International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.06,Issue.29
September-2017,
Pages:5725-5728

www.ijsetr.com

Secure Share Data KP_ABE with Third Party Verification in Cloud Computing

K. HARISH[1], G. LAKSHMI NARAYANA

[1]PG Scholar, Dept of CSE, Annamacharya Institute of Technology & Sciences, Tirupathi, AP, India,
Email: khnr.it@gmail.com.

[2]Assistant Professor, Dept of CSE, Annamacharya Institute of Technology & Sciences, Tirupathi, AP, India,
Email: laxminarayana0526@gmail.com.

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. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, 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. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit Secure Share Data KP_ABE with Third Party Verification 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. Besides, our scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.

Keywords: KP_ABE, VD-CPABE, Ciphertext, Cloud Servers.

I. INTRODUCTION

The emergence of cloud computing brings a revolutionary innovation to the management of the data resources. Within these computing environments, the cloud servers can offer various data services, such as remote data storage [1] and outsourced delegation computation [2], [3], etc. For data storage, the servers store a large amount of shared data, which could be accessed by authorized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user's demands. As applications move to cloud computing platforms, ciphertext-policy attribute-based encryption (CP-ABE) [4], [5] and verifiable delegation (VD) [6], [7] are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers. There are two complementary forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) [8], [9], [10], and the other is ciphertext-policy attribute-based encryption. In a KP-ABE system, the decision of access policy is made by the key distributor instead of the encipherer, which limits the practicability and usability for the system in practical applications. On the contrary, in a CP-ABE system, each ciphertext is associated with an access structure, and each private key is labeled with a set of descriptive attributes[11]. A user is able to decrypt a cipher-text if the key's attribute set satisfies the access structure associated with a ciphertext.

Apparently, this system is conceptually closer to traditional access control methods. On the other hand, in a ABE system, the access policy for general circuits could be regarded as the strongest form of the policy expression that circuits can express any program of fixed running time. Delegation computing is another main service provided by the cloud servers. In the above scenario, the healthcare organizations store data files in the cloud by using CP-ABE under certain access policies. The users, who want to access the data files, choose not to handle the complex process of decryption locally due to limited resources. Instead, they are most likely to outsource part of the decryption process to the cloud server. While the untrusted cloud servers who can translate the original ciphertext into a simple one could learn nothing about the plaintext from the delegation. The work of delegation is promising but inevitably suffers from two problems. a) The cloud server might tamper or replace the data owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext. b) The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed ciphertext to an unauthorized user, he could cheat an authorized one that he/she is not eligible. Further, during the deployments of the storage and delegation services, the main requirements of this research are presented as follows.

Confidentiality: (Indistinguishability under selective chosen plaintext attacks (IND-CPA))[12]. With the storage ser-vice 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.

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

Thus, in this paper, we will attempt to refine the definition of CP-ABE with verifiable delegation in the cloud to consider the data confidentiality, the fine-grained data access control and the verifiability of the delegation. The related security definition and IND-CPA security game used in the proof are presented in Section 3.2 to depict the above attacks of the adversaries.

II. EXISTING SYSTEM

Sahai and Waters proposed the notion of attribute-based encryption (ABE). In subsequent works, they focused on policies across multiple authorities and the issue of what expressions they could achieve. Up until recently, Sahai and Waters raised a construction for realizing KP-ABE for general circuits. Prior to this method, the strongest form of expression is Boolean formulas in ABE systems, which is still a far cry from being able to express access control in the form of any program or circuit. Cramer and Shoup proposed the generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length. Based on their ingenious work, a one-time MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption. Such improved model has the advantage of achieving higher security requirements. Green et al. designed the first ABE with outsourced decryption scheme to reduce the computation cost during decryption. After that, Lai et al. proposed the definition of ABE with verifiable outsourced decryption. They seek to guarantee the correctness of the original ciphertext by using a commitment. However, since the data owner generates a commitment without any secret value about his identity, the untrusted server can then forge a commitment for a message he chooses. Thus the ciphertext relating to the message is at risk of being tampered.

Disadvantages of Existing System:

It has two main problems: The first one is their have no construction for realizing CP-ABE for general circuits, which is conceptually closer to traditional access control. The other is related to the efficiency, since the exiting circuit ABE scheme is just a bit encryption one. Thus, it is apparently still remains a pivotal open problem to design an efficient circuit CP-ABE scheme.

For the main efficiency drawbacks of ABE, previous constructions provided an agile method to outsource the most overhead of decryption to the cloud. However, there is no guarantee that the calculated result returned by the cloud is always correct. The cloud server may forge ciphertext or cheat the eligible user that he even does not have permissions to decryption.

III. PROPOSED SYSTEM

Prompted by the requirements in the cloud, we modify the model of CP-ABE with verifiable delegation and present a concrete construction to realize Secure Share Data KP_ABE with Third Party Verification in Cloud Computing (VD-CPABE). To keep data private and achieve fine grain access control, our starting point is a circuit key-policy attribute-based encryption proposed by Sahai and Waters. We give the anti-collusion circuit CP-ABE construction in this paper for the reason that CP-ABE is conceptually closer to the traditional access control methods. To validate the correctness, we extend the CP-ABE ciphertext into the attribute-based ciphertext for two complementary policies and add a MAC for each ciphertext, so that whether the user has permissions he/she could obtain a privately verified key to verify the correctness of the delegation and prevent from counterfeiting of the ciphertext. Aiming at further improving the efficiency and providing intuitive description of the security proof, the conception of hybrid encryption is also introduced in this work. Besides, security of the VD-CPABE system ensures that the untrusted cloud will not be able to learn anything about the encrypted message and forge the original ciphertext. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, 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. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit Secure Share Data KP_ABE with Third Party Verification 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.

