ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

ML-ASBE: Security for Controlling the Access of Data through Multiple Levels Attribute-set-based Encryption

Prof. Asha Durafe[1], Rohan Shrivastava[2]

Professor, Department of Electronics Engineering, Shah and Anchor Kuttchi Engineering College, Chembur, Mumbai, Maharashtra, India

PG Student, Department of Electronics Engineering, Shah and Anchor Kuttchi Engineering College, Chembur, Mumbai, Maharashtra, India

ABSTRACT:The applications of cloud computing is immense and therefore it becomes very important to ensure that there should be no loop holes in this technology. The scope and access of cloud computing to user's data is limitless due to which it becomes a compulsion to ensure that no security breach occurs. The client data must not be compromised at any cost. Amongst the different services provided by the cloud such as SAAS, PAAS and IAAS, SAAS (software as a service) is most vulnerable to security breaches. As we know that there are various deployment model of cloud such as public, private, hybrid and community model. But among them hybrid and community models are very popular. So here we are going o propose a security system based on ML-ASBE for hybrid and community models. ML-ASBE is to provide the access control which is both flexible and scalable. Our system will enhance the expressing capability by combining the attributes in a controlled manner. This will be able to overcome the drawbacks of old encryption based systems and control policies.

KEYWORDS:Cloud security, Attribute set based encryption, Access control policy

I. INTRODUCTION

We are currently visualizing a new era of technology that is dominated by the cloud computing technology. This technology is a combination of various already existing technologies [1]such as virtualization. Currently most of the industries are moving towards the cloud based architecture. IT industries are majorly participating in this migration which means millions and trillions of data is getting migrated on cloud.

Cloud computing is growing day by day due to a number of advantages it provides to the client. Apart from being cost effective it is efficient, scalable and flexible. If an industry is using the cloud services then they need not to bother about the infrastructure maintenance. This is a huge benefit of using this. The concept of cloud can be understood by taking a simple example. If you want to use a car there are two ways of getting it. In one way you can purchase the car and use its facilities. If you are purchasing the car you need to look after the maintenance of it and even after the use you need to beer the take care of the car. On the other hand second way is to rent a car whenever you need it. In this option you need not to pay for the maintenance of the car and you need not to worry about it. You can just pay and use for a specific period. After the use you will leave the car and some other user will take it. Cloud can be compared with the same rented car. In cloud also the client pay for the period during which it is having the use of cloud. This is known as pay-as-you-go feature of cloud. In the recent times there is a spectacular growth in the SAAS service of cloud. It is estimated that more than 80% of public cloud market is captured by SAAS cloud services. As we have mentioned that cloud brings with it a number of advantages that attracts the client but along with it also raises a security concern [2]. The data confidentiality is always compromised if cloud is applied. Security has become a major roadblock in the growth of cloud computing technology. We are here building a security system for the SAAS. Cloud service providers

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

are providing services in three different deployment models which are public, private and hybrid cloud. Hybrid cloud is the combination of public and private cloud. Apart from these models there is a community model which needs scalability and flexibility. Our system is to provide the security to the hybrid cloud. Our model will give the security to the data along with maintaining the flexibility and scalability of the system. Our system is third party software that will take care of the security the client. So this system will come into picture before sending the data to the cloud and after receiving the data from the cloud. It is like a double security that is managed at the client end. Here the data is encrypted and then stored on cloud so that even if some security breach occurs the data is not compromised. In the past a number of methods for this encryption have been used but all of them were having some drawbacks[3][4[5]. In our proposed model we have overcome most of the drawbacks to make the system scalable and flexible. In our paper we are proposing multiple level attribute set based encryption (ML-ASBE). This helps us to provide a fine grained access control to the system.

II. RELATED WORK

Sometimes an image may contain text embedded on to it.Detecting and recognizing these characters can be very important, and removing these is important in the context of removing indirect advertisements, and for aesthetic reasons.

Our system aims at the automatic detection of text. This is done by the algorithm. Fig. 1 shows the flow diagram of text detection algorithm. The algorithm steps are summarized as follows.

