Hybrid Cryptography with Verifiable Delegation in Cloud Computing On Circuit Cipher text-Policy Attribute-Based Encryption

SK Basheer Ahamed[1], V. Padmaja[2], Dr. G.Minni[3]
[1]Student, M.Tech (CSE), Nimra College of Engineering & Technology, A.P., India.
[2]Associate Professor, Dept. Of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.
[3]HOD, Dept. Of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.

Abstract — Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. 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 realizing 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.

Keywords— Ciphertext-Policy Attribute-Based Encryption,Verifiable Delegation.

1. Introduction

Cloud computing brings a revolutionary innovation to the management of the in sources. Inside this computing setting, the cloud servers can give numerous information services, like remote information storage and outsourced delegation computation, etc. For information storage, the servers store an oversized quantity of shared information that may well be accessed by licensed users. For delegation computation, the servers may well be accustomed handle and calculate various information in step with the user's demands. As applications move to cloud computing platforms, cipher text -policy attribute-based encoding (CP - ABE)[1] and verifiable delegation (VD) area unit accustomed make sure the information confidentiality and also the verifiability of delegation on dishonest cloud servers. information of knowledge of information} within the cloud for reducing data storage prices and supporting medical cooperation. Since the cloud server might not be credible, the file crypto logical storage is an efficient methodology to forestall non-public information from being taken or tampered. Within the in the meantime, they'll got to share information with the one who satisfies some necessities. the wants, i.e., access policy, may well be creating such information sharing be accomplishable, attribute-based encoding is applicable. The advantage of cloud is cost savings. The prime disadvantage is security. 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 applications 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. To make such data sharing be achievable, attribute based encryption is used. There are two forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the second is ciphertext-policy attribute-based encryption. In CP-ABE system, each ciphertext is contains an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertextif and only if the key's attribute set satisfies the access structure associated with a ciphertext. The cloud server provides another service which is delegation computing.The VD-CPABE schemeshows that the untrusted cloud will not be able to learn anything about the encrypted message and build the original ciphertext. Since the cloud server might not be credible, the file cryptological storage is an efficient methodology to forestall non-public information from being taken or tampered. within the in the meantime, they'll got to share information with the one who satisfies some necessities. the wants, i.e., access policy, may well be creating such information sharing be accomplishable, attribute-based encoding is applicable.

2. Literature Survey

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 wh o 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 present a new methodology for comprehending Ciphertext -Policy Attribute Encryption (CPABE) 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 DieHellman Exponent (PBDHE) assumption that can be believed as a generalization of the BDHE assumption.

3. Implementation

1. Attribute Authority:

Authority will have to provide the key, as per the user's key request. Every users request will have to be raised to authority to get access key on mail. There are two complementary forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CPABE). 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.

2. Cloud Server:

Cloud server will have the access to files which are uploaded by the data owner Cloud server needs to decrypt the files available under their permission. Furthermore data user will have to decrypt the data to access the original text by providing the respective key. File has been decrypted successfully and provided for consumer.

3. Data owner:

Data owner will have to register initially to get access to the profile. Data Owner will upload the file to the cloud server in the encrypted format. Random encryption key generation is happening while uploading the file to the cloud. Encrypted file will be stored on the cloud.

4. Data Consumer:

Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data consumer can access the file based on the key received from mail id. As per the key received the consumer can verify and decrypt the data from the cloud.

4. Existing System

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) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers. The increasing volumes of medical images and medical records, the healthcare organizations put a large amount of data in the cloud for reducing data storage costs and supporting medical cooperation. There are two complementary forms of attribute based encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CPABE).

4.1 Disadvantages of Existing System:

- The cloud server might tamper or replace the data owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext.

- 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.

5. Proposed System:

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 secure 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.

5.1 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.

6. Conclusion

In this paper, 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. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertextpolicy 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 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.

References

Good Teachers are worth more than thousand books, we have them in Our Department.

[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.

[13] R. Cramer and V. Shoup, ”A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack,” in Proc. CRYPTO, pp.13-25, Springer-Verlag Berlin, Heidelberg, 1998.

[14] R. Cramer and V. Shoup, ”Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack,” in Proc. SIAM Journal on Computing, vol. 33, NO. 1, pp.167-226, 2004.

[15] D. Hofheinz and E. Kiltz R, ”Secure hybrid encryption from weakened key encapsulation,” in Proc. CRYPTO, pp.553-571, Springer-Verlag Berlin, Heidelberg, 2007.

[16] M. Abe, R. Gennaro and K. Kurosawa, ”Tag-KEM/DEM:A New Framework for Hybrid Encryption,” in Proc. CRYPTO, pp.97-130, Springer-Verlag New York, NJ, USA, 2008.

[17] K. Kurosawa and Y. Desmedt, ”A New Paradigm of Hybrid Encryption Scheme,” in Proc. CRYPTO, pp.426-442, Springer-Verlag Berlin, Heidelberg, 2004.

[18] J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, ”Securely Outsourcing Attribute-based Encryption with Checkability,” in Proc. IEEE Transactions on Parallel and Distributed Systems, 2013.

About Authors:

Mr.SK BASHEER AHAMED is a student of Nimra college of Engineering and Technology, ibrahimpatnam, VIJAYAWADA. He is presently pursuing his M.Tech degree from JNTU,Kakinada.

V Padmaja is presently working as Associate professor in CSE department, Nimra college of Engineering and Technology, Ibrahimpatnam, Vijayawada.

Dr.G Minni is presently working as Head of the Department in CSE department,Nimra college of Engineering and Technology, Ibrahimpatnam, Vijayawada.