Comparative Study of Attribute Based Encryption Techniques in Cloud Computing

R.Manjusha,
Research Scholar, Department of Information Technology, Sathyabama University, Chennai India,manjusha84rr@yahoo.co.in.

R.Ramachandran,
Professor (ECE), &Director (Research),
Sri Venkateshwara college of Engineering,
Sriperumbudur, Chennai, India,
rrama@svce.ac.in

***Abstract*—Cloud computing is a model on which organization and individuals can work with application from anywhere in the world on demand. The major issue of cloud computing is preserving confidentiality and integrity of data in data security. The primary solution to this problem is encrypting cloud data. Security in cloud computing being one of the classic research topic. Many techniques have been proposed on attribute based encryption techniques. In this paper multi authority hierarchical attribute based encryption is proposed and it is compared with key policy and cipher text policy attribute based encryption techniques. Based on NIST statistical test highest security attribute based encryption algorithm is selected in cloud.**

Keywords— Cloud security, Attribute based Encryption, NIST statistical test

I. INTRODUCTION

Cloud computing is internet based computing, which is used to share resource as service, software as service, infrastructure as services, platform as services are provided to the customers. For cloud customers it is secure to store and share the sensitive data in cryptographic cloud storage. We have applied revocation schema to cipher text policy, key policy, and multi authority hierarchical attribute based encryption. The problems of existing scheme is discussed in section 2.The working of attribute based encryption is explained in section 3. We use NIST test to select highest security attribute based encryption. We have applied revocation technique to key policy attribute based encryption in Section 4.In key policy attribute based encryption user gives secret keys based on set of attributes. In cloud a dummy attribute is set such that every file is encrypted with every cloud user, but the cloud does not know about the dummy attribute. The sensitive data in cloud is encrypted using the keys of the attributes such that a user who has all the attributes will be able to decrypt the sensitive data. User revocation is applied to cipher text policy encryption; each file stored in cloud has users who can access to re-encrypt severe computational overhead on the data owner. Three revocation techniques are used namely two layered encryption, proxy Re-encryption and lazy Re-Encryption. In Two-Layered Encryption technique, initially data owner encrypts data after which the cloud encrypts the data for the second time. When a user is removed, the data owner has the cloud server that decrypts the second layer then re-encrypts with a different encryption. In Proxy Re-Encryption technique the third party re-encrypts the already encrypted data to create a new encryption; the third party does not get to see the data decrypted so it never learns anything. In lazy Re-Encryption, cloud files are not re-encrypted until a user wants access and then spreads out the re-encryption over time to speed up access with the third party. We have applied revocation to cipher text policy attribute based encryption. In cipher text policy attribute based encryption is explained in Section 5 .We have applied revocation technique to multi authority Hierarchical attribute based encryption in Section 6 .We have implemented multi authority hierarchical attribute based encryption in Section 7.We compare various techniques for encryption that consist of attribute based encryption (ABE) and its types Key policy, cipher text policy and multi authority hierarchical attribute based encryption on NIST statistical test on Section 8.We have concluded based on NIST statistical test we have selected highest security attribute based encryption in cloud in Section 9.

II. DISCUSSED PROBLEMS

The science of encryption cryptosystem is divided into two types. They are classical cryptosystem and public key cryptosystems. The main problem of classical cryptosystem is key distribution and management is difficult. The problem of public key cryptosystem is operational problem because encryption and decryption keys are different. The limitation of key policy attribute based encryption is that it cannot decide which user is decrypting data which is in encrypted form. Key policy attribute based encryption can only choose descriptive attributes for data. Key policy attribute based encryption will trust the key issuer. It is providing fine grained access but has no longer flexibility and scalability. Limitations of cipher text policy attribute encryption are not fulfilling company requirements control. In cipher text policy attribute based encryption it is difficult to specify the policies and manage user attributes. It needs to be improved in the flexibility and efficiency of cipher text policy attribute based encryption. In cipher text policy attribute based encryption the decryption keys only support user attribute that are arranged in single set, so user uses single set of attributes to issue their keys to satisfy policies.

978-1-4799-5026-3/14/$31.00©2014 IEEE

III. WORKING OF ATTRIBUTE BASED ENCRYPTION

In Attribute based encryption access Policy of algorithm is associated with Private Key of user where leaf nodes are attributes coming from fuzzy identity. The attribute based key policy encryption setup algorithm generates Alice's master key. Alice's identity is being decided by key policy which in turn is being decided from identity. Key Policy algorithm generates private key for Alice. Cherishma encrypt message M with set of attributes k.

Priyanka can decrypt M if her key policy is satisfied with K.Alice can decrypt M if her key policy is satisfied with k.For Example Alice can decrypt the file encrypted with set of attributes{"Information Technology","Admission Committee"}.But Alice cannot decrypt the cipher text associated with attributes {"Information technology", "Program"} .The difference between key policy and cipher text policy attribute based encryption is , in key policy attribute based encryption access policy depends on private key and in cipher text policy attribute based encryption access policy depends on cipher text. The Hierarchical attribute based encryption is a combination of hierarchical identity based encryption and cipher text policy attributes based encryption. The Hierarchical attribute based encryption is classified into trees according to their relationship defined in the access control system. For example employee database access control depends on hierarchical attribute based encryption. According to concept of hierarchical attribute based encryption manager has privilege to access the entire data in the company. Team leader has privilege to access the employee's details and his own data in the company. Employee has privilege to access his own data in the company.

IV. IMPLEMENTATION OF REVOCATION TECHNIQUES ON KEY POLICY ATTRIBUTE BASED ENCRYPTION

In key-policy attribute based encryption private key is assigned to access policy and cipher text is associated with attributes. Decryption of data is possible only when a attribute satisfies the policy. Revocation of key policy encryption is important, without it no security control is ensured.

Key policy attribute based security algorithm

Step 1: Setup

Step 2: Encryption

Step 3: Key Generation

Step 4: Decryption

Setup stage of algorithm takes input as security parameter, let it be sp and produce output as master key and private key.

Encryption process is done using set of attributes.

Decryption of the message is done once access structure is satisfied, they can drive the key and decrypt the message.

The key is associated with access policy.

In Key policy attribute based encryption, the cipher text is associated with set of attributes and provides data owner with key and policy pair. The user decrypts the message if and only if attribute in cipher text of user satisfy the access policy in the key. For example in Hospital Management System, if the management need to encrypt the data attributes such as {Doctor, Nurse, Administrator, Inpatient, Outpatient, Research head, Manager, Dean, Vijaya hospital, Vijaya health center hospital}.Dolly is a doctor of Vijaya hospital and Research Head of Vijaya health center, so her access policy would be (Doctor AND Vijaya hospital) OR (research head AND Vijaya health center).Priya is a manager of Vijaya hospital her access policy be (Manager AND Vijaya Hospital).Aruna is manager for both Vijay hospital and Vijay health center her access policy would be (Manager AND(Vijaya hospital OR Vijaya health center).In cipher text Vijaya hospital would be encrypted with attribute {Doctor, nurse, administrator, inpatient, outpatient, Research head, manager}.Some information to Vijaya hospital and Vijaya health center known only to manager would be labeled (administrator,manager,vijaya hospital ,Vijaya health center).To implement policy to key, threshold gates are inserted to access tree. Key is issued to trust worthy party if and only if it satisfies access policy .For example key is not issued to policy: Vijaya hospital and Vijaya health center. Key is issued to policy: Doctor AND Vijaya hospital OR research head AND Vijaya health center.

V. IMPLEMENTATION OF REVOCATION TECHNIQUES ON CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION

In cipher text attribute based encryption Private Key is assigned to "attributes"

Cipher text is associated with "access policy" and it "Can decrypt only when attributes satisfy policy". Revocation of cipher text policy encryption is important without it no security control is ensured

Cipher text policy attribute based encryption

Step 1: Setup

Step 2: Encryption

Step 3: Key Generation

Step 4: Decryption

Setup stage of algorithm takes input as security parameter, let it be sp and produce output as master key and private key.

Encryption process is done using access structure of cipher text. Decryption of the message is done once access structure is satisfied with cipher text and decrypts the message. The cipher text is associated with access policy. Private Key is associated with attributes.

VI. IMPLEMENTATION OF MULTI AUTHORITY HIERARCHICAL ATTRIBUTE BASED ENCRYPTION

Hierarchical attribute based encryption is new methodology for providing full security, no partitioning and no aborts. Hierarchical attribute based encryption is a combination of Identity Based Encryption and cipher text policy attribute based encryption.

In hierarchical attribute based encryption attacker does not have key capable of decrypting. Attacker cannot distinguish nominal from regular semi functionality. Revocation of multi authority hierarchical attribute based encryption is important without it no security control is ensured.

Multi Authority Hierarchical attribute based encryption

Step 1: Setup
Setup 2: Create Domain master authority (DMA)
Step 3: Key Generation
Step 4: Encrypt the file
Step 5: Decrypt the file
In setup phase of multi Authority Hierarchical attribute based encryption(MAHABE) the Domain master administrator based on hierarchy gives privilege to user to access the data. In setup stage algorithm takes Input as security parameter sp and produces output as Master key mk and secret key sk. In employee database example Domain master administrator takes security parameter as input and gives master key and secret key as output to manager.
In Key generation phase of multi Authority Hierarchical attribute based encryption it generates master key and secret key.
Generation of Master key
When generating master key it takes input as public key of system pk , public key of user pk+1 and master key mk and produce output as Master key mk.+1.Master key is generated by domain master administrator by taking public key of system pk, public key of user pk+1 and master key mk.
Generation of Secret Key
When team leader sends request to domain master administrator for user identity secret key SKui and user attribute secret key SKua , domain master administrator verifies whether he is authorized user or not. If team leader is authorized user domain master administrator creates the user identity secret key and user attribute secret key by using the public key of the team leader, master key (MK), user identity of public key (PKu), user attribute of public key (PKa). Likewise the team leader generates the secret keys for the Employees in hierarchy way.
Encryption
In input of encryption phase is plaintext PT, set of attribute SA and public key PK and produces output as cipher text. Manager wants to send message M to team leader. Manager encrypts the message M and sends to cloud service provider. Cloud service provider sends the encrypted message (cipher text) to Team leader.
Decryption
In Decryption phase it takes input as cipher text CT, Public key and secret key SK and produces output as Plaintext PT.
Multi Authority Hierarchical attribute based encryption scheme security level is high since access control is based on hierarchy of the tree.

VII. IMPLEMENTATION STAGE

We have implemented the attribute based encryption in Salesfores.com website. In cloud the best practices for security is Salesforce.com software as service. In salesforce.com website we can encrypt the data like social security number and credit card numbers .After creating an encrypted custom fields, salesforce.com automatically encrypts the data using AEs 128.It will then split the key to separate the keying material between application server and database so that no single salesforce.com administrator can recover both parts of the key. The encrypted custom field have restrictions, they cannot be an external ID and do have default values and they are not searchable or available for use in filters such as list views, reports up summary fields and rule filters. When user application requires more control than one possible way, it is through declarative encrypted fields, user can use methods in Apex Crypto class to programmatically encrypt and decrypt sensitive information in saleforce.com.Apex crypto also provide you with methods for creating digest, message authentication codes and signatures.

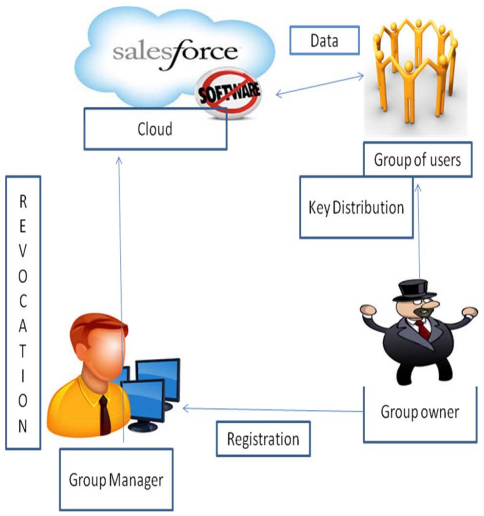

Fig. 1. Cloud Architecture

In salesfore.com cloud service provider website, data is shared by multiple data owners and multiple consumers. In salesfore web site group manager will take the charge of access control, system parameter generation, user revocation. For example the group manager is acted by administrator of the company. Group manager is fully a trusted party. In salesfore.com cloud service provider website, data is shared by multiple data owners and multiple consumers share them. Group owner is the one selected from group members and he is responsible for user registration, distributing updated revocation, assigning ID and traceability. To secure customer data in Salesfore.com we have implemented three attribute based encryption algorithm techniques. Steps to store data and to encrypt data in salesforce.com are follows.
Step 1: In this step we login to saleforce.com by giving username, email id and password which have already securely verified the user's registration, such as symmetric key based challenge reply login verification or through a onetime password.
Step 2: After the user's login has been successfully verified, Client can create account and save the data in encrypted form using attribute based encryption algorithm.
Step 3: Using attribute based encryption access policy to users is set.

Step 4: Three different algorithms are implemented to provide data security to user.
Step 5: First we have applied key policy attribute based encryption to client data. Access policy depends on user private key.
Step 6: Second we have applied cipher text policy attribute based encryption to client data .Access policy depends on cipher text.
Step 7: Third we have applied multi authority attribute based encryption to client data. Access policy depends on both cipher text and private key

Step 8: Once data is encrypted using attribute based encryption algorithm request is sent to the encryption/decryption service system along with userid
Step 9: Encrypted data is stored in encryption/decryption service system can serve multiple users and encryption/decryption for each user's data requires a different key.
Step 10: If Multiple users want to access the encrypted data, depending on access policy data can be decrypted and viewed by users.

VIII. Comparison of various Attribute Based Encryption based on NIST Statistical Test

We use NIST Statistical test to get the highest security attribute based encryption algorithm, NIST developed to test the randomness of binary sequence produced by either hardware or software based cryptographic random or pseudorandom number generator .We have to sign into sales fore website to create an account. Apply attribute based encryption algorithm to get ciphers text. Launch run NIST statistical test for each sequence to encryption algorithm to get P-value. Compare p-value to 0.01, if p-value less than 0.01 reject the sequence. We compare three encryption methods based on P-value and Rejection rate . We have 128 sequences for three encryption algorithm. The p-value represents the probability of observing the value of the test statistic which is more extreme in the direction of non-randomness. The maximum number of rejection was computed using above formula [1]

$$\text{Rejection rate}=s\ (\alpha+3\sqrt{\alpha(1-\alpha)}/s) \qquad (1)$$

Where s is sample size and α is significance level chosen 0.01. The comparison between three attribute based encryption algorithms performed based on p-value and rejection value.

The number of rejection rate is obtained from equation number 1. If P values are high and Rejection rate is less, then the algorithm is highly secured. The comparison of key policy attribute based encryption, cipher text policy attribute based encryption and multi authority attribute based encryption is based on p-value for 128 samples is shown in Figure 2. P-value measures, non randomness of the samples-value indicates failure. When statistical test is done on sequences p-value should be greater than 0.01 In Fig 2 X-axis represents Attribute based encryption techniques and Y-axis represents p-value.

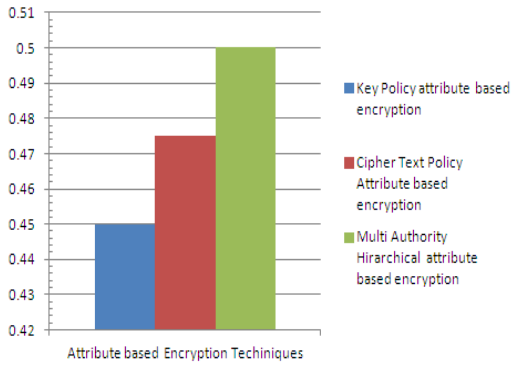

Fig. 2. The comparison of Attribute based encryption techniques based on p -value

The comparison of key policy attribute based encryption, cipher text policy attribute based encryption and multi authority attribute based encryption is based on Rejection rate for 128 samples is shown in Fig 6. In Fig 3 X-axis represents Attribute based encryption techniques and Y-axis represents rejection rate.

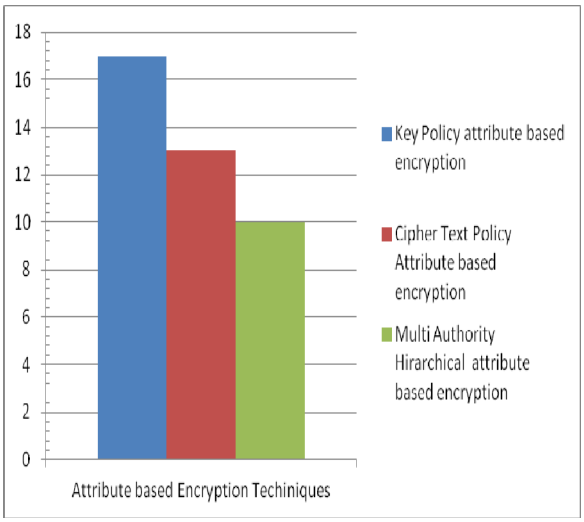

Fig. 3. The comparison of Attribute based encryption techniques based on Rejection Rate

Based on NIST statistical test rejection list of attribute based encryption is listed in table 1.The test case of NIST input is values obtained from sales force website of three algorithms and output is acceptance and rejection rate of algorithm.

TABLE I. COMPARSION BETWEEN ATTRIBUTE BASED SECURITY ALGORITHM BASED ON REJECTION RATE TO GET HIGHEST SECURITY

NIST TEST	Key –Policy Attribute based Algorithm		Cipher Text Policy Attribute based Algorithm		Multi Authority Hierarchical Attribute Based Algorithm	
	Reject	Accept	Reject	Accept	Reject	Accept
1	1	127	3	125	1	127
2	0	128	2	126	0	128
3	2	126	52	76	2	126
4	2	126	51	77	4	124
5	4	124	0	128	3	125
6	3	125	2	126	0	128
7	1	127	4	124	2	126
8	3	125	52	76	4	124
9	2	126	51	77	3	125
10	52	76	0	128	0	128
11	51	77	1	127	52	76
12	0	128	0	128	51	77
13	2	126	2	126	0	128
14	4	124	0	128	1	127
15	3	125	2	126	0	128
16	3	125	2	126	2	126

The key policy attribute based encryption accepts the sequence in NIST test 2 and NIST 12 so acceptance rate key policy attribute based encryption is 2 and rejects the sequence in NIST test 1,3,4, 5, 6,7,8,9,10,11,13,14, 15,16 so rejection rate is 14.The cipher text policy encryption algorithm accepts the sequence in NIST test 5, NIST test 10 and NIST test 14 so acceptance rate of sequence is 3 and rejects the sequence in NIST test 1,2,3,4, 6,7,8,9,11,12,13, 15,16 so rejection rate is 13. In multi authority hierarchical attribute based encryption algorithm accepts the sequence in NIST test 2 NIST test 6 ,NIST test 10, NIST test 13 and NIST test 15 so acceptance rate of sequence is 5 and rejects the sequence in NIST test 1,3,4,5,7,8,9,11,12,14,16 so rejection rate is 11.Multi authority attribute based algorithm has highest security based on NIST test result based on p-value or rejection rate. The rejection rate of multi authority hierarchical encryption is less compare to key policy attribute based and chipper text policy attribute based encryption.

IX. CONCLUSION

In this paper we have compared various techniques for encryption that consist of attribute based encryption (ABE) and its types; Key policy, cipher text policy and multi authority hierarchical based encryption on NIST statistical test. Based on NIST statistical test we have selected highest security attribute based encryption in cloud. The rejection rate of multi authority hierarchical encryption is less compared to key policy attribute based and chipper text policy attribute based encryption. Multi authority hierarchical attribute based encryption ensures the most security in user data. Multi authority hierarchical encryption take less time to encrypt the data compared to key policy and cipher text policy hierarchical attribute based.

X. FUTURE ENCHANCEMENT

In future we are going to enhance security of multi authority hierarchical attribute based encryption to homomorphic multi authority hierarchical based encryption algorithm in cloud. In homomorphic multi authority hierarchical based encryption algorithm we are combining homomorphic encryption technique with multi authority hierarchical attribute based encryption to decrease the encryption and decryption time of existing algorithm.

REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control inCloud Computing" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012

[2] Eman M.Mohamad ,Hatem S.Abdelkader,"Enhahanced data security Model for cloud computing", The 8th International conference on Informatics and system(InFo2012)14-1 May 2012

[3] Affiliation Juan Soto,National Institute of Standards and Technology 1oo bureau Drive,Stop 8930 Gaithersburg"Randomness Testing of Advnced Encryption Standard Candidate Algorithm "

[4] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[5] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009

[6] Zhibin Zhou, Dijiang Huang" On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption"

[7] [5] R.Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non-monotonic access structures". In Proc. of CCS'06, New York, NY, 2007.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data". In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.

[9] Ximeng Liu[1], Pei-Shan Chung[2] and Min-Shiang Hwang," Ciphertext Policy Hierarchical Attribute-Based Solution for Fine Grained Acess control of Encrypted Data.International Journal of Network Security vol 16. July 2014

[10] Eman M.Mohamed,Hatern S,Abdelkader,Sherif EI-Etriby,"Enchanced Data Security Model For Cloud Computing,International conference on Informatics and System(Info 2012)14-16 cloud and mobile computing track.