1. An efficient edge detection scheme is applied to the greyscale image. The image I is blurred (to reduce false edges and over-segmentation) using open-close and close-open filters. The final blurred image Ib is the average of the outputs of these filters. The 3 x 3 8-connected structuring element of type ‘square’ is used here. Next, the morphological gradient operator is applied to the blurred image Ib resulting in an image G as follows:

   G = Dilation (Ib) – Erosion (Ib)

   The Morphological gradient is an edge-strength extraction operator that gives symmetric edges between foreground and background regions.

   The resulting image is then thresholded to obtain a binary edge image. Global thresholding technique is used for that.
2. Closed edges in the binary edge image are grouped by dilation using eight- connected structuring elements. Then small connected components in the dilated image are filtered using erosion. The output is a binary image that contains text candidate regions.
3. Connected component labelling is performed to label each object separately.
4. After applying connected component labelling, the first set of criteria is applied which eliminate all objects whose area is greater than 10000and filled area is greater than 8000. One more criteria namely major axis length is used which is used to retain the text region alone. All objects, whose major axis lengths are in between 20 to 3000, are considered to be text. To eliminate small objects, connected component labelling is applied to the resultant image and the second set of criteria is applied which eliminates all the objects whose area is less than 300 and filled area is less than 500.

After applying all these 4 steps, we get a filtered image that contains only text regions.

III SYSTEM MODEL

A. System model

As we have shown in Fig.1, the system we are proposing is comprised of the below modules. These modules are consolidated to provide a secure system based on cloud.

- CSP or Cloud service provider is providing the space to store the data.
- Data owners are the user who owns the data or in other words this data is his asset. He encodes the data and put it on cloud storage.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

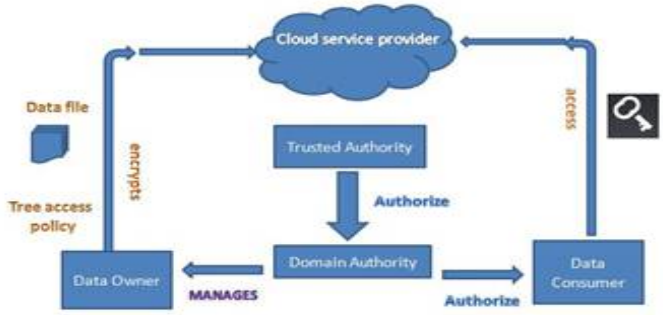

Figure (a) System Architecture

- Data consumers are the user who needs the data from data owner. He is the user who uses the data for performing various operations on it. He downloads the encrypted data and then decrypts it using his private key.

- Domain authority is the authority which is responsible for the management of the data owner as well as data consumer.

- The trusted third party is the root authority which deals with the management of all the domain authorities.

B. Mathematical model

Bilinear Maps: Assume that G, Gt, GPT are the cyclic groups. These groups are multiplicative and are having a order p. Here p is denoting prime[13][14].

Let us take $g1_p$ as the generator of group GP1, and similarly $g2_q$ as the generator of GP2

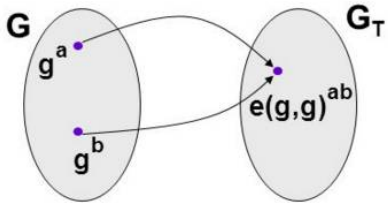

Fig 2.Cyclic group of prime order p

thus e: GP1 × GP2 → GPT will be a bilinear map only if the following properties are satisfied:
1.Bilinearity: $e(g1_p, g2_q)=e(g2^q, g1^p)=e(g1, g2)^{qp}=1$
$e(g1_p, g1_p^x \cdot g2_q^y) = e(g1_p, g1_{ap})x$

2. Non-degeneracy: We can call Gp as a bilinear group if the operation of group as well as its bilinear map e is efficiently computed.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

III. OUR CONSTRUCTION

Security of the data can be ensured only if the data or information that is being transmitted inside the system is in encrypted form. Also whenever a remotely located server is used then there should be check for malware detection.. Here we are developing a third party application that is helping us to protect our data at our end. Cloud service provider also ensures us to provide the security to our data but we are applying another level to secured system so that even if a security breach occurred in cloud, our data remains confidential. Here we are using DES algorithm for encrypting the data. Also for the purpose of authentication we are creating a certificate hat will be based on RSA. This certificate is used while authenticating an individual.

