ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Secure Circuit Ciphertext-Policy Attribute-Based Encryption in Cloud Computing

Shirapure Chanchal[1], Natve Madhavi[1], Nakhate Shweta[1], Prof.R.S.Patil[2]

Student, Department of Computer Engineering, SKN-Sinhgad Institute of Technology & Science, Lonavala,Savitribai Phule Pune University, Pune, India[1].

Student, Department of Computer Engineering, SKN-Sinhgad Institute of Technology & Science, Lonavala,Savitribai Phule Pune University, Pune, India[2].

ABSTRACT: In the cloud, for accomplishing access control and data security, the data owners could uses attribute-based encryption to encrypt the stored data. Cloud storage service allows data owner to host their data in thecloud and through which provide the data access to the users. Becausethe cloud server is not trustworthy in the cloud storage system,we cannot rely on the server to conduct data access control. Toachieve data access control on untrusted servers, traditional methodsusually require the data owner to encrypt the data and deliverdecryption keys to authorized users. In these methods, however,the key management is very complicated and inefficient. In thispaper, we design an access control framework in cloud storage systemsand propose a fine-grained access control scheme based onTo reduce the cost, the users which have a limited computing power are nevertheless more likely to delegate the mask of the decryption task to the cloud servers. The result shows, attribute-based encryption with delegation come out. Still, there are some problems and questions regarding to previous related works. For example, during the delegation or release, the cloud servers could misrepresent or replace the delegated ciphertext and respond a fake result with malevolent intent. As well as for the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible during the encryption. Since policy for general circuits are used to achieve the strongest form of access control, a construction to design circuit ciphertext-policy attribute-based encryption is developed. In this scheme each ciphertext is contains an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if and only if the key's attribute set satisfies the access structure associated with a ciphertext.

KEYWORDS: Ciphertext-policy attribute-based encryption, circuits, verifiable delegation, hybrid encryption

I. INTRODUCTION

Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. The advantage of cloud is cost savings. The prime disadvantage is security. The appearance of cloud computing transports a radical novelty to the organization of the data possessions within this calculating surroundings, the cloud servers can present different data services, such as isolated data storage and outsourced allocation calculation etc. For information cargo space, the servers amass a huge quantity of communal information, which might be accessed by certified users. For allocation calculation, the servers could be accustomed to hold and determine frequent data dealing to the user's burden. As appliances shift to cloud computing proposals, verifying delegation process using cipher text-policy attribute-based encryption (CP-ABE) is used to guarantee the data privacy and the verifiability of allocation on untruthful cloud servers. Captivating health check data distribution as an example.among the rising volumes of health check images and health check records, the medical care associations set a big amount of data in the cloud for dropping.The Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for dataaccess control in cloud storage systems, because it gives the dataowner

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

more direct control on access policies and the policy checkingoccurs “inside the cryptography". However, due to the attributerevocation problem, it is very costly to apply the CP-ABE approachto the access control in cloud storage systems. We call a user whoseattribute is revoked as a revoked user.In this paper, we design an attribute-based access control frameworkfor cloud storage systems and propose a fine-grained accesscontrol scheme with efficient attribute revocation. Our scheme doesnot require the server to do any auxiliary access control and dataowners are not required to be online all the time. The revocation isconducted efficiently on attribute level rather than on user level.The advantage of cloud is cost savings. The prime disadvantage is security. The appearance of cloud computing transports a radical novelty to the organization of the data possessions within this calculating surroundings, the cloud servers can present different data services, such as isolated data storage and outsourced allocation calculation etc. For information cargo space, the servers amass a huge quantity of communal information, which might be accessed by certified users. For allocation calculation, the servers could be accustomed to hold and determine frequent data dealing to the user’s burden. As applications shift to cloud computing proposals, verifying delegation process using cipher text-policy attribute-based encryption (CP-ABE) is used to guarantee the data privacy and the verifiability of allocation on untruthful cloud servers. Captivating health check data distribution as an example among the rising volumes of health check images and health check records, the medical care associations set a big amount of data in the cloud for dropping. To make such data sharing be achievable, attribute based encryption is used. There are two forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the second is ciphertext-policy attribute-based encryption. In CP-ABE system, each ciphertext is contains an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if and only if the key’s attribute set satisfies the access structure associated with a ciphertext.

