RESEARCH ARTICLE OPEN ACCESS

Secured Authorized Data Using Hybrid Encryption in Cloud Computing

Dinesh Shinde[1], Harsh Mathur[2]
[1]*Mtech CSE, IITM Bhopal,M.P.,India*
[2]*Asst. Professor CSE,IITM Bhopal,M.P.,India*

ABSTRACT
In today's world to provide a security to a public network like a cloud network is become a toughest task however more likely to reduce the cost at the time of providing security using cryptographic technique 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 to solution to all problems 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. 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. 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. 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 cipher text-policy attribute-based encryption. In a KP-ABE system, the decision of access policy is made by the key distributor instead of the enciphered, which limits the practicability and usability for the system in practical applicationsthe 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.

Keywords: Cipher text-policy attribute-based encryption, circuits, verifiable delegation, multilinear map, hybrid encryption

I. INTRODUCTION

THE necessity of cloud computing makes a revolutionary innovation to the management of the data resources. Within this computing atmosphere, 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, cipher text-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

II. EXSISTING SYSTEM

The cloud servers could replace the delegated cipher text and respond to unauthorized computing result with malicious material. 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.

III. PRAPOSED SYSTEM

Praposed method is proven to be secured which is based on k-multilinear Decisional Diffie-Hellman assumption. The costs of the computation and communication consumption show that the method 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.

IV. LITERATURE SURVEY

Attribute-based encryption.Sahai and Waters [11] proposedthe notion of attribute-based encryption (ABE). In subsequent works [8], [12], they focused on policies across multi-ple authorities and the issue of whatexpressions they couldachieve. Up until recently, Sahai and Waters [9] raised aconstruction for realizing KP-ABE for general circuits. Priorto this method, the strongest form of expression is Boolean formulas in ABE systems, which is still a far cry from beingable to express access control in the form of any program orcircuit. Actually, there still remain two problems. The firstone is their have no construction for realizing CP-ABE forgeneral circuits, which is conceptually closer to traditionalaccess control. The other is related to the efficiency, sincethe exiting circuit ABE scheme is just a bit encryption one.Thus, it is apparently still remains a pivotal open problemto design an efficient circuit CP-ABE scheme.Cramer and Shoup [13], [14] proposedthe generic key encapsulation mechanism (KEM)/DEMconstruction for hybrid encryption which can encrypt messages of arbitrary length. Based on their ingenious work, aone-time MAC were combined with symmetric encryptionto develop the KEM/DEM model for hybrid encryption

[15], [16], [17]. Such improved model has the advantage of achieving higher security requirements.*ABE* with verifiable delegation. Since the introduction of ABE, there has been advances in multiple directions. The application of outsourcing computation [18],is one of an important direction. Green et al. [2] designed the firstABE with outsourced decryption scheme to reduce the computation cost during decryption. After that, Lai et al.[3] proposed the definition of ABE with verifiable out-sourced decryption. They seek to guarantee the correctness of the original cipher text by using a commitment.

V. OUR TECHNIQUES

Verifiable delegation is used to protect authorized users from being deceived during the delegation. The data owner encrypts his message M under access policy f, then computes the complement circuit f, which outputs the opposite bit of the output of f, and encrypts a random element R of the same length to M under the policy f . The users can then outsource their complex access control policy decision and part process of decryption to the cloud. Such 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.

In CP-ABE we use a hybrid variant for two reasons: one is that the circuit ABE is a bit encryption, and the other is that the authentication of the delegated cipher textshould be guaranteed. The cipher text of the hybrid VD-CPABE system is divided into two components: the CP- ABE for circuit'sfandfmakes up the key encapsulationmechanism part, and a symmetric encryption plusthe encrypt-then-mac mechanism make up theauthenticated encryption mechanism (AE) part. EachKEM encrypts a random group element and then maps itvia key derivation functions into a symmetric encryptionkey**dk**and a one-time verified key**vk** .Then the random

Encryption key**dk**is used to encrypt the message of anylength.**Vk**and the data owner'sIDare used to verify theMAC of the cipher text. Only when the server dose notforge the original ciphertext and respond a correct partialdecrypted cipher text, the user could be able to properlyvalidate the MAC.

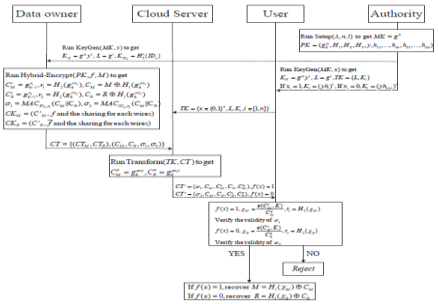

Figure: Our secure hybrid VD- CPABE scheme.

VI. CONCLUSION

To the best of our knowledge, we firstly present a circuit cipher text-policy attribute-based hybrid encryption 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 cipher text-policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. In addition, the proposed scheme is proven to be secured 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.

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 thedecryption of ABE Ciphertexts," inProc. USENIX Security Symp,San Francisco, CA, USA, 2011, p. 34.

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

[4] A. Lewko and B. Waters, "Decentralizing attribute-basedencryption," inProc. 30th Annu. Int. Conf. Theory Appl. Cryptograph.Techn., 2011, pp. 568–588.

[5] B. Waters, "Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization," inProc.14th Int. Conf. Practice Theory Public Key Cryptograph. Conf. PublicKey Cryptograph., 2011, pp. 53–70.

[6] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegateand verify in public: Verifiable computation from attribute-basedencryption," inProc. 9th Int. Conf. Theory Cryptograph., 2012, pp. 422–439.

[7] S. Yamada, N. Attrapadung, and B. Santoso, "Verifiable predicateencryption and applications to CCA security and anonymouspredicate authentication," inProc. Int. Conf. Practice Theory PublicKey Cryptograph.Conf. Public Key Cryptograph., 2012, pp. 243–261.

[8] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decen-tralized key-policy attribute-based Encryption,"IEEE Trans. Paral-lelDistrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[9] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute-based encryption for circuits from multilinear maps," inProc. 33rdInt. Cryptol. Conf., 2013, pp. 479–499.

[10] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-basedencryption for circuits," inProc. 45th Annu.ACM Symp.TheoryComput., 2013, pp. 545–554.

[11] A. Sahai and B. Waters, "Fuzzy identity based encryption," inProc. 30th Annu.Int. Conf. Theory Appl. Cryptograph.Techn., 2005,pp. 457–473.[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-basedEncryption for Fine-grained access control of encrypted data," inProc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[12] 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.

[13] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertextattack," SIAM J. Compute vol. 33, no. 1, pp. 167–226, 2004.

[14] D. Hofheinz and E. Kiltz R, "Secure hybrid encryption from weak-ened key encapsulation," inProc. 27th Int. Cryptol. Conf., 2007,pp. 553–571.

[15] M. Abe, R. Gennaro, and K. Kurosawa, "Tag-KEM/DEM:A newframework for hybrid encryption," inProc. 28th Int. Cryptol. Conf.2008, pp. 97–130.

[16] K. Kurosawa and Y. Desmedt, "A new paradigm of hybridencryption scheme," in Proc. 24th Int. Cryptol. Conf., 2004, pp. 426–442.

[17] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcingattribute-based encryption with checkability,"IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013