Our trusted third party system is a collection of software's that ensures the end to end security of a system. This software's apply security policies on the system which enhance the resistance of system against attack from hackers. The TTP ensures that a user of one domain cannot access the data of the user of other domain. Among domain also it ensures that the user can only access the data of the level for which he is having the access. A secret key is generated by the TTP for each user and this key is not even known to the TTP as it is in an encrypted form. This key is used for encryption as well as decryption.

Key Structure: As our system ML-ASBE is based on CP-ASBE [10][9][11]the access structure is intact with the ciphertext. The attributes are associated with the key tree structure and this key is used by the user to decrypt the file. If the key structure matches with the ciphertext access structure then only user will be able to decrypt it.

E.g. here we are going to explain the concept of our proposed system through an example

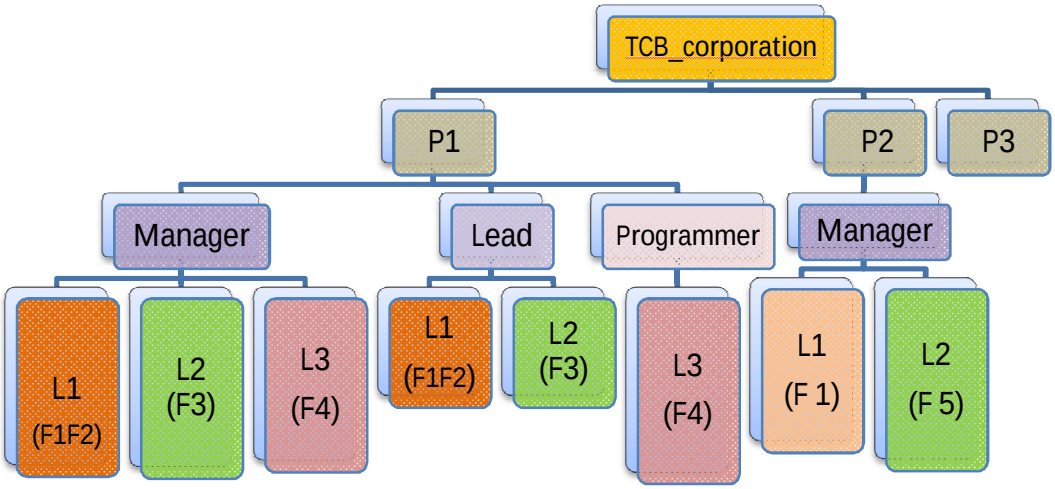

Fig3. System model example

In the below example there is an organization named as TCB. In TCB there are a number of projects but we will take here three projects. There are three different positions under which an employee can be categorized in TCB. These are manager, lead and programmer. Now a manager can have access to three levels L1, L2 and L3, lead will have the access to L1 and L2, and programmer will have the access to only L1 level.

So for example let us take a scenario in which an employee is at the post of manager for project 1 but simultaneously he is playing a role of lead in project 2. So in fist project he must be having the access to all the three levels but in second project he should be having only the access to level 1 and 2. So in our system this employee cannot combine the attributes of first project to access the three levels of project 2 as the combination across the sets is not allowed.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Access policy: Access policies define the access structure of data. Here we are going to use the similar scheme used in [11][12]. The attributes are represented by the leaf nodes and the gates such as AND and OR gates are being represented by the non leaf nodes. In our system we are going to take threshold values as 1 and 2. In fig.3 we have shown the access structure of company TCB. According to this structure only a user belonging to TCB company and is a manager or lead can access the data at level 1 and 2. The combination of attributes is possible only within the domain, inter domain combination is not allowed.

