MANTECH Publications
Recent Trends in Computer Science and Software Technology
Volume 2, Issue 2, May-August 2017

A Secure Delegation Process using AND-OR circuit in Cloud Computing

Deepika P. Pachpute[1], Vina M. Lomte[2]
Student[1], HOD[2]
Department of Computer Science and Engineering
RMDSSOE, Pune, India
Corresponding Author's Email: *dpachpute6@gmail.com[1]*

Abstract

In the cloud, for achieving access management and keeping information confidential, the information the information house owners might adopt attribute -based encoding to encode the keep data. Users with restricted computing power are but a lot of possible to delegate the mask of the decoding task to the cloud servers to cut back the computing value. As a result, attribute -based encoding with delegation emerges. Still, there are caveats and queries remaining within the previous relevant works. As an example, throughout the delegation, the cloud servers might tamper or replace the delegated cipher text and respond a cast computing result with malicious intent. They will additionally cheat the eligible users by responding them that they're ineligible for the aim of value saving. What is more, throughout the encoding, the access policies might not be versatile enough likewise. Since policy for general circuits allows realizing the strongest variety of access management, a construction for realizing circuit cipher text-policy attribute-based hybrid encoding with verifiable delegation has been thought of in our work. In such a system, combined with verifiable computation and encrypt -then-mac mechanism, the information confidentiality, the fine-grained access management and also the correctness of the delegated computing results are well bonded at identical time.

Keywords: *Cipher text-policy attribute-based encryption, circuits, verifiable delegation, multi linear map, hybrid encryption*

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. 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.

LITERATURE SURVEY

Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems in this paper, it proposes an access control mechanism using cipher text-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. Privacy-preserving decentralized key-policy attribute-based Encryption. In this paper, in this system 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, it referred the solution the first decentralized ABE scheme with privacy-preserving based on standard.

Securely outsourcing attribute-based encryption with check ability ABE construction which provides check ability 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.

EXISTINGSYSTEM

The cloud servers could replace the delegated cipher text and respond a forged computing result with malicious intent. They may also cheat the suitable 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

1. There is no guarantee that the calculated result returned by the cloud is always correct.

2. The cloud server may forge cipher text or cheat the eligible user that he even does not have permissions to decryption.

PROPOSED SYSTEM

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. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.

Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, combined 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 same time.

Advantages of Proposed System:

1. Our scheme achieves security against chosen-plaintext attacks under the k-multi linear Decisional Diffie-Hellman assumption.

Table: 1

Type Size(pts.)	Execution	Time	Time
1	Average execution time for data owner	Low	High
2	Average execution time for Cloud Server	Low	High
3	Average execution time for User	Null	Null

1.1 Mathematical Model

Let us consider S as a system for CONCEPT BASED CIPHERTEXT.

S= {……

INPUT:

- Identify the inputs

F= {f_1, f_2, f_3 …..,f_n| 'F' as set of functions to execute commands.}

I= {i_1, i_2, i_3…|'I' sets of inputs to the function set}

O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets}

S= {I, F, O}

I = {Data submitted by the Owner, ...}

O = {Output of desired data,...}

F = {Functions implemented to get the output}

CONCLUSION

To the best of our knowledge, we initially here a circuit cipher text-policy attribute-based hybrid encryption with provable allocation method. Universal circuits are helpful to articulate the strongest form of entrée manage strategy. Collective provable calculation and encrypt-then-Mac system with our cipher text policy attribute-based hybrid encryption, it could hand over the provable fractional decryption paradigm to the cloud server. Within calculation, the proposed system is established to be safe based on k-multi linear Decisional Diffie-Hellman supposition.

On the other hand, to execute scheme above in the integers the expenses of the

calculation and announcement expenditure show that the method is sensible in the cloud computing. Thus, we could be relevant it to create confident the data privacy, the fine-grained entrée manages and the demonstrable allocation in cloud.

ACKNOWLEDGEMENT

I take this chance to express my appreciation to my guide and head of department, Prof. V. M. Lomte, Department of Computer Engineering, RMDSSOE, for their kind cooperation and guidance during the entire research work. I would also like to thank our, Principal and Management for providing lab and other facilities.

REFERENCES

1) Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin "Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing"IEEE transactions on parallel and distributed systems, vol. 27, NO. 1, JANUARY 2016.

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.

11) Junbeom Hur and Dong Kun Noh," Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", VOL. 22, NO. 7, JULY 2011 IEEE.