International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 5th Dec 2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-12

Title : CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION AND MULTI LINEAR MAP IN CLOUD COMPUTING

Volume 06, Issue 12, Pages: 92–96.

Paper Authors

M MADHAVA, M VENKATESH NAIK , M VENKATESH NAIK

CRIT , Anantapur

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION AND MULTI LINEAR MAP IN CLOUD COMPUTING

M MADHAVA[1], M VENKATESH NAIK [2], M VENKATESH NAIK [3]

[1]PG Scholar, CSE Department, CRIT , Anantapur

[2] Asst Professor, CSE Department, CRIT , Anantapur

[3] Asst Professor ,CSE Department, CRIT , Anantapur

Abstarct

In the cloud, for achieving access management and keeping information confidential,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 ciphertext 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 to realize the strongest variety of access management, a construction for realizing circuit ciphertext-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. Besides, our theme achieves security against chosen-plaintext attacks beneath the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an intensive simulation campaign confirms the practicability and potency of the projected answer.

Keywords — Ciphertext-policy attribute-based encryption, Circuits, Verifiable delegation, Multilinear map, Hybrid encryption.

1. INTRODUCTION:

Cloud computing is novel processing system that is based on virtualization, parallel and distributed computing, utility processing, and service oriented architecture. In the past decades, distributed computing has developed as a standout amongst the most compelling ideal models in the IT business, and has pulled in broad consideration from both the academia and industry. Nonetheless, the individual client prerequisites might be differing and require diverse types of outsourced calculation, while current PVC plans support only a single structure. Customers might wish to demand estimations from a specific server or to issue a solicitation to a huge pool of servers.The access policy is totally in view of authorization relationship where the relationship is between user attributes and asset properties. The properties might be any data of the client's profession, work parts that is given and is utilized to concede the access. However, all together to outline an access strategy component there are numerous difficulties to conquer some of them are

(1) User can transfer any sort of information such as content, media etc.

(2) Any can give any number of attributes and thus two or more clients might have same characteristics.

(3) Any individual might fabulous any sort of access to any number of clients.

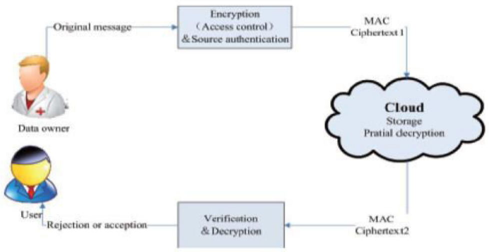
This methodology permits the client to actualize the access control on their information specifically in content sharing service instead of central administrator. To give an intricate access policy component, we require adaptable and versatile cryptographic key administration estimations. For enhancing these disservices, we are utilizing attribute based encryption. Subsequently, we employed CPABE (Cipher Text Policy schema – Attribute Based Encryption) method as a solution for the aforementioned problem. In CP-ABE, the beneficiary can unscramble the information just when the client attribute fulfill the access policy.

2 RELATED WORKS:

Outsourcing Decryption of Multi-Authority ABE Cipher texts Keying Li and Hue Ma 2013 The believed of multi-authority attribute established encryption was gave by Pursue in TCC 2007. In this paper, we enhance Chase's scheme to permit encryptions to ascertain how countless qualities are needed for every single ciphertext from connected attribute authorities. The counseled scheme can be perceived as a multi-trapdoor construction. Further-more, we apply the LMSSS to outsource the decryption of multi-authority attribute established encryption scheme for colossal universe. Also, the outsourcing scheme can be comprehended in the setting of multi-authority key-policy attribute established encryption. Both our schemes can be spread to RCCA safeguard ones. Attribute Instituted Encryption alongside Privacy Maintaining employing Asymmetric Key in Cloud Computing S.Sankareswar and S.Hemanth 2014 Symmetric key algorithm uses alike key for both encryption and decryption. The authors seize a centralized way whereas a solitary key allocation center (KDC) distributes hidden keys and qualities to all users. A new decentralized admission manipulation scheme for safeguard data storage in clouds that supports nameless authentication. The validity of the user who stores the data is additionally verified. The counseled scheme is to obscure the users qualities employing SHA algorithm .The Parlier cryptosystem, is a probabilistic asymmetric algorithm for area key cryptography. Parlier algorithm use for Conception of admission strategy, file accessing and file refubishing procedure and additionally obscuring the admission strategy to the user employing query established algorithm. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Safeguard Realization Brent Waters 2006 We present a new methodology for comprehending Ciphertext-Policy Attribute Encryption (CP-ABE) below concrete and non-interactive cryptographic assumptions in the average model. Our resolutions permit each encrypt or to enumerate admission manipulation in words of each admission formula above the qualities in the system. In our most effectual arrangement, ciphertext size, Encryption and decryption period scales linearly alongside the intricacy of the admission formula. The merely preceding work to accomplish these parameters was manipulated to a facts in the generic cluster model. We present three constructions inside our framework. Our arrangement is proven selectively safeguard below an assumption that we call the decisional Parallel Bilinear Die-Hellman Exponent (PBDHE) assumption that can be believed as a generalization of the BDHE assumption. Our subsequent two constructions furnish presentation transactions to accomplish provable protection suitably below the (weaker) decisional Bilinear-Di e-Hellman Exponent and decisional Bilinear Die-Hellman assumptions. How to Representative and Confirm in Public: Verifiable Computation from Attribute-based Encryption Bryan Par no Mariana Beam ova and Vend Vaikuntanathan 2011 The expansive collection of tiny, computationally frail mechanisms and the producing number of computationally intensive tasks makes it appealing to representative computation to data centers. Though, outsourcing computation is functional merely after the returned consequence can be trusted, which Makes verifiable computation (VC) a have to for such scenarios. In this work we spread the meaning of verifiable computation in two vital directions: area delegation and area verifiability, that have vital requests in countless useful delegation scenarios. Yet, continuing VC constructions established on average cryptographic assumptions flounder to accomplish these properties Cryptanalysis of the Multilinear Chart above the Integers Jung He Chon, Kyoohyung Han and Altering Lee 2014.We delineate a polynomial-time cryptanalysis of the (approximate) multilinker chart of Croon, Leporine and Debouche (CLT). The attack relies on an adaptation of the so-called zero sizing attack opposing the Garb, Gentry and Halve (GGH) candidate multilinear map. Zero sizing is far extra desecrating for CLT than for GGH. In the case of GGH, it permits to break generalizations of the Decision Linear and Subgroup Membership setbacks from pairing-based cryptography. For CLT, this leads to a finished break: all numbers meant to be retained hidden can be efficiently and openly recovered.

3.EXISTING SYSTEM

Existing system in every ciphertext is related to associate degree access structure, and every non-public secret is labeled with a group of descriptive attributes. A user is in a position to rewrite a ciphertext if the key’s attribute set satisfies the access structure related to a ciphertext. CP-ABE below sure access policies. The users, UN agency wish to access the information files, select to not handle the complicated method of decoding domestically as a result of restricted resources. Instead, they're presumably to source a part of the decoding method to the cloud server. whereas the untrusted cloud servers UN agency will translate the first ciphertext into a straightforward one may learn nothing concerning the plaintext from the delegation. whereas the untrusted cloud servers UN agency will translate the first ciphertext into a straightforward one may learn nothing concerning the plaintext from the delegation.



4. IMPLEMENTATION

a) Attribute Authority Authorities will need to give the key, according to the client's key solicitation. Each client’s solicitation must be raised to authority to get access key via mail. There are two correlative types of trait based encryption. One is key policy-attribute based encryption (KP-ABE) and the other is Ciphertext-Policy Schema based Attribute Encryption (CPSBAE). In a KP-ABE framework, the decision of access arrangement is made by the key merchant rather than the en-cipher, which constrains the practicability and ease of use for the framework in the practical applications. If the decryption is incorrect then that account will be blocked.The blocked account will get the access if the authority decide to give access to the particular account.

b) Cloud Server Cloud server will have access to the file which is transferred by the data proprietor. Cloud server needs to unscramble the documents accessible under their consent. Moreover, information user will need to unscramble the information to get to the first content by giving the particular key. File has been decoded effectively and accommodated for consumer. This process is done only after the cloud is login.

c) Data Owner: Information proprietor will need to enroll at first to access the profile. Information Owner will transfer the document to the cloud server in the scrambled arrangement Arbitrary encryption key era is going on while transferring the file to the cloud Scrambled record will be put away on the cloud . To upload the particular file owner should be login.

d) Data Consumer: Information consumer will at first request the key to the Authority to confirm and decode the file in the cloud. Information customer can get to the file in view of the key obtained from mail id. According to the key obtained to the consumer can check and unscramble the information from the cloud. To do this process the consumer should register in the cloud . To access the particular file consumer must be login.

5.CONCLUSION:

In this paper, we addressed an important issue of attribute revocation for attribute based systems. In particular, semi-trustable proxy servers are available, and proposed a scheme supporting user’s attribute revocation schema. A unique property of our proposed scheme is that it places minimal load on authority upon the events in user's revocation. We achieved this by uniquely combining the proxy re-encryption technique with CPSBAE and enabled the authority to delegate most laborious tasks to proxy servers. Our proposed scheme is provably secure against chosen cipher-text attacks. In addition, we also showed the applicability of our method to the KP-ABE scheme. An experimental design shows the effectiveness and efficiency of our proposed work.

6. REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," University of California, Berkeley, Technical Report, no. 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.

[3] J. Lai, R. H. Deng, C. Guan and J. Weng, "Attribute-Based Encryption with Verifiable Outsourced Decryption," in Proc. IEEE Transactions on information forensics and security, vol. 8, NO. 8, pp.1343-1354, 2013.

[4] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[5] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: an Expressive, Enficient, and Provably Secure Realization," in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.

[6] B. Parno, M. Raykova and V. Vaikuntanathan, "How to Delegate and Verify in Public: verifiable computation from attribute-based encryption," in Proc. TCC, pp.422-439, Springer-Verlag Berlin, Heidelberg, 2012.

[7] S. Yamada, N. Attrapadung and B. Santoso, "Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication," in Proc. PKC, pp.243-261, Springer- Verlag Berlin, Heidelberg, 2012.

[8] J. Han, W. Susilo, Y. Mu and J. Yan, "Privacy- Preserving Decentralized Key-Policy Attribute-Based Encryption," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012.

[9] S. Garg, C. Gentry, S. Halevi, A. Sahai and B. Waters, "Attribute-Based Encryption for Circuits from Multilinear Maps," in Proc. CRYPTO, pp.479- 499, Springer-Verlag Berlin, Heidelberg, 2013.

[10] S. Gorbunov, V. Vaikuntanathan and H. Wee, "Attribute-Based Encryption for Circuits," in Proc. STOC, pp.545-554, ACM New York, NY, USA, 2013.

[11] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption," in Proc. EUROCRYPT, pp.457-473, Springer-Verlag Berlin, Heidelberg, 2005.

[12] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for Fine-grained access control of encrypted data," in Proc. CCS, pp.89-98, ACM New York, NY, USA, 2006.