Secure Access Control For Cloud Data Using Attribute Based Encryption Schemes

Divya Vadlamudi, Sunanda Garlapati, Qhairunnisa Syed, Krishna Kishore Nunna

Abstract— Access Control is a pervasive procedure to shield information from an unapproved client. In many access control frameworks, each data may lawfully be gotten to by a few unique clients. Such a framework is regularly executed by utilizing an authenticated server. The server should be able to store every information with the significant access control Policy. A client would sign in and the server will selectively show the data the client is allowed to access. On the off chance that the server is harmed then the attacker can access all the delicate information. One characteristic answer for the above issue is to implement a cryptographically encrypted access control system, for example, Attribute Based Encryption (ABE). Attribute Based Encryption is envisioned as a basic instrument for keeping an eye on the issue of protected and fine-grained data sharing and access control. ABE has a noteworthy advantage standpoint over the conventional Public Key Cryptography natives as it accomplishes flexible one-to-many encryption rather than one- to-one. The focal point of this work is to discover an approach to make Attribute-based encryption (ABE) more reasonable for access control which we have done using Intelligent Cryptography. Our work includes data distribution algoritms based on sensitivityof data.

Keywords: Attribute Based Encryption, Public Key Cryptography

I. INTRODUCTION

Cloud computing mainly refers to usage of internet and computer technology. The term cloud is a style of computing paradigm where the users can access the resources like data, programs files, third party resources through internet. It is providing the users to utilize the computation, storage and other resources, on demand. The working definition given by National Institute of Standards and Technology(NIST) refers to five features and four deployment models, also three service models.

A.

1. The attributes of cloud computing are:

- On demand service: It is am attribute of cloud computing where it offers the users resources and services on-demand and instantly in many cases without limits.
- Wide Network Access: The data available in private cloud accessible from devices in broad ranges such as tablets, smart phones, PCs etc. The resources can be accessed from broad range of geographic locations which provides online access.

Rapid Elasticity: The most important features that drive cloud forward are scalability and flexibility. The services and platforms offered by the computing cloud should be scaled across various concerns such as geographical location, software configurations, hardware requirements.

Measured Service: Cloud systems are able to control the usage of resources and can be able to optimize them.

Resource Pooling: Using multi-tenant model the CSP's resources are collected to serve multiple consumers according to the different physical and virtual resources they required that are assigned to them dynamically.

Four Deployment models: Public Cloud: The infrastructure provided by cloud is open for use by the public. It is owned by business, academic or any government organization.It is not a trusted one because it is available to everyone. Ex: Microsoft Azure.

Private Cloud: The infrastructure provided by cloud is open for multiple consumers within a single organization. It is owned, managed and operated by the organization and not open for all the users. It is a trusted one as its scope is for only limited users.

Hybrid Cloud: It is an organization of at least two cloud arrangement models(Public and Private mostly).

Community Cloud: The infrastructure provided by cloud is open for use by the multiple consumers within a single organization who have common shared concerns like policy, security requirements etc.

Three service models: SaaS: The consumer have only limited user application configuration settings like using the app through the interface like web based email and is accessible from various client devices. The consumer does not have grip on the infrastructure like servers, OS(operating system), the network and storage.

PaaS: The tools and services provided by CSP are used to deploy the application on cloud by using programming languages, libraries. The consumer has control over the application hosting environment and some software configuration settings but doesn't have control over underlying infrastructure like network and storage.

Revised Version Manuscript Received on April 05, 2019.

Divya Vadlamudi, CSE Department, KLUniversity, Vijayawada, AP, India (e-mail: divya.movva@kluniversity.in)
Sunanda Garlapati, CSE Department, KLUniversity, Vijayawada, AP, India (e-mail: sunandagarla- pati612@gmail.com)
Qhairunnisa Syed, CSE Department, KLUniversity, Vijayawada, AP, India (e-mail: qhairunnisa.syed@gmail.com)
Krishna Kishore Nunna, CSE Department, KLUniversity, Vijayawada, AP, India (e-mail: krishnakishorenunna1018@gmail.com)

IaaS: The consumer have control over hosting environment and can be able to deploy applications and run the software. Also the capabilities of consumers include control over operating systems and software and limited control of networking components.