A. Advantages of Proposed System

Our proposed scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.

B. System Modules

1. Data Owner and User Registration & Login
2. Key Generation

3. Encrypt & Upload
4. Download, Decrypt & Verify

TABLE 1. Role Description

Role	Description
Authority	Attribute key generator centre (trusted third party)
Data owner	Encrypting party who uploads his encrypted data to the cloud
User	Decrypting party who outsources the most overhead computation to the cloud
Cloud server	The party who provides storage and outsourced computation services

IV. MODULES DESCRIPTION

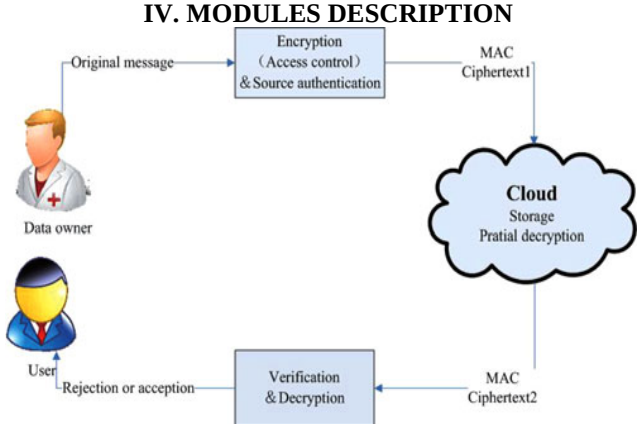

Fig.1. Medical data sharing system.

A. Data Owner and User Registration & Login

In this module, Data Owner and User Register with cloud server using his username, password, name and mobile number for upload file. Then Data Owner and Users can login with his user name and password then access the cloud server.

B. Key Generation

In this module, data owner send key request to Authority (Attribute key generator center), which is an entity for key generation. The authority is supposed to be the only party that is fully trusted by all participants. Then authority login and view key request details. Then choose any data owner and generate keys for this data owner. Finally he will send keys to Data owner.

C. Encrypt & Upload

In this module, data owner browse any file, then encrypt it. Here we use a circuit ciphertext-policy attribute-based encryption scheme, a symmetric encryption scheme and an encrypt-then-Mac mechanism are applied to ensure the confidentiality, the fine-grained access control and the verifiable delegation. Then upload these ciphertext to cloud server.

D. Download, Decrypt and Verify

In this module, user wants to download a file from cloud server, so he got transformation key from Authority. Then he will forward the download request to cloud server. Cloud Server partially decrypts uploaded file using users transformation key and forward partially decrypted content to user. Finally user decrypt this partially decrypted content and access that file then verify this file is safe or not.

V. CONCLUSION

To the best of our knowledge, we firstly present a circuit Secure Share Data KP_ABE with Third Party Verification with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-Mac mechanism with our Secure Share Data KP_ABE with Third Party Verification, we could delegate the verifiable partial decryption paradigm to the cloud server. In addition, the proposed scheme is proven to be secure based on k-multilinear 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.

VI. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Kon-winski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaha-ria, "Above the clouds: A berkeley view of cloud computing," Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

[2] 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.

[3]E.gayatri, N.Lakshmi chaitanya,V.SyamaSudha published "Quality Assurance Of Links In Wireless Sensor Networks By Using Code Dissemination" in International Journal of Modern Trends in Engineering and Research, Volume 2, Issue, 7 ,p.no 260-265,July- 2015.

[4] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryp-tion with verifiable outsourced decryption," IEEE Trans. Inf. Foren-sics Secur., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2011, 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. 53–70.

[7] S. Yamada, N. Attrapadung, and B. Santoso, "Verifiable predicate encryption and applications to CCA security and anonymous predicate authentication," in Proc. Int. Conf. Practice Theory Public Key Cryptograph. Conf. Public Key Cryptograph., 2012, pp. 243–261.

[8] V.Syamasudha,G.HariPrasad published "Implementation Of Dbrain Search Algorithm On Page Clustring" in International Journal of Emerging Trends & Technology in Computer Science, Volume 1, Issue 3,p. no 194-198, September – October 2012.

[9] J.Han, W.Susilo, Y. Mu, and J. Yan, "Privacy-preserving decen-tralized key-policy attribute-based Encryption," IEEE Trans. Paral-lel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.
[10] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute-based encryption for circuits from multilinear maps," in Proc. 33rd Int. Cryptol. Conf., 2013, pp. 479–499.
[11] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," in Proc. 45th Annu. ACM Symp. Theory Comput., 2013, pp. 545–554.
[12] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2005,457–473

Author's Profile:

K.Harish did his Bachelor of Technology in Information Technology & Engineering at Narayana Engineering College, Gudur and doing Master of Technology in Computer Science & Engineering at Annamacharya Institute Of Technology & Sciences, Tirupathi, Karakambadi, Tirupathi, Chittoor, Andhra Pradesh, India.

G.Lakshmi Narayana did his Bachelor of Technology in Computer Science & Engineering at Narayana Engineering College, Nellore and did Master of Technology in Computer Science & Engineering at SV University College of Engineering, Tirupati. Presently doing Ph.D. in SV University, College of Engineering, Tirupathi, Chittoor, and Andhra Pradesh, India.