Objective

1. The Main Concept of the project security which are provides by the Data Owner and Cloud Storage.
2. Authority are the only which are crated key with particular key usual Data owner are upload file to cloud that time encryption key are generated and Cloud are stored the file into cloud and they are available to decryption.
3. Data user or Data Consumer are want to key they are send to request for key and Authority are view all request given by Data user and send key to mail. And then data consumer is receiver the key are they are used it and downloads the file.

II. LITERATURE SURVEY

Number	Paper Name	Author Name	Proposed System	Referred Point
1.	Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems	JunbeomHur and Dong Kun Noh.	In this paper,propose an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability.	In this Paper, we referred the solution attribute-based encryption and selective group key distribution in each attribute group.
2.	Privacy-preserving decentralized key-policy attribute-based Encryption	J. Han, W. Susilo, Y. Mu, and J. Yan.	In this paper, propose a privacy-preserving decentralized key-policy ABE scheme where each authority can issue secret keys to a user independently without knowing anything about his GID.	In this Paper, we referred the solution the first decentralized ABE scheme with privacy-preserving based on standard complexity assumptions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

3.	Securely outsourcing attribute-based encryption with check ability	J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang.	This paper propose an outsourced ABE construction which provides check ability of the outsourced computation results in an efficient way. ExtensiveSecurity and performance analysis show that the proposed schemes are proven secure and practical.	In this Paper, we referred the solution ABE with verifiable delegation. Since the introduction of ABE, there have been advances in multiple directions.
4.	A new paradigm of hybrid encryption scheme	K. Kurosawa and Y. Desmedt.	In this paper, we show that a key encapsulation mechanism (KEM) does not have to be IND-CCA secure in the construction of hybrid encryption schemes, as was previously believed	In this Paper, we have referred the solution to develop the KEM/DEM model for hybrid encryption.
5.	A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack	R. Cramer and V. Shoup.	A new public key cryptosystem is proposed and analyzed. The scheme is quite practical, and is provably secure against adaptive chosenciphertext attack under standard intractability assumptions.	In this paper, we have referred the solution to present and analyze a new public key cryptosystem that is provably secure against adaptive chosen ciphertext attack
6.	Attribute-based encryption with verifiable outsourced decryption	J. Lai, R. H. Deng, C. Guan, and J. Weng.	In this Paper we proposed ABE system with outsourced decryption largely eliminates the decryption overhead of server. In such system, the proxy server such as cloud service provider is present which has a transformation key	In this Paper , we referred the solution to the cloud servers can offer various data services, such as outsourced delegation computation.
7.	Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization	B. Waters.	In this Paper, we proposed the solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system.	In this Paper, we referred the solution to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers.
8.	Decentralizing attribute-based encryption	A. Lewko and B. Waters.	In this Paper, We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters.	In this Paper, we referred the solution to ABE authority by creating a public key and issuing private keys to different users that reflect their attributes.
9.	How to delegate and verify in public: Verifiable computation from attribute-based	B. Parno, M. Raykova, and V. Vaikuntanathan.	In this Paper, we Proposed the public delegation and public verifiability, which have important applications in many practical delegation scenarios	In this Paper , we referred the solution the verifiability of delegation on dishonest cloud

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

	encryption			servers.
10.	Outsourcing the decryption of ABE Ciphertexts.	M. Green, S. Hohenberger, and B. Waters.	In this Paper, we propose a new paradigm for ABE that largely eliminates this overhead for users.	In this Paper, we referred the solution the cloud servers can offer various data services and outsourced delegation computation.

III. EXISTING SYSTEM

In existing system, the attribute-based encryption technique was used. But this scheme contains some problems and questions regarding to related works. Like during the delegation or release the cloud servers could misrepresent or replace the delegated cipher text and respond a fake result with malevolent intent. For the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible enough as well during the encryption.

Disadvantage of Existing System-

1. No guarantee that the calculated result returned by the cloud is always correct.
2. The cloud server may build ciphertext or fraud the eligible user that he even does not have permissions to decryption.

\

IV. PROPOSED SYSTEM

The work of delegation is promising but inevitably suffersfrom two problems.

1. The cloud server might tamperor replace the data owner's original ciphertext for maliciousattacks, and then respond a false transformed ciphertext.
2. The cloud server might cheat the authorized user for costsaving.

Though the servers could not respond a correcttransformed ciphertext to an unauthorized user, he couldcheat an authorized one that he/she is not eligible.The proposed system, design a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. In this scheme the circuits are used which express the strongest form of access control policy. On the other side, this scheme can be useful over the integers. As well as during the delegation computing, a user could validate whether the cloud server responds a correct transformed ciphertext to help him/her decrypt the ciphertext immediately and correctly.

During the deployments of the storage and delegation services, the main requirements of this research are

1) Confidentiality

(Indistinguishability under selective chosen plaintext attacks (IND-CPA)). With the storage service provided by the cloud server, the outsourced data should not be leaked even if malware or hackers infiltrate the server. Besides, the unauthorized users without enough attributes to satisfy the access policy could not access the plaintext of the data. Furthermore, the unauthorized access from the untrusted server who obtains an extra transformation key should be prevented.

2) Verifiability

During the delegation computing, a user could validate whether the cloud server responds a correct transformed ciphertext to help him/her decrypt the ciphertext immediately and correctly. Namely, the cloud servercould not respond a false transformed ciphertext or cheat the authorized user that he/she is unauthorized.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

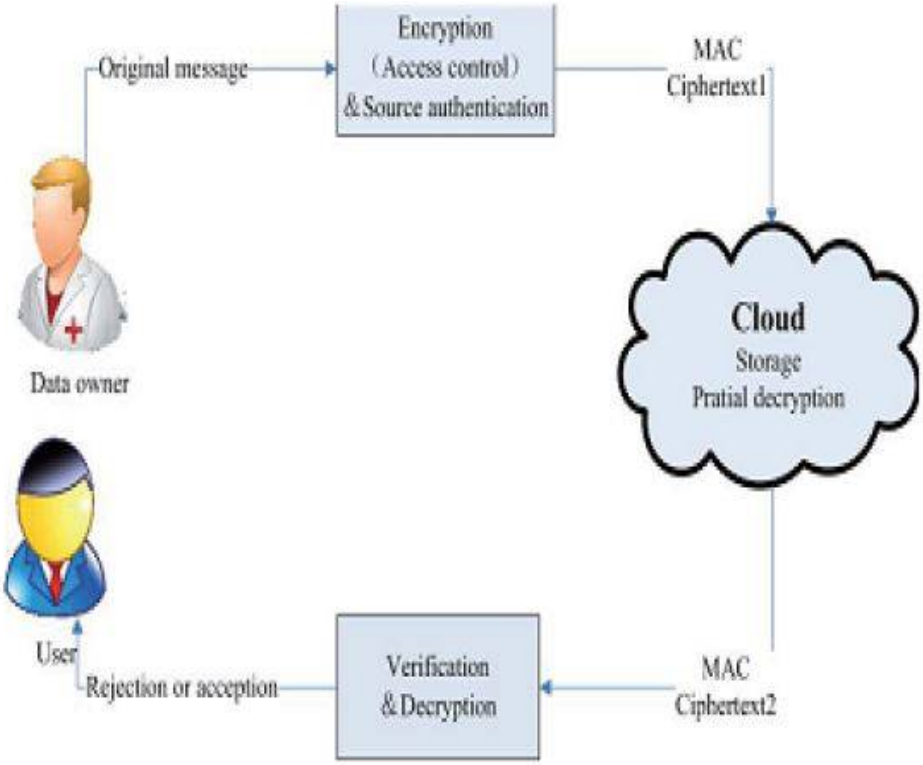

Fig1 : System Architecture

The system contains four modules,

1) Owner
2) User
3) Authority
4) Cloud Server

Owner: Owner is responsible to upload the data and assign the attribute to data and create the access structure.
Authority: Authority is responsible to generate keys, which are public key, private key, Master key and Transformation key. Public key is used by owner to encrypt the data. Master key is kept secret. Transformation key is used by Cloud server to partially decrypt the cipher text. Private Key is used by user to verify and decrypt the data.
User: User is responsible to access the data.
Cloud Server: Cloud server is responsible to provide storage space and partially decrypt the data when user wants to access.

Advantage of Proposed System-

1. The generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length.
2. Gives guarantee for correctness of the original ciphertext by using a commitment.
3. Achieves security, confidentiality as well as access control

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

V. ALGORITHMS OF EXISTING SYSTEM

Existing system includes following algorithms:

Linear Secret Sharing Schemes

A secret-sharing scheme over a set of parties P is called linear (over Z_p) if

1. The shares for each party form a vector over Z_p.
2. There exists a matrix an M with ` rows and n columns called the share-generating matrix For all i = 1….l the i'th row of M we let the function p denoted the party labeling row i as p(i). When we consider the column vector v = (s, r_2…. r_n), where s € $Z_p$is the secret to be shared, and r_2…. r_n€ Z_p are randomly chosen, then M v is the vector of l shares of the secret s according to . The share $(M v)_i$ belongs to party p(i).

It is shown in that every linear secret sharing-scheme according to the above definition also enjoys the linear reconstruction property, defined as follows:

Suppose that is an LSSS for the access structure A. Let S € A be any authorized set, and let I C {1, 2…..l } be defined as I = { i ,p(i) € S}. Then, there exist constants { w_i€ Z_p} $_{i \in I}$ such that, if { λ_i} are valid shares of any secrete.

VI. CONCLUSION

Design a secure circuit ciphertext-policy attribute-based encryption scheme. The universal circuits are helpful to achieve or clear the strongest form of entrée manage strategy In this scheme each ciphertext is contains an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if and only if the key's attribute set satisfies the access structure associated with a ciphertext. In this system when owner uploads the data, the data is store on private cloud and if storage space of private cloud exceeds then automatically data will be store on public cloud. The k-multilinear Decisional Diffie-Hellman assumption proves the proposed scheme is secure. On the other side, this scheme can use over the integers. The conclusion show that the method is sensible in the cloud computing. Thus, can be able to achieve data privacy, the fine-grained entrée manages and the demonstrable allocation in cloud. Our future work will be we can achieve more security by creating secure hardware device.

REFERENCES

[1]JunbeomHur and Dong Kun Noh," Attribute-Based Access Control with EfficientRevocation in Data Outsourcing Systems", VOL. 22, NO.7, JULY 2011 IEEE.
[2] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. ParallelDistrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.
[3] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013.
[4] K. Kurosawa and Y. Desmedt, "A new paradigm of hybridencryption scheme," in Proc. 24th Int. Cryptol. Conf., 2004, pp. 426–442.
[5] R. Cramer and V. Shoup, "A practical public key cryptosystemprovably secure against adaptive chosen ciphertext attack," inProc.18th Int. Cryptol. Conf., 1998, pp. 13–25.
[6] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryptionwith verifiable outsourced decryption," IEEE Trans. Inf. ForensicsSecur., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[7] B. Waters, "Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization," in Proc.14th Int. Conf. Practice Theory Public Key Cryptography. Conf. PublicKey Cryptography., 2011, pp. 53–70.
[8] A. Lewko and B. Waters, "Decentralizing attribute-basedencryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph.Techn. 2011, pp. 568–588.
[9] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegateand verify in public: Verifiable computation from attribute-basedencryption," in Proc. 9th Int. Conf. Theory Cryptograph., 2012,pp. 422–439.
[10] M. Green, S. Hohenberger, and B. Waters, "Outsourcing thedecryption of ABE Ciphertexts," in Proc. USENIX Security Symp, San Francisco, CA, USA, 2011, p. 34.