Encryption Used: Clients can transfer their information into the distributed storage framework and this framework not just supports secure and strong information and recovery, yet in addition enables a client to forward his information in the capacity servers to another client without recovering back the information . This makes the ownership information unused and secured at the time of retrieval.The long term storage services over the internet are provided by the archie-tecture of cloud storage which is collection of storage servers having higher end configuration.The cloud environment is a distributed computing over a network. In this condition an untrusted servers, for example, the cloud server, numerous applications require components for complexaccess-command over encrypted information .This issue is tended to as the idea of ABE. ABE is another public key based one to many encryption that empowers get to command over encrypted information utilizing access approaches and credited attributes related with private keys and ciphertexts. There are many sorts of ABE plans but only two are important.The policies are Keybased(KP-ABE) and, next Ciphertext Based (CP-ABE). In a KP-ABE plot empowers senders to encode messages under an arrangement of private keys and attributes which deals with access policies that indicate which encrypted text the person authorized to access will be permitted to decode. The security property of the ABE plot with re- appropriated decoding ensures that an enemy (counting the pernicious cloud server) be not ready to master anything about the encoded message and gives of the accuracy of the change done by the cloud server. Anyway in such framework the transformation key is visible to the customers. In the state that, the outsider distinguishes the transformation key K at that point there is a probability of known the data. With the end goal to stay away from such circumstance our plan proposes the triple DES idea with the end goal to scramble the key.

II. LITERATURE SURVEY

First way to guarantee the controlled access is, restructure access control problem into key management. In the literature, there exists many Attribute Based Encryption(ABE) schemes[1][2][3][4] which have been made based on the key. Even though there are several limitations related to these schemes. The most illogical issue is the point at which the clients get to authorization is revoked, all the keys known to this client and furthermore the general population esteems identified with those keys ought to be changed. Another approach is to follow either of the access control methods mentioned in [5]. Many systems depend on Role Based Access Control (RBAC) for access to the resources stored by third party like web servers and cloud providers. They use either their own access control strategy which is then translated and acknowledged by distributed computing or utilize cryptographic solutions to encrypt data to allow only authorized users[6][7][8]. Similarly for access control, there are similar schemes such as Single Sign-On systems Kerberos, OpenID[9] and OAuth 2.0[10]. Kerberos had been used widely for controlling access to network resources. Ticket Granting Service(TGS) in a Kerberos system provides ticket to the authenticated user to access the resource. The resource and the TGS have to share either some common secret or belong to same domain. [11] shown is a broad framework for monitoring access control and increasing the efficiency on computational resources. This framework provides fine-grained and history based access controller. When the users credentials are not sufficient to execute the application the framework presented in[12] creates a session to interact with the user in order to establish enough trust needed to execute the resource. In [13] Mansura and Aslam proposed a permission based user access control management scheme. The overall structure was designed and different techniques for authorization, authentication and identification was developed to multiply efficiency of cloud security. The security and efficiency analysis was performed. At every stage the verification of information will be performed which improves the security to the great extent.

III. EXISTING SCHEMES

A.

