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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing

Vishal Pachangane[1], Prof. Priti Gode[2]

M. E Student, Dept of Computer Engineering, Alard College of Engineering and Management, Savitribai Phule Pune University, Pune, India [1]

Dept of Computer Engineering, Alard College of Engineering and Management, Savitribai Phule Pune University, Pune, India [2]

ABSTRACT: In the cloud, for achieving access control and data security, the data owners could uses attribute-based encryption to encrypt the stored data. To reduce the cost, the userswhich has 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 hybrid encryption with verifiable delegation has been developed. This system is mixed with verifiable computation and encrypt-then-Mac mechanism, the data confidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time. As well as this scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, this scheme achieves feasibilityas well as efficiency.

KEYWORDS: Ciphertext-policy attribute-based encryption, circuits, verifiable delegation, multi linear map, hybrid encryption.

I. INTRODUCTION

Cloud computing is innovation which uses advanced computational power as well as 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 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertextif and only if the key's attribute set satisfies the access structure associated with a ciphertext. The cloud server provides another service which is delegation computing.The VD-CPABE schemeshows that the untrusted cloud will not be able to learn anything about the encrypted message and build the original ciphertext.

II. PROBLEM STATEMENT

The cloud server is able to replace 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. In suchscheme,the access policies may not be flexible during the encryption.

III. EXISTING SYSTEM

In existing system,the attribute-based encryptiontechnique was used. But this scheme contains some problems and questions regarding to related works. Like during the delegation or releasethe 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:-

- No guarantee that the calculated result returned by the cloud is always correct.
- The cloud server may buildciphertext or fraud the eligible user that he even does not have permissions to decryption.
- Loss the data security, confidentiality as well as access control.

IV. PROPOSED SYSTEM

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. The k-multilinear Decisional Diffie-Hellman assumption proves the proposed scheme is secure. 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.

Advantage of Proposed System:-

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

V. LITERATURE SURVEY

Number	Paper Name	Author Name	Proposed System	Referred Point
1.	Attribute-Based Access Control with EfficientRevocation 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 withefficient attribute and user revocation capability.	In this Paper, we referred the solutionattribute-based encryption and selective group key distribution in each attribute group.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

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 secretkeys 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 standardcomplexity assumptions.
3.	Securely outsourcing attribute-based encryption with checkability	J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang.	This paper proposes anoutsourced ABE construction which providescheckability of the outsourced computation results in an efficient way. Extensive Security 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 hybridencryption 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 cryptosystemprovably 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

6.	Attribute-based encryptionwith 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 canoffer various data services, such as outsourced delegation computation.
7.	Ciphertext-policy attribute-based encryption: Anexpressive, 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-basedencryption	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 delegateand verify in public: Verifiable computation from attribute-basedencryption	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 servers.
10.	Outsourcing thedecryption 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

VI. SYSTEM ARCHITECTURE

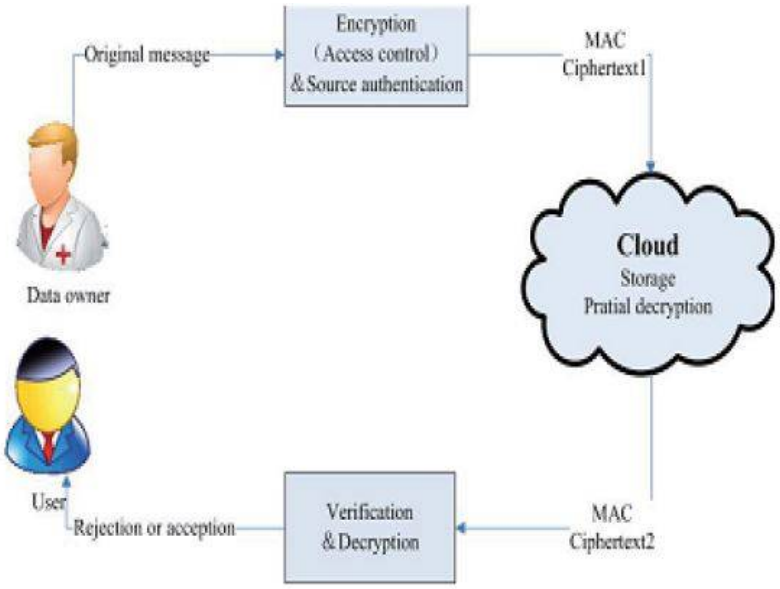

Fig. System Architecture

The system contains four modules,

1. Cloud Storage Module
2. Data Owner Module
3. Data User Module
4. Authority Module

Cloud Storage:
Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data.

Data Owner:
The data owner encrypts his message under access policy, then computes the complement circuit, which outputs the opposite bit of the output of f, and encrypts a random element R of the same length to under the policy

Data User:
The users can outsource their complex access control policy decision and part process of decryption to the cloud. Which extended encryption ensures that the users can obtain either the message M or the random element R, which avoids the scenario when the cloud server deceives the users that they are not satisfied to the access policy, however, they meet the access policy actually.

Authority:
Authority generates private keys for the data owner and user.

VII. CONCLUSION

Design a circuit ciphertext-policy attribute-based hybrid encryption with provable allocation method. The universal circuits are helpful to achieve or clear the strongest form of entrée manage strategy. Collective provable calculation and encrypt-then-Mac system with our ciphertext policy attribute-based hybrid encryption, we could assign the provable fractional decryption paradigm to the cloud server. The k-multilinear Decisional Diffie-Hellman assumption proves the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

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.

REFERENCES

[1]JunbeomHur and Dong Kun Noh," Attribute-Based Access Control with Efficient Revocation 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. PublicKeyCryptography., 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.