security and also will provide the activation code to the user through mail id .It follows the RSA algorithms which will encrypt the data using public key and decrypt the file using private key that private will the activation code for the user to download the data. While registering with data base all the information will be stored into the database table of the data owner which will visible to the cloud server when they will approve the requests from the user they can be able to check the information about the user which have given the request for the file.

Figure 3: Data owner

B. End user

It includes the user registration login details.It is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail email before enter the activation code. It also can view the file but cannot download until it won't put the activation code. And can also view the files.

Figure 4:End user

C. Cloud server

In this module[8] we have implemented the process of e process of authentication of the file request from the end user. It also can view the file and the file request. After the verification of the file will done by the third party arbitrator it will allow the user to give the request the files that have needed and those file will be stored into the database. It can also see the verification of the file and allow them to request every request from the user will be viewed by cloud server.

Figure 5: Cloud server

D. Third party arbitrator

These modules have many properties and have the authentication privilege. It can also verify the file while encryption and the information will be sent to the data owner. The third party auditor is one who is having the capabilities if doingthe cloud operations on user's request. Third party auditor is also acloud server which is connected with remaining all distributed cloudservers so that TPA can able to verify the user files in the cloudeither any malfunctioning or misbehaving server is corrupting theusers data by proving the challenge which contains size of the fileand token keys of the file to the distributed cloud servers. TPAstores the user's file related tokens and encrypted data and comparesthe received challenge results from different servers if both are samethen there is no malfunctioning in any server if any one server givesnot equal results then it we can easily identify that is themisbehaving server malfunctioning is occurred in that particular server.

Figure 6: Third party arbitrator

E. Attacker

This module[9][10] have developed in order to check the security level of the application , It will try to get the information from the cloud using fake id's and password , It also tries to make some kind of changes in the database. If this module will fail to change the document then process of login will be block for this module again it have to take permission from the data owner to start the proceedings as much wrong efforts will done that many times it will be blocked if the data owner can't able to permit the module it will not be able to process further in any kind of the activities. The data which have been changed this module can be retrieved by the cloud server

.

Figure 7: Attackers

6. Algorithms

Cipher Text Policy Attribute Based Encryption:-

The concepts of another adapt form of ABE called CP-ABE [1] that is Cipher text Policy Attribute Based Encryption. A new CP-ABE scheme, attribute policies are combine with data and attributes are combine with keys and only those keys that the combined attributes delight the policy combine with the data are able to decrypt the data. CP-ABE works in the flip-flop way of KP-ABE. With CP-ABE, the cipher text is with an access tree structure and each user secret key is fixed with a set of attributes. In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system and user secret keys. Only authorized users (i.e., users with calculated access structures) are able to decrypt by province the algorithm Decryption. In CP-ABE, each user is combine with a set of attributes. His secret key is developed based on his attributes. While encrypting a message, the encryptor described the threshold access structure for his attentive attributes. Through this the message is then encrypted, based on this access structure such that only those whose attributes delight the access structure can decrypt it. Along with CP ABE technique, encrypted data can be kept classified and secure against collusion attacks.

CP-ABE scheme consists of following four algorithms:

1. **Setup**: Here, this algorithm takes as input a security frame work and returns the public key as well as a system master secret key. The public key is used by message senders for encryption. Private Key is used to form user secret keys and is known only to the authority.

2. **Encrypt**: This algorithm takes as input the public framework PK, a message M, and an access structure .It outputs the cipher text.

3. **Key-Gen**: Here, this algorithm takes as input a set of attributes combine with the user and the public secret key, Private Key. It outputs a secret key that approve the user to decrypt a message encrypted under an access tree structure if and only if matches T.

4. **Decrypt**: Here, this algorithm takes as input the cipher text [CT] and a secret key [SK] for an attributes set. It returns the message [M] if and only if satisfies the access structure combine with the cipher text [CT]. In CP-ABE build upon how attributes and policy are combine with cipher texts and users' decryption keys. In a CP-ABE scheme, a cipher text is combining with a monotonic tree path structure and a user's decryption key is combining with set of attributes. In this scheme, the roles of cipher texts and decryption keys are switched as that in KP-ABE. The cipher text is encrypted with a access tree policy chosen by an encryptor.

And the corresponding decryption key is created with respectto a set of attributes. As the set of attributes of a decryptionKey delight the access tree policy combine with a given cipher text, the key can be used to decrypt the cipher text. CPABE is theoretical closer to traditional access control models such as Role-Based Access Control (RBAC), as users' decryption keys are combining with a set of attributes. Hence CP-ABE is more natural to applied, to enforce access control of encrypted data.