Attribute based encryption: Sahai and Waters first presented the attribute based encryption for implemented access control through public key cryptography. The primary objective for these algorithmic is to give secure and access control. The basic perspectives are to give flexibility, adaptability and fine grained access control. In conventional model, this can be done exactly when client(user) and server are in coherence in space . Be that as it may, imagine a scenario where their spaces are not trusted or not same. Thus, the new access control plot came into existence which is Attribute Based Encryption .This plan was presented comprising of of key strategy property based encryption. As contrasted and traditional model, KP-ABE given fine grained access control. Anyway it comes up short as for adaptability and versatility when experts at various dimensions are considered. In ABE both the client secret key and the ciphertext are related with a list of features. A client can decode the figure content if and just if no less than an edge number of characterstics cover among the encoded text and client secret key. Not the same as customary open key cryptography, for example, ID Based Encryption, ABE is actualized for one-to many encryption where cipher text is not really encoded to one specific client, it might be for number of clients. In ABE scheme,which was proposed by Sahai and Waters the threshold semantics are not exceptionally expressive to be utilized for planning more broad access con- trol framework. ABE in which approaches are determined and implemented in the encryption calculation itself.Key Policy Attribute Based Encryption(KP-ABE) : To enhance and to give wide access control, Goyal, Pandey, Sahai, and Waters proposed a KP-ABE scheme. It is ta form

of traditional model of ABE. Investigating KPABE plan, data is related with attributes and attribute policies are related with keys. The keys just connected with the policy that will be satisfied by the characteristics that can decode the information. KP-ABE is an open(public) key encryption system that is proposed for one-to-numerous correspondences. In this plan, data is related with the characteristics that an (public) key is characterized for each. Encrypter, that is who encrypts the information, is related with the structure of characteristics to the databy encoding it with an public key. Clients are given an entrance tree structure over the information attributes. The nodes of the entrance tree are the threshold entryways. The leaf nodes are related with attributes. The mystery key of the client is depicted to mirror the entrance tree structure. Thus, the client can decipher the information that is a ciphertext if and just if the information qualities fulfill the entry tree structure.In KP-ABE, a course of action of traits is connected with ciphertext and the customer's unscrambling key is connected with a monotonic access tree structure. Right when the traits related with the ciphertext satisfy the passage tree structure, by then the customer can disentangle the ciphertext.In the distributed computing for proficient renouncement, an access control component dependent on KP-ABE and a re-encryption procedure utilized together. To decrease the major-ity of the computational overhead to the servers is enabled to the data owner. The KP-ABE plan gives access control which is finegrained. Each record or message is encoded using symmetric data encryption key, which is encoded by a public key, that is relating to an arrangement of attributes in KP-ABE, which is produced comparing to an access tree structure. The encoded information document is put away with the relating characteristics and the encoded DEK. if the characteristics of file in cloud fulfil the access structure of users key, then the client can decode the encrypted DEK. That can be utilized to decode the record or message.

KPABE scheme comprises of the accompanying 4 calculations:

Setup : This estimation takes as data a security parameter κ and reestablishes open key PK and an master secret key MK. For encryption Public key(PK) is used by senders . Master Key is used for creation of customer puzzle keys and is familar only to the owner.

Encryption : This calculation uses a message M,and also the public key PK, an arrangement of attributes as input. It yields the ciphertext E.

Key Generation : This count takes as info an entrance structure T and the master key MK. It yields a secret key that engages the customer to interpret a message encrypted under a course of action of attributes if and just if matches T.

Decryption : This step uses as input the mystery key of client which satisfies structure of access and the encoded text E, which was encoded according to the set of characterstics . If the set of characterstics fulfills the access policy , step yields original message M.

Restrictions of KP-ABE: Encryptor can't choose who can decode the encoded information. It can just pick descrip-tive attributes for the information, and must choose the option to trust the key issuer. KPABE isn't normally appropriate to specific applications. For instance, modern communicated encryption, where clients are portrayed by different characteristics and in this, the one whose characteristics coordinate an arrangement related with a ciphertext, that users can decrypt the decoded text. KPABE plot bears client mystery key responsibility. It is giving fine grained access yet has no adaptability and scalability.

Expressive Key Policy Attribute Based Encryption: In KP-ABE, empowers the one who sends to encode messages with an set of characterstics called attributes and private keys are in related with tree structure of acces control. Only the Access tree structure can determine which encoded texts the key holder is permitted to decode. The non-monotonic access structures are taken into consideration for this type of ABE. Those structure contain discredited attributes and with steady ciphertext size. This is more proficient than KP-ABE.

