Verifiable Delegation Along With Attribute-Based Hybrid Encryption in Cloud Computing

[1]Snehal Rathod, [2]Prof. Dr.S.A.Ubale
Department of Computer Engineering, Zeal College of Engineering and Research, Pune.

Abstract: *-In the cloud, for achieving access control and keeping information confidential information owners may adopt attribute-based encoding to encode the hold on data. Users with restricted computing power are but additional possible to delegate the mask of the decoding task to the cloud servers to reduce the computing cost. As a result, attribute-based encoding with delegation emerges. Still, there are caveats and queries remaining within the previous relevant works. For instance, during the delegation, the cloud servers might tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. they will also cheat the eligible users by responding them that they're ineligible for the aim of cost 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 ciphertext-policy attribute-based hybrid cryptography with verifiable delegation has been thought-about 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 square measure well bonded at a similar time. Besides, our theme achieves security against chosen-plaintext attacks underneath the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an intensive simulation campaign confirms the practicableness and potency of the projected answer.*

Keywords: Ciphertext-policy attribute-based encryption, circuits, verifiable delegation, multilinear map, hybrid encryption.

I. INTRODUCTION

THE emergence of cloud computing brings a revolutionary innovation to the management of the info resources. Within this computing environment, the cloud servers will offer varied information services, like remote information storage and outsourced delegation computation [3-4] etc. For data storage, the servers store an oversized quantity of shared data that can be accessed by licensed users. For delegation computation, the servers can be wont to handle and calculate various information per the user's demands. As applications move to cloud computing platforms, ciphertext-policy attribute-based encoding (CP-ABE)[5] and verifiable delegation (VD)[6-7] square measure won't to guarantee the data confidentiality and also the verifiability of delegation on dishonest cloud servers. Taking medical information sharing as Associate in nursing example with the increasing volumes of medical pictures and medical records, the aid organizations place an oversized quantity of data within the cloud for reducing information storage prices and supporting medical cooperation. Since the cloud server might not be credible, the file cryptological storage is a good method to stop non-public information from being purloined or tampered. In the meanwhile, they'll get to share information with the one that satisfies some necessities, they want, i.e., access policy, can be nine Chief Doctor. To make such information sharing be realizable, attribute based encryption is applicable.

There are 2 complementary kinds of attribute-based encryption. One is key-policy attribute-based encoding (KP-ABE) [9-10-11] and also the alternative is ciphertext-policy attribute-based encoding. During a KP-ABE system, the choice of access policy is formed by the key distributor instead of the encipherer that limits the utility and value for the system in sensible applications. On the contrary, in a CP-ABE system, every ciphertext is related to associate in nursing access structure, and every non-public secret is tagged with a group of descriptive attributes. A user is ready to rewrite a ciphertext if the key's attribute set satisfies the access structure associated with a ciphertext. Apparently, this method is conceptually closer to ancient access management ways. On the other hand, during a ABE system, the access policy for general circuits can be thought to be the strongest sort of the policy categoricalion that circuits will express any program of fixed period.

Delegation computing is another main service provided by the cloud servers. within the on top of situation, the aid organizations store information files within the cloud by victimisation CP-ABE under sure access policies. The users, WHO wish to access the data files, opt for to not handle the advanced method of decryption regionally thanks to restricted resources. Instead, they are possibly to source a part of the cryptography method to the cloud server. Whereas the untrusted cloud servers WHO can translate the initial ciphertext into a straightforward one may learn nothing regarding the plaintext from the delegation.

II. RELATED WORK

Sahai and Waters [1] proposed the notion of attribute-based encryption (ABE). In subsequent works [8], [12], they focused on policies across multiple authorities and the issue of what expressions they could achieve. Up until recently, Sahai and Waters [9] 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. Actually, there still remain two 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. Hybrid encryption. Cramer and Shoup [13], [14] proposed the generic key encapsulation mechanism (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. ABE with verifiable delegation. Since the introduction of ABE, there have been advances in multiple directions. The application of outsourcing computation [8], [9] is one of an important direction. Green et al. [2] designed the first ABE with outsourced decryption scheme to reduce the computation cost during decryption. After that, Lai et al.[3] 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. Furthermore, just modify the commitments for the ciphertext relating to the message is not enough. The cloud server can deceive the user with proper permissions by responding the terminator? To cheat that he/she is not allowed to access to the data.

III. PROPOSED SYSTEM AND ALGORITHMS

We firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. 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. During the delegation computing, a user could validate whether the cloud server responds a correct transformed ciphertext to help him/her decrypt the ciphertext immediately and correctly.

Advantages of Proposed System:

- The generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length.
- They seek to guarantee the correctness of the original ciphertext by using a commitment.
- We give the anti-collusion circuit CP-ABE construction in this paper for the reason that CPABE is conceptually closer to the traditional access control methods.

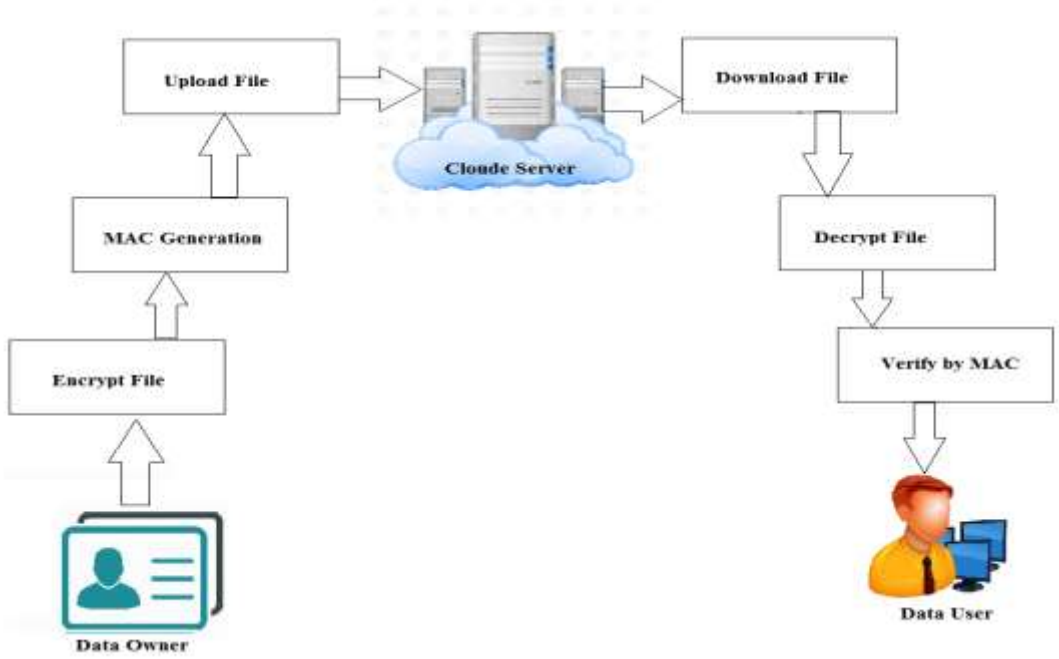

Fig.1: Architecture Diagram

Diffie–Hellman key exchange (**D–H**) Algorithm is a method of securely exchanging Cryptographic keys over a public channel and was one of the first public-key protocols. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. The keys for the algorithm are generated the following way:

1. Choose two distinct prime numbers *p* and *q*.
   - For security purposes, the integers *p* and *q* should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits[] to make factoring harder. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.

- n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3. Compute $\lambda(n) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(p-1, q-1)$, where λ is Carmichael's totient function. This value is kept private.
4. Choose an integer e such that $1 < e < \lambda(n)$ and gcd(e, $\lambda(n)$) = 1; i.e., e and $\lambda(n)$ are coprime.
5. Determine d as $d \equiv e^{-1} \pmod{\lambda(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\lambda(n)$).

- This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\lambda(n)}$.
- e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $e = 2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
- e is released as the public key exponent.
- d is kept as the private key exponent

Objective:

- Describing cloud storage model of our system then providing threat model considered and security goals we want to achieve.
- Valid and efficient data is being shared among users in which ensure security of public data integrity auditing with multi user modification and maintain the data after revocation of user.

IV. CONCLUSION

To the most effective of our information, we tend to first gift a circuit ciphertext-policy attribute-based hybrid encoding with verifiable delegation theme. General circuits square measure accustomed specific the strongest sort of access management policy. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertext-policy attribute-based hybrid encoding, we tend to may delegate the verifiable partial decipherment paradigm to the cloud server. Additionally, the projected theme is well-tried to be secure supported k-multilinear Decisional Diffie-Hellman assumption..

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," 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] 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.

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

[5] 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.

[6] 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.

[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 Cryptography. Conf. Public Key Cryptography, 2012, pp. 243–261.

[8] 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.

[9] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attributebased encryption for circuits from multilinear maps," in Proc. 33rd Int. Cryptol. Conf., 2013, pp. 479–499.

[10] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," in Proc. 45th Annu. ACM Symp. Theory Comput., 2013, pp. 545–554.

[11] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[13] 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.

[14] R. Cramer and V. Shoup, "Design and analysis of practical publickey encryption schemes secure against adaptive chosen ciphertext attack," SIAM J. Comput., vol. 33, no. 1, pp. 167–226, 2004.

[15]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