http://dx.doi.org/10.21172/ijiet.81.020

Advanced Cipher-Text Policy using Hybrid Attribute based Encryption and Customizable Authorization in Cloud Computing

Mahesh S. Gunjal
Department of Computer Engineering
Amrutvahini College of Engineering,Sangamner

Dr. B.L.Gunjal
Associate Professor, Department of Computer Engineering
Amrutvahini College of Engineering,Sangamner

Abstract- In most of the several centralized systems a user has authority to access data if a user has a certain set of attributes. Presently, the one method for compete such policies is to use an authorized cloud server to maintain. The user data and has access control over it. Many times, when one of the servers keeping data is compromised, then the security of the user data will be compromised. In the cloud, for getting access control and maintaining data secure and for the exactness of the secure computing results, the data owners has to kept attribute-based security to encrypt the stored data. Since, during the delegation, the cloud servers have tampered or replaced the cipher-text and change a forged computing result with malicious intent. They may also cheat the authorized users by responding them that they are unauthorized for the cost saving purpose. Many times, during the encryption, the control access attribute policies may not easy enough as well. In this paper we present a system for maintaining complex access control on encrypted data that we call Cipher-text-Policy Attribute-Based Encryption with verifiable customizable authorization. By using our techniques encrypted data can be kept data confidential even if the storage server is comprised. Further Moreover, our methods are highly secured against collusion attacks. Our scheme provides security against chosen-plaintext attacks under the k-multi-linear Decisional Diffie-Hellman assumption. In advance, we provide an implementation of our system and give performance measurements.

Keywords – Cipher-text-policy attribute based encryption, hybrid encryption, user authorization, circuits, multi-linear map, Dual Encryption.

I. INTRODUCTION

Cloud computing is an on requested service in which shared data, information, software and other devices are provided according to the user need at that time. It's a condition which is usually used in case of Internet. The whole Internet can be termed as a cloud. Capital and execution costs can be less using cloud computing [4].

Within these computing environments, the cloud servers can validate numerous data services, such as access control data, storage and outsourced secure computation. For data storage, the servers kept a huge amount of shared data, which has to be accessed by, authorize centralized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user's needs. Presently, the use of cloud computing is tremendous. So confidentiality and delegation problems are arising. More present public key attribute methods allow a party to encrypt data to a specific user, but are unable to effectively handle more expressive types of encrypted access control. So there is a need to enhance a security problem of cloud computing [2].

As applications move to cloud computing platforms for the use of security, a ciphertext-policy attribute-based encryption (CP-ABE) and customizable authenticity are used to validate the data confidentiality and the authenticity of delegation on cloud servers. Delegation computing is a major service given by the cloud servers. Delegation is a process which is performed by the users who are containing the minor computing power. [8] They delegate their decryption process to the cloud server to reduce the computation time. Proposed system uses the k-multi linear Decisional Diffie-Hellman algorithm in order to validate the security to the encrypted data. This takes only small computational and communication time [6] [11]. Customizable delegation is given to defend approved users from human being to bring throughout the delegation. Attribute-based encryption (ABE) is a wider vision for public key encryption that gives users to encrypt and decrypt messages based on user attributes [7] [15]. There are two types of attribute-based encryption methods, are as follows:

- Key-Policy Attribute-Based Encryption(KPABE)
- Cipher-text Policy Attribute Based Encryption(CP-ABE)

In a Key-Policy Attribute-Based Encryption i.e. KP-ABE system, key distributor is the major part. The decision Of access control policy is made by the key distributor instead of the enciphered, which having limited that is it Controls the practicability and usability for the system in practical applications [8] in a Cipher-text-Policy Attribute-Based Encryption i.e. CP-ABE system, each cipher-text is related with an access structure, and each private key is given with a set of different attributes. A user is able to decrypt a cipher-text if the keys attribute set validates the access control structure relates with a cipher-text. Many more, during the deployments of the storage and security services, the main purpose of this research are given as below:

1. Confidentiality: Confidentiality is hardly identical to privacy. It is designed to avoid private data or information from getting to unauthorized people, while making validate that the authorized people can in fact get it. Data encryption is a user known method of ensuring confidentiality.

2. Verifiability: In cipher-text policy based attribute, during the delegation computing, a user could validate whether the cloud server changes a correct makes cipher-text to help him/her decrypt the cipher-text fast and correctly [1].

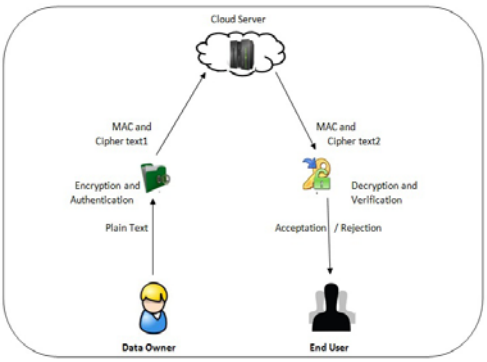

Figure 1. Data Sharing System

A. Our Contribution-

In this work, we use the first construction of a cipher-text policy attribute-based encryption (CP-ABE) with customizable authorization to relate this problem, and give the first construction of such a scheme. In our system, a user's private key will be associated with a random number of attributes expressed as strings numbers. On the other way, when a party encrypts a message in our system, they specify an associated access control structure over attributes. A user only is able to decrypt a cipher-text if that users attributes pass through the cipher-text access control structure. At a mathematical level, access control structures in our system are expressed by a monotonic access tree, where nodes of the access structure are composed of threshold gates and the leaves describe attributes.

We have that AND gates can be constructed as no of n threshold gates and OR gates as 1-of-n threshold gates. Furthermore, we can handle many complex access controls such as numeric ranges by transferring them to minimum access trees.

The rest of the paper is organized as follows. Problem Statement is presented in section II. Proposed work is explained in section III. Proposed algorithms are explained in section IV. Experimental results are presented in section V. Concluding remarks are given in section VI.

II. Problem Statement

For customizable authorization in cloud computing and for accessing control and maintaining data secure by elimination computing cost and to achieves security against chosen-plaintext attack a system is developed called Cipher-text Policy Attribute-based Encryption (CP-ABE) and customizable authenticity, under the k-multi-linear Decisional Diffie-Hellman assumption are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers. The main motto of our project is for achieving access control and keeping data confidential by reducing computing cost and to achieve security against chosen plaintext attacks in order to prove the efficiency of the proposed work.

III. Proposed Work

We mainly present a circuit cipher-text-policy attribute-based hybrid encryption with customizable authorization scheme. General circuits are used to deploy the strongest form of access control policy. The proposed scheme is proven to be secured based on k-multi-linear Decisional Diffie-Hellman assumption. On the other hand, we

implement our scheme over the integers. During the delegation computing, a user could validate whether the cloud server responds a correct transformed cipher-text to help him/her decrypt the cipher-text immediately and correctly. We have design an architecture which is proven to be secure based on k-multi-linear Decisional Diffie-Hellman assumption. On the other hand, we implement our scheme over the integers. The cost of the computation and communication consumption has that the scheme is practical in the cloud computing [13]. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable customizable authorization in cloud. Since policy for general circuits provides to achieve the strongest form of access control, a construction for realizing circuit cipher-text policy attribute-based hybrid encryption with customizable authorization has been considered in our work. In such a system, added with verifiable computation and Encrypt-then-Mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the instant time. Besides, our scheme achieves security against chosen-plaintext attacks under the k-multi-linear Decisional Diffie-Hellman assumption [12].

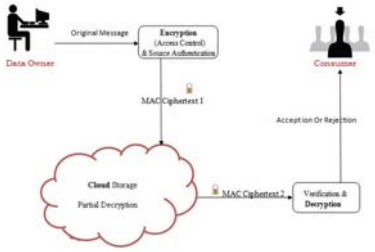

Figure2. System Architecture

In the system, the data owner and the users are both registered entities and got private keys from the authority. The authority is supposed to be the only party that is fully trusted by all participants. Similar to the previous schemes [3] [18], the Figure 3.System Architecture server is supposed to be un-trusted. Sound trust management standards as well as auditing standards could be used to establish fine business providence between the cloud server and the user. According to this frame, the cloud server could be regarded as a trustworthy cloud service provider. Actually, the role-based access control is proposed based on this assumption. However, using this single mechanism, we will be at the risks of unknown attacks and the existing of the malicious system administrator, which may result in data leakage, invalidation of access control and failure of outsourcing [17]. Besides, trust management mechanism may cause an extra workload for the auditor. Thus, it is high time to construct a practical cryptography scheme to protect data and control access with an unauthorized server.

IV. PROPOSED ALGORITHM

A. System Flow-

The various system attributes are following:

1. Attribute Authority: Authority will have to provide the key, as per the user's key request. Every users request will have to be raised to authority to get access key on mail.

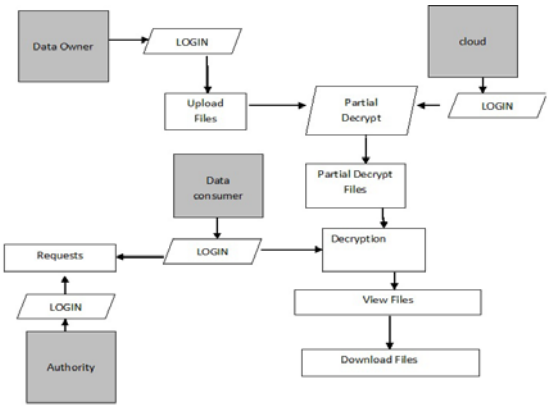

Figure3. System Flow

2. Data owner: Data owner will have to register initially to get access to the profile. Data Owner will upload the file to the cloud server in the encrypted format. Random encryption key generation is happening while uploading the file to the cloud. Encrypted file will be stored on the cloud.
3. Data Consumer: Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data consumer can access the file based on the key received from mail id. As per the key received the consumer can verify and decrypt the data from the cloud.
4. Cloud Server: Cloud server will have the access to files which are uploaded by the data owner. Cloud server needs to decrypt the files available under their permission [10]. Furthermore data user will have to decrypt the data to access the original text by providing the respective key. File has been decrypted successfully and provided for consumer.
5. Email Authentication: Email authentication is a collection of techniques aimed at equipping messages of the email transport system with verifiable information. It is a coarse-grained authentication, usually at Administrative Management Domain (ADMD) level and implies no sort of authorization. That is, the purpose of email authentication is to validate the identities of the parties who participated in transferring a message, as they can modify the message. The results of such validation can then be used in delivery decisions, which are beyond the scope of email authentication proper, and are quite different in nature.

If you're receiving mail: Recipients can use authentication to verify the source of an incoming message and avoid phishing scams. For example, if you see messages claiming to be from google.com, but are not properly authenticated as coming from google.com, these are phishing messages. You should not enter or send any personal information. Remember, Google will never ask you to send personal information.

B. Proposed Algorithm

1) Algorithm 1: Cipher-text-Policy Attribute Based Encryption Algorithm: A cipher-text policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Encrypt, Key Gen and Decrypt.

i. *Setup:* The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.
ii. *Encrypt (PK, M, A):* The encryption algorithm takes as input: the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a cipher text CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message.
iii. *Key Generation (MK, S):* The key generation algorithm takes as input: the master key MK and a set of attributes S that describe the key. It outputs: private key SK.
iv. *Decrypt (PK, CT, SK):* The decryption algorithm takes as input: the public parameters PK, a cipher-text CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the cipher-text and return a message M.
v. *Delegate (SK, S):* The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S Ł S. It output a secret key SK for the set of attributes S.

2) Algorithm 2: Diffie-Hellman Algorithm: Requires: Two large numbers, one prime (p), and (a), a primitive root of P Consider: Michael (Sender) wants to share key through a medium with Stuart (Receiver) but spy (Third Party) access all data.
Step 1: Select a sufficiently large prime number q.
Step 2: Select an integer a.
Step 3: This should be a primitive root of q.
Step 4: That means it should satisfy the following: The values of mod q , 2 mod q, 3 mod , ... , q-1 mod q, should all be distinct i.e. they should be different.
Step 5: Actual key exchange; and q are selected, the two numbers are made public.
Michael:
1. Select a random number M and keeps it with him.
2. Calculates, Y= M mod q
Stuart:
1. Select a random number C and keeps it with him.
2. Calculates, Z= C mod q

Step: 6 The Key Michael: Uses Z to calculate key k1 by the following way using his secret key M.
K1= ZM mod q
Stuart: Uses Y to calculate key K2 by the following way using his secret key C.
K2= YC mod q
Step 7: But K1=K2, Thus both of them gets the key even after sharing certain keys publicly.
Step 8: Y= M mod q //a primitive root of q.
Step 9: So Y= M mod q becomes a discrete log problem.
In discrete log problem if you know Y and q then it is close to impossible to find M.
Result: Hence the secret keys are protected. Thus transfer of keys is possible.

V. EXPERIMENT AND RESULT

The experimental result for existing Key-Policy ABE Algorithm model is represents in Table 1.1. The table shows the selecting the number of Attributes, Access control [15] count and Access permission count. The table contains the various attributes, owner and access policy control and access permission count.

Table- 1.1 Security Analysis of Existing Model (KP-ABE)

S. No	Attribute	Owner	Access Control [N]	Access Permission Count [N]
1	Name	P	6	80
2	Age	Q	8	115
3	DOB	R	12	205
4	Salary	S	14	240
5	Attendance	T	19	355

The experimental result for existing Key-Policy ABE Algorithm model is represents in Figure 4. It shows the selecting the number of Attributes and Access permission count based on the access control policy count.

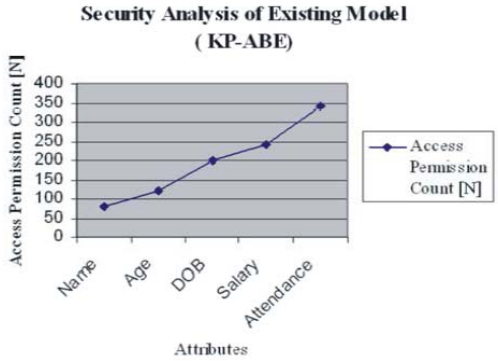

Figure4: Security Analysis of proposed KP-ABE

The experimental result for the proposed Cipher Text-Policy Attribute-Based Encryption (CP-ABE) with User Revocation model is represents in Table 1.2. The table shows the selecting the number of Attributes, Access control count and Access permission count [15]. The table contains the various attributes, owner, and access policy control and access permission count.

Table 1.2: Security Analysis of proposed CP-ABE

S. No	Attribute	Owner	Access Control [N]	Access Permission Count [N]
1	Name	P	10	180
2	Age	Q	15	270
3	DOB	R	18	310
4	Salary	S	26	430
5	Attendance	T	28	520

The experimental result for proposed cipher-text Policy based ABE Algorithm model represents in Figure 5. It shows the selecting the number of Attributes and Access permission count based on the access control policy count.

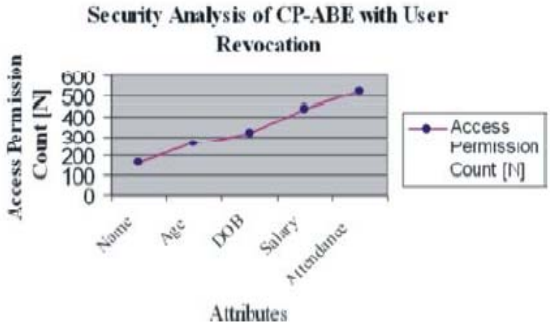

Figure5: Security Analysis of proposed CP-ABE

The comparison result of existing Key-Policy ABE Algorithm and Cipher-text Policy base ABE is represents in Figure 6 [17]. It shows the selecting the number of Attributes and Access permission count based on the access control policy count.

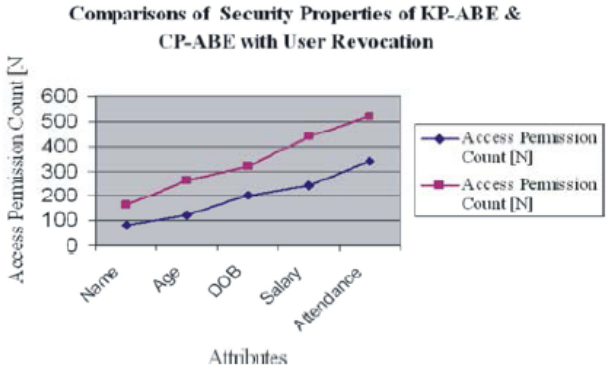

Figure 6: Comparisons of Security Properties of KP-ABE and CP-ABE with User Revocation

VI.CONCLUSION

We mainly have a circuit cipher-text policy attribute-based hybrid encryption with customizable authorization scheme. Combined verifiable computation and encrypt-then-Mac mechanism with our cipher-text policy attribute-based hybrid encryption, we could provide the verifiable partial decryption paradigm to the cloud server. In advance, the proposed scheme is being to be secure based on k-multi-linear Decisional Diffie-Hellman assumption. We implement our scheme over the integers. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could allow it to trust the data confidentiality, the fine-grained access control and the verifiable customizable authorization in cloud servers.

REFERENCES

[1] Jie Xu, Qiaoyan Wen, Wenmin Li and Zhengping Jin, "Circuit Ciphertextpolicy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems VOL. 27, NO. 1, pp.119-129,January 2016

[2] Melissa Chase and Sherman S. M. Chow, Improving privacy and security in multi authority attribute-based encryption in ACM Conference on Computer and Communications Security, pages 121-130, 2009.

[3] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, Securely outsourcing attribute-based encryption with checkability, IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 8, pp. 2201-2210, Aug. 2013.

[4] A. Sahai and B. Waters, Fuzzy Identity Based Encryption, in Proc.EUROCRYPT, pp.457-473, Springer-Verlag Berlin, Heidelberg, 2005.

[5] A.Lewko and B. Waters, Decentralizing attribute-based encryption, in Proc. 30th Annu. Int. Conf Theory Appl. Cryptograph. Techn.,011,pp. 568-588.

[6] B. Waters, Ciphertext-policy attribute-based encryption: An expressive,efficient, and provably secure realization, in Proc. 14th Int. Conf. Practice Theory Public Key Cryptograph. Conf. Public Key Cryptograph, 2011,pp. 5370.

[7] John Bethencourt, Amit Sahai, Brent Waters, Ciphertext-Policy Attribute Based Encryption, Supported the US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316.

[8] Sarath Kumar Reddy, Anish Varsha, Sai Praneeth R.V.C, A Secure Delegation Process using Diffie-Hellman Assumption in Cloud Computing, International Journal of Computer Applications (0975 -8887), Volume 130 No.2, November 2015.

[9] S. angel leola sruthi, Umamageswari, Ciphertext-Policy Attribute-based Encryption for Secure Mobile Applications in Cloud, International Journal of Innovative Trends and Emerging Technologies, ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015.

[10] B. Waters, Ciphertext-Policy Attribute-Based Encryption: An Expressive,Enficient, and Provably Secure Realization, in Proc. PKC, pp.53-70, Springer Verlag Berlin, Heidelberg, 2011.

[11] Bryan Parno, Mariana Raykova, and Vinod Vaikuntanathan, How to delegate and verify in public: Verifiable computation from attribute-based encryption, In TCC, pages 422-439, 2012.

[12] S. Garg, C. Gentry and Shai Halevi, Candidate Mulitilinear Maps from Ideal Lattices and Applications, in Proc. EUROCRYPT, pp.1-17,Springer-Verlag Berlin, Heidelberg, 2013.

[13] J. Lai, R. H. Deng, C. Guan, and J. Weng, Attribute-based encryption with verifiable outsourced decryption, IEEE Trans. Inf. Forensics Secur., vol. 8, no. 8, pp. 1343-1354, Aug. 2013.

[14] Jonathan Katz, Amit Sahai, and Brent Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, In EUROCRYPT, 2008.

[15] Golle, P., J. Staddon, M. Gagne and P. Rasmussen, "A Content Driven Access Control System,"Proc. Symp. Identity and Trust on the Internet,pp: 26-35,2008

[16] Tatsuaki Okamoto and Katsuyuki Takashima, Adaptively attribute-hiding (hierarchical) inner product encryption, In EUROCRYPT, pages 591-608,2012.

[17] M. Maryam Jameelah, C. Suresh Gnana Dhas and P. Suganya," Ciphertext Policy Attribute Based Hybrid Encryption with User Revocation in Data Outsourcing Systems" Middle-East Journal of Scientific Research 24, 242-248, 2016

[18] K. Kurosawa and Y. Desmedt, A new paradigm of hybrid encryption scheme, in Proc. 24th Int. Cryptol. Conf., 2004, pp. 426- 442.

[19] J. Hur and D. K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Trans. Parallel Distrib.Syst., vol. 22, no. 7, pp. 1214-1221, Jul. 2011.

[20] T. Granlund and the GMP development team. (2013). GNU MP: The GNU multiple precision arithmetic library, 5.1.1 [Online].Available:http://gmplib.org/

[21] J. Coron, T. Lepoint, and M. Tibouchi, Practical multilinear maps over the integer, in Proc. 33rd Int. Cryptol. Conf., 2013, pp. 476- 493.

[22] S. Garg, C. Gentry, and S. Halevi, Candidate mulitilinear maps from ideal lattices and applications, in Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2013, pp. 117.