Cipher Text Policy Attribute Based Encryption: Cipher Text Policy Attribute Based Encryption: Sahai et al. displayed the possibility of another adjusted kind of ABE called CP-ABE that is Ciphertext Policy Attribute Based Encryption. In CP-ABE plot, property approaches are connected with information and traits are connected with keys and simply those keys that the related characteristics satisfy the game plan related with the information can disentangle the data CP-ABE works in the switch method for KP-ABE. In the ABE plot the one which uses ciphertext i.e; CPABE the ciphertext is related with an tree structure of access control and every client secret key is inserted with an arrangement of attributes. In ABE, having KP-ABE and CP-ABE, the owner runs the calculation Setup and Key Generation to create framework MK, PK, and client secret keys. Just recognised clients (i.e., clients with expected access structures) can decode by calling the algorithm Decryption. In CP-ABE, every client is related with an arrangement of attributes His secret key is produced dependent on his attributes. While encoding the data, the person who encrypts the data determines the threshold structure of access for his own characterstics. This message is then encoded dependent on this access structure with the end goal that just those whose attributes fulfill the structure of access can decode it. By using CP ABE procedure, encoded. information can be kept private and secure against collusion attacks.

CP-ABE plot comprises of following four calculations:

Setup : The calculation uses information a secure parameter κ and restores people in general key PK and also a framework ace mystery key. PK which is utilized by senders of the data for encoding. MK is utilized to create client secret keys and so it is familar only to the owner.

Encryption : This calculation takes a message M, access structure T and public parameter PK. It yields the ciphertext CT.

Key-Gen : This calculation uses as info an arrangement of attributes related to client and the master secret key MK. It yields a secret key which engages the customer to translate a message encoded under an tree structure of access control T if and just if suits T. Decryption : This calculation takes decoded text CT and a secret key SK as an input for a attribute

set. It restores the message M if and just if fulfills the structure of access control related with the encoded text.

CPABE rests on on how characteristics and strategy are related with cipher text and clients' decoding keys. CPABE plan, a cipher text is connected with a tree access structure and a customer's decoding key is connected with different set of combinations.In this plan, the jobs of cipher texts and decryption keys are exchanged as same as in KP-ABE. Here cipher text is encoded with an access tree approach picked by an person who encrypts. What's more, the relating decoding key is made concerning an arrangement of attributes. As the arrangement of attributes of an decryption key fulfill the access tree approach related with a given encoded text and the key can be utilized to decode the cipher text. CPABE is thoughtfully closer customary access control models, for example, Role-Based Access Control (RBAC) as clients' decryption keys are related with an arrangement of attributes. Henceforth, CP-ABE is more normal to apply rather than KP-ABE, to uphold access control of encoded information.

Restrictions of CPABE: Nonetheless, essential CP-ABE schemes are not satisfying the venture necessities of access control which require significant adaptability and profi-ciency. It has constraints in determining strategies and managing client characterstics. In CP_ABE conspire, decoding keys just help client properties that are composed intelligently as a one, so clients can just utilize every conceivable mix of attributes in a single set given in their keys to fulfill policies. For acknowledging complex access control on encrypted information and keeping up secret capacity, CP-ABE can be utilized. Encoded information can be kept private regardless of whether the capacity server is un-trusted; additionally, our strategies are secure against collusion attacks. KP-ABE utilizes attributes to depict the encoded information

and incorporated policies with client's keys. In other hand CP-ABE, attributes are utilized to portray a client's certifications. Information encryptor decides an arrangement for who can decode.