Limitations of CP-ABE:-

Despite, basic CP-ABE schemes are still not conclude the enterprise requirements of access control which require considerable flexibleness and efficiency. CP-ABE has drawbacks in specifying policies and controlling user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized reasonably as a single set, so users can only use all possible combinations of attributes in a single set expressed in their keys to delight policies. For attaining complex access control on encrypted data and maintaining confidential-ability, CP-ABE can be used. Encrypted data can be kept confidential even if the storage server is un-trusted; furthermore, our methods are secure against collusion attacks. CP-ABE uses attributes to describe the encrypted data and built policies into user's keys. In other hand CP-ABE, attributes are used to report a user's credentials. Data encryptor determines a policy for who can decrypt. Cipher text Policy Attribute-Set Based Encryption (CPASBE):- As compared to CP-ABE scheme in which the

decryption keys only guide user attributes that are organized logically as a individual set, so users can only use all possible sequence of attributes in a individual set issued in their keys to delight policies.

RSA Algorithm

Key Generation:[6] A user P on random chooses two large distinct primes m, n and computes A = mn and ϕ(A) (m −1)(n − 1). Next, he chooses an integer x such that 1 < x &ltϕ(A) and gcd(x,ϕ(N)) = 1, i.e., x and ϕ(A) are co-prime, and determines dis such that x · dis = 1 (mod ϕ(A)) using the extended full- fledged Euclidean algorithm.

Encryption: Given the public key (x,A) of the user, once an encrypt a message m1 where m1 is a positive integer less than A by computing comp = E(m1,pk) = m1 x (mod A) where c is the cipher text of m1.

Decryption: The user can decrypt[7] the cipher text c with the private key d by computing m1 = D(c,sk) = c dis (mod A).

8. Conclusion and Acknowledgement

Within this paper we have overviewed dissimilar attributes based encryption (ABE) schemes that can be used in cloud systems for malleable, scalable and well grained access control. During ABE scheme, there are together the ‘secret key’ and ‘cipher text’ are linked with a set of attributes. ABE is additional modified into KP-ABE that provides well grained admittance control. Inside KP-ABE, attribute policies are linked with keys and data is linked with the attributes. Keys linked with the strategy that is content by the attributes can decrypt the data. In addition, we have explored CP-ABE and CP-ASBE. The CP-ABE scheme differs from KP-ABE in such a way that in CP-ABE, cipher text is linked with an ‘access tree structure’ and each user ‘secret key’ is rooted with a ‘set of attributes’. Attribute policies are linked with data and attributes are linked with keys and only those keys that the linked attributes convince the policy linked with the data are capable to decrypt the data. HASBE combines the functionalities of HIBE and ASBE. HASBE scheme flawlessly incorporates a hierarchical structure of system users.

We would like to thank our guide Ms. Adlene Ebenezer for helping us to select this topic and making us understand the concepts and also encouraging us to present it as a paper and publish it. We would also like to thank the Editor, the Associate Editor and anonymous reviewers for their valuable comments, which are very helpful for us to enhance our paper.

References

[1] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute based encryption,” IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[2] Ivan Damgård, Thomas P. Jakobsen, JesperBuus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[3]A. Beimel, "Secret-sharing schemes: A survey," in Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao,China, May 30-June 3, 2011. Proceedings, 2011, pp. 11–46.

[4]Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", Journel of Security Engineering, vol.2, 2012.

[5] ChangjiWang1,2,3 and Jianfa Luo1,2 "An EfficientKey-Policy Attribute-Based Encryption Scheme with Constant Cipher text Length" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013.

[6]M. Bellare and P. Rogaway. Optimal asymmetricencryption - how to encrypt with RSA. In Proc. Eurocrypt1994.

[7]Shinde, G.N. and H.S. Fade War,.Faster RSA algorithm fordecryption using Chinese remainder theorem. ICCES,Vol.5,No.4,pp.255-261,2008.

[8] T. Kawno, S. Matsui, T. Yasue, and C. Konno, "Secure Communication Infrastructure for Mobile," in Hitach Review, vol. 48, no. 1, pp. 15-20, 1999.

[9]Prasad Saripalli, and Ben Walters, "QUIRC: a quantitative impactandrisk assessment framework for cloud security," IEEE 2rd InternationalConference on Cloud Computing (2010).

[10] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey,you,getoff of my cloud: exploring information leakage in third-party compute clouds," in Proceedings of the 16th ACM conference on Computer and communications security, 2009.