TB-ASBE: Secure Key Agreement for Data Access Control Using Tree Based Attribute-set-based Encryption

Kaushiki Upadhyaya
Computer Engineering
Vidyalankar institute of technology
Wadala, Mumbai, Maharashtra
kaushikiupadhyaya@gmail.com

Prof .Umesh kulkarani
Computer Engineering
Vidyalankar institute of technology
Wadala, Mumbai Maharashtra
Umesh.kulkarani@vit.edu.in

Abstract— Cloud computing proliferation is immense and so the need for its security of highest importance. Amongst its various service model PAAS (platform as a service), IAAS (infrastructure as a service) and SAAS (software as a service), SAAS is the one most susceptible to security and privacy breaches. As Hybrid and community deployment models are the most popular ,we present access control using TB-ASBE (Tree Based attribute set based encryption) that is flexible with multi assignment for a particular attribute and highly scalable for fine grained access control for a SAAS model deployed on a community or hybrid cloud. It overcomes all the limitations of existing Encryption Techniques and access control policies. It Al

Keywords—*Cloud security,Attribute set based encryption, Access control policy*

*****

I. Introduction

Cloud computing is a new paradigm that builds a parallel , virtual ,distributed computing, utility computing and service oriented architecture. We are migrating from information age to participation age.We are participating on the net not just viewing stuff, we build the infrastructure and use the services..

Now days cloud computing is emerged service, the cloud computing providing lot of benefits include the cost and capital expenditures, increased operational efficiencies, scalability and flexibility so on. Attributes of cloud are broad network access that is availability across the world that is being ubiquitous ,rapid elasticity that is optimal scalability what we simply need is a device that can support the middleware needed for cloud, measured service: Pay as you go ,on-demand ,resource pooling i.e. multitenant user scenario.eg bank1 and bank2 want to procure a cloud then the end user would be their employee ,tenant would be bank1 or bank 2 and configuration would be according to the tenant. Cloud provides three types of service models [1] SAAS e.g. CRM, email, PAAS e.g. middleware, Database, build/dev/test), IAAS e.g. virtual server, unlimited storage, high speed bandwidth. There is a tremendous growth in SAAS, with its market size estimated to be over 80% of the global public cloud market. We are providing security on SAAS which is built on PAAS. Cloud also provides various deployment models like: Public, Private, and Hybrid which is a combination of public and private cloud, Community cloud. We are going to provide security for hybrid cloud (scalability of public and security of private) or community cloud e.g. GoGrid, Amazon VPC. Based on this services IT industry will get fine state on art technology. The hardware/software maintenances should be very easy to state. That plays a major role in cost management for Infrastructure and human resources.

Although there are great benefits brought by cloud computing paradigm are exciting for, academic researchers, IT companies and potential cloud users, security problems pose a serious obstacle, which without being appropriately addressed, will prevent cloud computing extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in cloud computing [2] due to its Internet-based data storage. The security for the cloud data, user access limits and authorization services have to be managed properly. Data audit ability is managed by providing a trusted third party for managing certificates and authorizing for system security accountability. The major construct of our work will provide securable data with specific access control, along with authentication and maintain the data security. To provide security there are several other encryption and access control techniques, the majority of the work will be on attribute based encryption and access control solutions. IN our paper we have proposed the Tree Based Attribute Set Based Encryption (TB-ASBE). The TB-ASBE is highly scalable and flexible. It removes the coarse graded structure and inculcates fine grade access control.

A *Attribute Based Encryption*

The PKI system [3] required the user to always communicate with the PKI system before any communication and every time re-encryption of data was needed by a user, a new pair of keys was generated, so whenever scalability was required key management became an issue.

Then came the IBE identity based encryption [4], in identity based encryption arbitrary string can be used to make identity (e.g. email address) and security is tied to authenticating users before providing them there private key. In IBE different identities of a user in different situations was not considered.

Role-based access control [5] (RBAC) was incompetent in delegation aspect. The Attribute-based encryption was first proposed by Amit Sahai and Brent Waters [6] . It is a public-key encryption mechanism in which the secret key of a user and the ciphertext are associated with attributes. The decryption of a ciphertext is only possible if the attributes of the user key matches that of the ciphertext. Main concern for security in Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys can access the data only if any one of his key grants is successful.ABE is of two types: KP-ABE and CP-ABE.