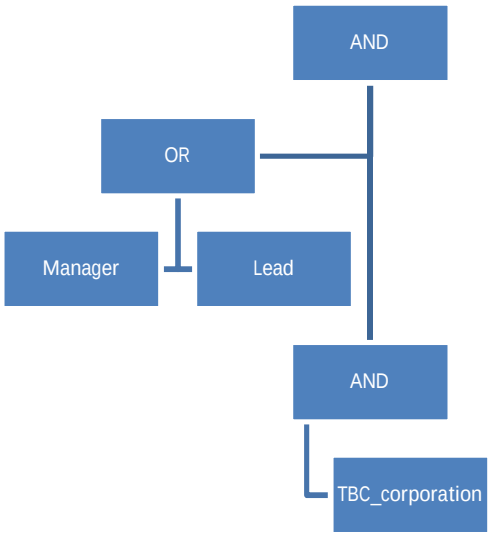

Fig 3.access structure

V. IMPLEMENTATION

The implementation of ML-ASBE is inspired by the CP-ASBE[10] and HASBE[9][12]. The simulation is done on a laptop which is having an Intel i3 processor possessing 1.8 GHz speed. The RAM is 4GB and windows 8.1 version is used. The system is built using the JAVA language. JAVA libraries have been used and DES algorithm has been used for encryption purpose.

The following algorithm is used in our implementation

Algorithm:

1) ***Setup (d):***The parameter d is the depth parameter. This d defines depth of the structure of key. The key depth is dependent on the symmetric bilinear maps. This is having k's value whose range varies from 1 to d.

2)***CreateDomain (*PK,A*)***:This takes the public key (PK) as one of the input parameter and recursive attribute set is taken as another parameter. This set is defined as $A=\{A_0\ A_1\ A_2 \ldots A_N\}$ where $A_m=\{A_{m,1}, A_{m,2}, A_{m,3} \ldots A_{m,n}\}$. Here m is the m^{th} element of this set and n denotes the no of attributes. Whenever any new domain authority i.e. DA_i request to enter the system, TTP validates it and if it a valid domain then CreateDomain ( ) function is called to create the domain.

3) ***Create User (DA$_i$, U, A):*** After the domain is created its time to create the user. To create the user system takes the domain as input in which user has to be created. Along with this the identity of the user as u and a key structure a is also taken. Finally the output is a secret key SK_u for user u.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

4) New file creation: User places his data on cloud which is in the form of files. These files are firstly encrypted by the user and then they are stored. The steps for encryption are as follows:

1. Select one unique id that will be used for the data file.
2. A data encryption key k is chosen randomly and then data file is encrypted using DES.
3. The final step is to depict a tree access structure t for the file. After defining this file can be encrypted as below:

Encrypt (PK, M, CT)*: The inputs to this function are the public key PK, the message* ***M*** *and the access tree structure. From these inputs the output is generated as a cipher text* ***CT****.*

5) ***Decrypt (CT, SKu):*** Now when the data consumer wants to use the data uploaded by the data owner he will request the cloud. Cloud will provide the data if user is authorize to that. But even this data will be in encrypted form. Now the user must be able to decrypts the data. For decryption purpose the user function *Decrypt* ***(CT, SKu)****is used. This function takes the* cipher text CT and secret key $SK_u$for user *u as an input after decryption the output is the message M.*

VI. CONCLUSION

Security concern is a major roadblock in the growth of cloud computing. So is the demand of the time to ensure that the data is safe and secured on cloud. Along with security providing access control helps cloud to evolve and thus provide flexibility to it. In this Paper we have demonstrated the use of ML-ASBE algorithm. Here we have focused on authenticity mechanism and Authorization such that it supports the assignment of multiple values to attributes along with maintaining the confidentiality.

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 ,International 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] HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud ComputingZhiguo Wan ; Key Laboratory for Information System Security, Ministry of Education, Tsinghua National Laboratory for Information Science and Technology, and School of Software, Tsinghua University, China ; Jun'e Liu ; Robert H. Deng
[10] Xingbing Fu and Zufeng Wu:Ciphertext Policy Attribute Based Encryption with Immediate Attribute Revocation for Fine-Grained Access Control in Cloud Storage ,IEEE 2013
[11] John Bethencourt, Amit Sahai, Brent Waters :Ciphertext-Policy Attribute Based Encryption 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 Encryption Rakesh,University of Illinois at Urbana-Champaign {rbobba,hkhurana,mmp}@illinois.edu,July 27, 2009.
[13] http://www.upl.cs.wisc.edu/~bethenco/bilinear_maps.pdf
[14] Published on May 9, 2013,The 3rd Bar-Ilan Winter School on Cryptography: Bilinear Pairings in Cryptography, which was held between February 4th - 7th, 2013