Ciphertext Policy Attribute-Set Based Encryption (CPASBE): When contrasted with CP-ABE scheme in which the decryption keys just help client characterstics that are sorted out logically as a single

set,so customers can simply use in a single set each combination of attributes issued in their keys to satisfy arrangements.To take care of this issue, ciphertext-policy attribute-setbased encryption (CP- ASBE or ASBE for short) is presented by Bobba, Waters et al . ASBE is an all-extended type of CPABE which sorts out client attributes into a recursive set structure. Ciphertext Policy Attribute Set Based Encryption (CP- ASBE) is a changed type of CP-ABE. It contrasts from existing CP-ABE designs that address the customer attributes. It arranges client attributes into a recursive set based structure and empowers customers to compel dynamic impediments on how those attributes may be joined to fulfill an approach.

The CP-ASBE comprises of recursive arrangement of at-tributes. The attractive component and the recursive key structure is actualized by four calculations, Setup, KeyGen, Encrypt, and Decrypt:

Setup: Consider the depth of key.Uses info a depth 'd'. It yields a secret master key MK and a public key PK.

Key-gen: It takes the identity of client u, a key structure A and the master secret key MK as input. By using this yields a secret key SK for client u.

Encrypt: Takes as information a message M, access tree T and a public key PK. It yields a ciphertext CT.

Decrypt: For user it takes ciphertext CT and secret key SK as data. It yields a message m .

On the off chance that the key structure A related with the secret key SK, fulfills the access tree T, related with the ciphertext CT, at that point m is the first right message M. Something else, m is invalid.Particularly CP-ASBE per-mits Client attributes are composed into a recursive group of sets and Allowing attributes to join from different sets. Subsequently, by gathering client characteristics into sets and no confinement on how they can be consolidated, CPASBE can bear characterstics. Greater adaptability and fine grained access is given by CPASBE. Basically, various assignments which are numerical for a given attributes can be made by setting each task in an alternate set and placing it into a single set.

Restrictions of CP-ASBE: The test in building a CPASBE plan is in specifically enabling clients to join attributes from numerous sets inside a given key. Then There is test of keeping clients of consolidating properties from various keys.

TABLE I COMPARISON TABLE FOR ABE'S

Algorithm	Limitation	Efficiency	Data Confi-dential-ity	Computation overhead	Scalability
KP-ABE	It cannot decide who can decrypt the data	Low	High	Low	No
Expressive KP-ABE	In suf-ficient and complex	High	High	More	No
CP-ABE	Decrypt key only support user attribute that are orga-nized logically	Average	High	Average	Yes
CP-ASBE	Each au-thority attribute set should be disjoint	High	High	More	Yes
IBE	Unsuitable to im-plement	Low	High	More	No

PROPOSED SCHEME & RESULT

Based on security they want to their data,the priority is given to the user and also instead of giving same security for all, and providing more security for confidential data, its decreases the overhead and improve efficiency. One such method is discussed below.

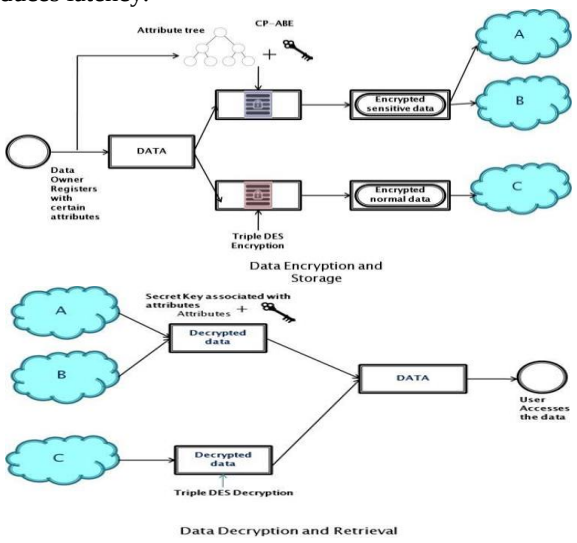
Named data packets- These are searchable labelled data packets made from the data by the data owners and CSPs.

Pre-stored∃ Name∈ List (PNL)- It contains all labels of sen-sitive data.

CP-ABE- Cipher Policy Attribute based encryption.

Both the data owner and user needs to register themselves in a registration portal. They further login through their respective portals to upload and access the data.The data owner will take Named Data Packets and Pre-stored Name List as requirements and data is stored in the cloud as input. The data is said to be sensitive data when the label if there exists a label in Pre-stored name list (PNL) that is present in Named Data Packets (NDP). If the given input data contains Sensitive data, we apply any of the Cipher Policy Attribute based encryption scheme on it else simply we perform simple triple DES operation on the normal data (the part which is not sensitive). For retrieval, the client needs to send demand to the owner of the data. The owner of the data would get another access request for which he creates a secret key and sends it to the client who requests for the data.

The user now accesses the decrypted data using the secret key. Thus this ensures access control along with security and reduces latency.



A.

11) *Algorithm:* Input: NDP, PNL

1. For all NDP do
2. For each data packet do
3. if a Li PNL then
4. Execute CP-ABE Algorithm
5. Generate α
6. else
7. Execute Triple DES encryption Algorithm Generate β
8. end if
9. end for
10. end for
11. Obtain Values of D after decryption *α, β

are the encoded data.

The encoding-decoding process for triple DES is as following

1. Encode the plaintext blocks using single DES with key K1.
2. Now decrypt the output of stage 1 using single DES with key K2.
3. Finally, encrypt the output of stage 2 using single DES with key K3.
4. The output of stage 3 is the cipher text.
5. Decryption of a cipher text is a transform methodology. Customer at first translates using K3, by then encodes with K2, ultimately decodes with K1.

CONCLUSION

One of the primary disadvantage of ABE scheme is that decoding is expensive for resource-limited devices because of matching activities, and the quantity of blending tasks required to decode a ciphertext develops with the complexity of the access approach. As of late proposed framework wipes out this issue by presenting the thought of Intelligent cryptography which is a combination of ABE and triple DES with re- appropriated decoding, which to a great extent disposes of the decryptionoverhead.

REFERENCES

1. A Survey on Access Control Models in Cloud Comput- ing RajaniKanth Aluvalu1 and Lakshmi Muddana2 Department of Computer Engineering, RK University Rajkot, India.
2. S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," ACM Trans. Comput. Syst., vol. 1, no. 3, pp. 239–248, 1983.
3. M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in Proc.ACM Conf. Comput. Commun. Sec., Nov. 2005, pp. 190–202.
4. H. R. Hassen, A. Bouabdallah, H. Bettahar, and Y.Challal, "Key management for content access control in a hierarchy," Comput. Netw., vol. 51, no. 11, pp. 3197–3219,6 2007.
5. A Review On Different Access Control Mechanism In Cloud Environment
6. ZhouL,VaradharajanV,HitchensM(2011)Enforcing role-based access control for secure data storage in the cloud.ComputJ.
7. YuS,WangC,RenK,LouW(2010)Achieving secure ,scal -able, and fine-grained data access control in cloud computing
8. LiJ,ZhaoG, ChenX, XieD, RongC, LiW, TangL, TangY(2010) Fine-grained data access control systems with user accountability in cloudcomputing.
9. RecordonD ,ReedD(2006) OpenID2.0: aplatform for user-centric identitymanagement.
10. Fine-grained and History-based Access Control with Trust Management for Autonomic Grid Services *
11. TheOAuth2.0authorizationframework.RFC6749. https:// tools.ietf.org/html/rfc6749
12. Access Control Management for Cloud Mansura Habiba Department of Computer Science, Ameri- can International University Bangladesh, Dhaka, Bangladesh.
13. A New Approach to Access Control in Cloud Mansura Habiba1 • Md. Ra?qul Islam2 • A. B. M. Shawkat Ali3 • Md. Zahidul Isla

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication