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. 4, Issue 12, December 2016

Cipher Text-Policy Attribute-Based Encryption in Cloud Computing for Data Sharing

Deepika P. Pachpute, Prof.Vina M. Lomte.

M.E., Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India

Head of Department, Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. For instance, during the delegation, the cloud servers could tamper or replace the delegated cipher text and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. In this paper, we revisit attribute-based data sharing scheme in order to solvethe key escrow issue but also improve the expressiveness of attribute, so that the resulting scheme is more friendly to cloud computing applications. We propose an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually.

KEYWORDS: Secure data sharing, attribute-based encryption,removing escrow, weighted attribute, cloud computing.

I. INTRODUCTION

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. Ciphertext-policy attribute-based encryption (CP-ABE) has turned to be an important encryption technology to tackle the challenge of secure data sharing. In a CP-ABE, user's secret key is described by an attribute set, and ciphertext is associated with an access structure. DO is allowed to define access structure over the universe of attributes. A user can decrypt a given ciphertext only if his/her attribute set matches the access structure over the ciphertext. In this paper, the weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but also to simplify access policy. Thus, the storage cost and encryption cost for a ciphertext can be relieved. We use the following example to further illustrate our approach.

II. LITERATURE SURVEY

1) Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems

In this paper,we 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

In this paper, we 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

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. 4, Issue 12, December 2016

Complexity assumptions

3) Securely outsourcing attribute-based encryption with check ability

ABE, there have been advances in multiple directions.

4) A new paradigm of hybrid encryption scheme

In this paper, we show that a key encapsulation mechanism (KEM) does not have to be IND-CCA secure in the construction of hybrid

We 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.

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

A new public key cryptosystem is proposed and analyzed. The

Scheme is quite practical, and is provably secure against adaptive.

III. EXISTING SYSTEM

Owner saves his data on cloud.The cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well.

Disadvantages of Existing System:

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

IV. PROPOSED SYSTEM

We propose an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. Moreover, we introduce the concept of attribute with weight, being provided to enhance the expression of attribute, which can not only extend the expression from binary to arbitrary state, but also lighten the complexity of access policy.

In this system we design an attribute-based data sharing scheme in cloud computing. The improved key issuing protocol was presented to resolve the key escrow problem. It enhances data confidentiality and privacy in cloud system against the managers of KA and CSP as well as malicious system outsiders, where KA and CSP are semi-trusted. In addition, the weighted attribute was proposed to improve the expression of attribute, which can not only describe arbitrary state attributes, but also reduce the complexity of access policy, so that the storage cost of cipher text and time cost in encryption can be saved.

Advantages of Proposed System:

1. Data stored on cloud will not temper.
2. Authenticated user can only access data.

V. CONCLUSION

In this system we design an attribute-based data sharing scheme in cloud computing. The improved key issuing protocol was presented to resolve the key escrow problem. It enhances data confidentiality and privacy in cloud system against the managers of KA and CSP as well as malicious system outsiders, where KA and CSP are semi-trusted. In addition, the weighted attribute was proposed to improve the expression of attribute, which can not only describe arbitrary state attributes, but also reduce the complexity of access policy, so that the storage cost of ciphertext and time cost in encryption can be saved. Finally, we presented the performance and security analyses for the proposed scheme, in which the results demonstrate high efficiency and security of our scheme. In future system Contain 2FA Concept

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. 4, Issue 12, December 2016

one for user password and one given OTP.If Certain condition Cloud are full due to the all file so Time complexity and Space complexity large due to increase the Space complexity. if any file contain larger than 24hour then they are automatically move to private Cloud to the public 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. Parallel Distrib. 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. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013.
[4] K. Kurosawa and Y. Desmedt, "A new paradigm of hybrid encryption scheme," in Proc. 24th Int. Cryptol. Conf., 2004, pp. 426–442.
[5] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in Proc. 18th Int. Cryptol. Conf., 1998, pp. 13–25.
[6] 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.
[7] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography. Conf. Public Key Cryptography., 2011, pp. 53–70.
[8] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. 30th Annu.Int. Conf. Theory Appl. Cryptograph.Techn., 2011, pp. 568–588.
[9] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption," in Proc. 9th Int. Conf. Theory Cryptograph., 2012, pp. 422–439.
[10] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE Ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011, p. 34.