In KP-ABE[7][8]the main features of construction are: access formula are encoded with a linear secret sharing scheme, the share of the secret is tied to the attributes and the presence of attribute in cipher text is achieved through an element H_i raised to random exponent .Here collusion is prevented by injecting a personalized randomness factor $R_{i.}$ The problem with this was that the encryptor does not know who can decrypt the data except relying in the key issuer. It is not a suitable scheme for many real life situations and moreover secret sharing scheme is limited to expressing monotonic key access

In CP-ABE[9][10] the access policy is associated with the cipher text and the attributes are associated with an access structure and then current CP-ABE schemes can only support user attributes that are organized logically in a single set; i.e., users can use all possible combinations of attributes issued in their keys to satisfy various policies. This imposes some undesirable restrictions. First, it becomes very difficult to manage “compound attributes” and second specifying policies using them. For example, attributes that combine a lecturer role with short-term responsibilities like food committee for some event result in useful compound attributes.

So CP-Attribute Set based Encryption came into role. Form of CP-ABE, that addresses the above limitations of CP-ABE by introducing attributes in a recursive set based structure, which are associated with user keys. Specifically CP-ASBE [11] allows, 1) user attributes are organized into a recursive family of sets and 2) access policies that can restrict users to decrypt if they use attributes from within a single set or cross domain attribute mix-matching is not allowed. TB-ASBE works on the principle of CP-ASBE .Thus, by grouping user attributes into sets have no restrictions on their combination and can support compound attributes without sacrificing the flexibility to easily specify policies. Our TB-ASBE set based encryption along with access tree structure in supporting compound attribute and multi-value assignments.

A. Access Control

Access control systems help facilitate the process of granting differential access right for different set of users.eg: giving the administrator more rights than that of other users using an operating system is an example.

The administrator can set access rights for a user while making it, same is our system the domain authority acts as the administrator and assigns the access structure for a user, giving the user the authority to make his own private key i.e. password of a user account in our anomaly. So Access control basically relies on some check to ensure that the data accessed by a particular user is available to it, only if he is authorized for it. Many techniques rely on hierarchies and a common secret key within a hierarchy. The data is then classified according to hierarchy and encrypted by the private key assigned for the hierarchy. There are mainly two types of attribute based encryption mechanism KP-ACP, here data is encrypted with a symmetric data encryption key ,then the key is encrypted by a public key corresponding to a set of attribute following a certain access structure for a particular user. So the data is stored in the cloud in the encrypted form with a set of attribute if the users key access structure or policy matches the attribute for a particular user he can decrypt the data. We are developing a much richer type of attribute-based encryption structure where the private keys of different users are associated with different access structure

II. SYSTEM MODEL

A. System model

As depicted in Fig.1, our system consists of the below mentioned entities that work in synchronization to provide secure and private data storage and retrieval.

- The cloud service provider manages the cloud as the private data storage service.
- Data owners encrypt the files and store them in the cloud for sharing with data consumers.
- Data consumers access the files and download the encrypted files and decrypt the files. The Data owner/consumer is administrated by the domain authority.
- The trusted authority is the root authority and responsible for managing the domain authorities.

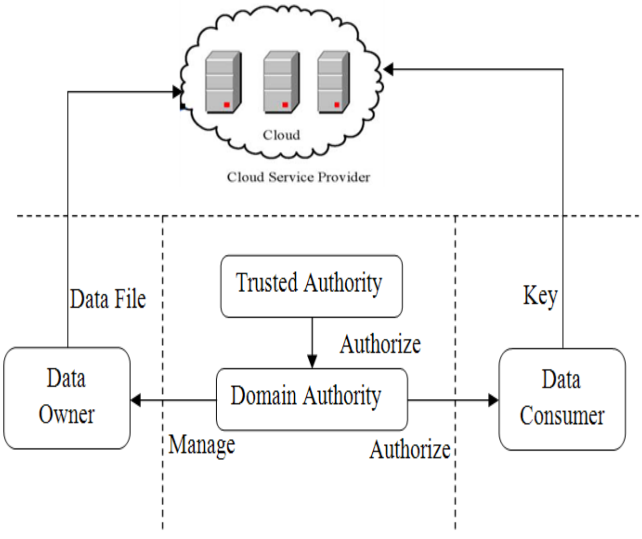

Fig1.System Architecture

B.Mathematical model

Bilinear Maps: Let G1, G2, GT be cyclic (multiplicative) groups of order p, where p is a prime.

Let g_p be a generator of G1, and g_q be a generator of G2.

Then e: G1 × G2 → GT is a bilinear map if and only if it has the following properties:

1.Bilinearity: $e(g_p, g_q) = e(g^q, g^p) = e(g, g)^{qp} = 1$
$e(g_p, g_p^x \cdot g_q^y) = e(g_p, g_{ap})x$

It state that the groups have orthogonal mapping .i.e. if we have a dirty element which has a portion of it in both the groups. This represents something in one group and something other in the next group and if we try to pair it with any element in any of the groups by bilinearity the extra element y gets dissipated.

2. Non-degeneracy: G is called a bilinear group if the group operation and the bilinear map e can be efficiently computed

III. OUR CONSTRUCTION

Secure communication can only happen when data that is being exchanged within a cloud should be encrypted, calls to the remote server should be examined for imbibed malware .our focus here is encryption and authenticity before giving access controls. For encryption we are using a DES symmetric algorithm and for authenticity a shared public key certificate using RSA.A certification process is used to bind individuals to their public keys as used in public key cryptography where a CA (certificate authority) verifies a person's identity. The certifying agent signs the certificate using his own private key. The certificates are then send to a repository.

Then comes our TCB (trusted computing base) or our TTP (trusted third party) is a total combination of a protection mechanism within a system. It is a collection of Software and firmware that are trusted to enforce a security policy of a computing system. It ensures that the processes from one domain do not access memory location of another domain. The TTP stores all cryptographic keys but do not know what the key is as the keys are present in a encrypted manner. This key which is generated by the TTP is called the secret key (symmetric) and used for encryption and decryption.

Key Structure: In our TB-ASBE an access structure is associated with the ciphertext. Users with decryption key value equal to the attributes embedded in their key tree structure. If satisfy the access structure associated with the cipher text then only he can decrypt the cipher text.

e.g. The following is an example of a company name ABC, where a user named U1 is a lead in project 1 and a manager in Project 2.the manager has access to all three levels of data as the company policy i.e. L1, L2, L3.So as a manager in project 2 he has access to all the three levels of data whereas in project 1 he has only level L2, L3 data. So his key structure of user U1 would comprise of three subsets {A0, A1, A2} each level is identified as a unique label index i. where 1 ≤ i ≤ n. n is the no of sets at a particular level as in [].So when a user is trying to satisfy a policy ,he may only use attribute elements within a set but cannot combine across the sets.

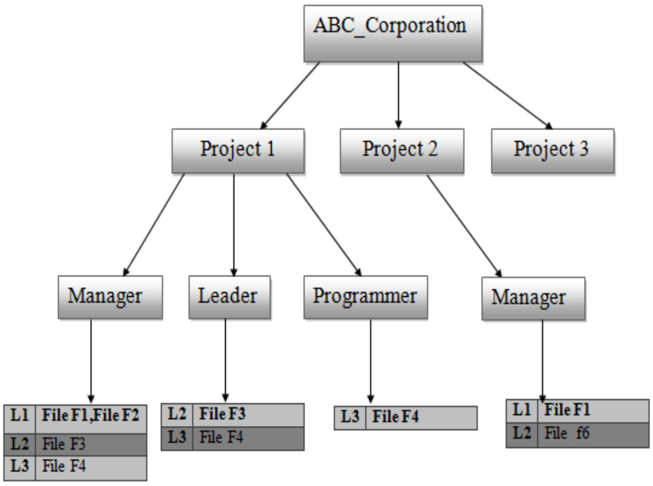

Fig2. System model example

Access policy : we are using the same scheme used in [11] for the access structure defined for a data. the leaf nodes will represent the attributes and the non leaf nodes represent the threshold gates like AND an OR in our case the threshold values being 1 and 2. because of this the non monotonic access structure limitation of adding the not gate. the access policy described in fig 3 address that the data or files at level l1 and l2 can only be accessed by a user, who is either a manager or lead. Access policies can combine attributes within a domain only that is intra domain possible and .inter domain not possible

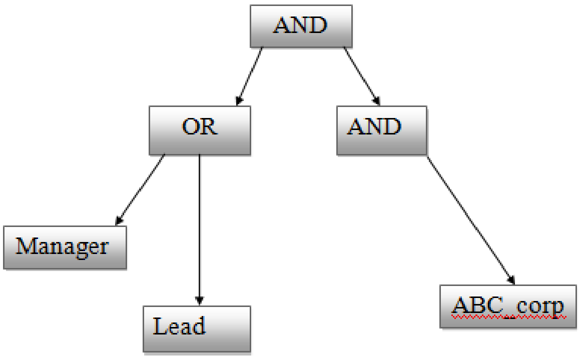

fig 3.access structure

IV. IMPLEMENTATION

We have implemented TB-ASBE based on CP-ASBE [11][10] and HASBE [12] which uses the pairing based cryptography. The experiment is conducted on the laptop with intel core i3 with 1.80 GHz processor with up to 4GB RAM running windows 8.1.we have made use of the java build libraries security and crypto for using DES symmetric algorithm and various other build in security features .

Our implementation is based on the following algorithm

Algorithm:

1)***Setup(d):*** The input parameter to this primitive are the depth parameter d which is the depth of the key structure, which is defined on the basis of bilinear maps which is symmetric having k's value range from 1 to d. Its outputs a public key PK.

2) ***CreateDomain(*****PK,A*)*:takes as input the parameter public key pk and recursive attribute set $A=\{A_0\ A_1\ A_2 \ldots A_N\}$where $A_m=\{A_{m,1}, A_{m,2}, A_{m,3} \ldots A_{m,n}\}$where m being the m^{th} element in the set and n being the no of attributes. when a new domain authority i.e DA_i wants to join the system the TTP will first verify if it is a valid domain and then call function ***CreateDomain***( ).

3) ***CreateUser* (*DA*$_i$*, U, A*)*:*** takes as input the domain in which it has to be created, identity of the user as u and a key structure a. it outputs a secret key SK_u for user u.

4) New file creation: to protect data stored on cloud the data owner first encrypts the data file for this the steps are:

1. Pick a unique id for this data file.
2. Randomly uses a data encryption key k, and encrypt the data file using DES.
3. Define a tree access structure t for the file and encrypt using ***Encrypt* (*PK, M, T*)*: this primitive take as input public key PK, the message **M** and the access tree structure **T**. It outputs a cipher text **CT**.*

5) ***Decrypt (CT, SKu):*** when the user sends request for a data file, the cloud sends the corresponding cipher text back .The user decrypts by calling the function *Decrypt(**CT,SKu**)*..Take as input a cipher text CT and secret key SK_u for user *u* .it outputs a message M. If the key structure A associated with the key structure $\boldsymbol{SK_u}$ satisfies the access tree *T,* associated with ciphertext *CT*, then *m is* the original correct message *M*, otherwise *M* is null.

V. CONCLUSION

Security increases data protection and access management makes cloud capable to evolve and respond to ever changing needs of cloud. In our Paper the TB-ASBE algorithm uses authenticity mechanism and Authorization that support multivalve assignment of attribute without compromising the security at any level.

REFERENCES

[1] Ling Leng, Lin Wang :Research on cloud computing and key technologies,2012 International Conference on Computer Science and Information Processing (CSIP).

[2] Wentao Liu :Research on Cloud Computing Security Problem and Strategy,2012 IEEE

[3] The Public Key Infrastructure Approach Security https://docs.oracle,.com /cd/B10501_01/network.920/a96582/pki.htm

[4] Dan Boneh, Matthew Franklin :Identity-Based Encryption from the Weil Pairing, Appears in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003. An extended abstract of this paper appears in the Proceedings of Crypto 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229, Springer-Verlag, 2001.

[5] D.F. Ferraiolo and D.R. Kuhn (1992) "Role Based Access Control" 15th National Computer Security Conf. Oct 13-16, 1992, pp. 554-563 the original paper that evolved into the NIST RBAC mode

[6] R.Manjusha,Research Scholar, R.Ramachandran: Comparative Study of Attribute Based Encryption Techniques in Cloud Computing ,Internnatio -nal Conference on Embedded Systems - (ICES 2014)

[7] Shuaishuai Zhu, Xiaoyuan Yang, XuGuang Wu :Secure Cloud File System with Attribute based Encryption, 2013 5th International Conference on Intelligent Networking and Collaborative Systems

[8] Chang-Ji Wang , Jian-Fa Luo :A Key-policy Attribute-based Encryption Scheme with Constant Size Cipher text, IEEE nov 2012

[9] Changji Wang and Jianfa Luo:An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length, Mathematical Problems in Engineering Volume 2013 (2013), Article ID 810969

[10] Xingbing Fu and Zufeng Wu:Ciphertext Policy Attribute Based Encryption withImmediate Attribute Revocation for Fine-Grained Access Control in Cloud Storage ,IEEE 2013

[11] John Bethencourt, Amit Sahai, Brent Waters :Ciphertext-Policy AttributeBasedEncryption,https://www.cs.utexas.edu/~bwaters/publications/papers/cp-abe Bobba, Himanshu Khurana and Manoj Prabhakaran

[12] ,Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based EncryptionRakesh,University of Illinois at Urbana-Champaign {rbobba,hkhurana,mmp}@illinois.edu,July 27, 2009.

[13] Zhiguo Wan ; Key Lab. for Inf. Syst. Security, Tsinghua Univ., Beijing, China ; Jun'e Liu ; Deng, R.H.,HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing.