International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

Attribute Based Hybrid Encryption with Verifiable Delegation in Cloud Computing Using Circuit Ciphertext-Policy

S.SUSHMA[1]& ISHAQ SHAREEF C[2]

[1]M-Tech, Dept. CSE, P.V.K.K Institute of Technology, Affiliated to JNTUA, AP, India.

[2]Assistant Professor, Dept. CSE, P.V.K.K Institute of Technology, Affiliated to JNTUA, AP, India

ABSTRACT

In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-predicated encryption to encrypt the stored data. Users with inhibited computing power are however more liable to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-predicated encryption with delegation emerges. Still, there are caveats and questions remaining in the precedent germane works. For instance, during the delegation, the cloud servers could tamper or supersede the delegated ciphertext and respond a forged computing result with malignant intent. They may withal cheat the eligible users by responding them that they are ineligible for the purport of cost preserving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the most vigorous form of access control, a construction for realising circuit ciphertext-policy attribute-predicated hybrid encryption with verifiable delegation has been considered in our work. In such a system, coalesced 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 ensured concurrently. Besides, our scheme achieves security against culled-plaintext attacks under the k-multilinear Decisional Diffie-Hellman postulation. Moreover, an extensive simulation campaign corroborates the feasibility and efficiency of the proposed solution.

Key words: - Attribute based encryption, data sharing, verifiable delegation, authentication, confidentiality.

1. INTRODUCTION

Cloud computing is the utilization of registering assets (equipment and programming) that are conveyed as an administration over a system (commonly the Internet). The name originates from the basic utilization of a cloud-formed image as a deliberation for the unpredictable base it contains in framework graphs. Cloud computing (CC) is a model to enable

convenient, on-demand network access for a shared pool of configurable computing resources (e.g., servers, networks, storage, applications, and services) that could be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing is featured by that users can elastically utilize the infrastructure (e.g., networks, servers, and storages), platforms (e.g., operating systems and middleware services), and softwares (e.g., application programs) offered by cloud providers in an on-demand manner. Not only the operating cost and business risks as well as maintenance expenses of service providers can be substantially lowered with CC, but also the service scale can be expanded on demand and web-based easy access for clients could be provided benefiting from CC. Distributed computing depends remote organizations with a customer's data, programming and computation. Distributed computing involves gear and programming resources made available on the Internet as supervised outcast organizations. These organizations typically offer access to forefront programming applications and first class frameworks of server PCs. Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world.

2. RELEGATED WORK

2.1Existing System

The servers could be habituated to handle and calculate numerous data according to the user's demands. As applications peregrinate to cloud computing platforms, ciphertext-policy attribute-predicated encryption (CP-ABE) and verifiable delegation (VD) are acclimated to ascertain the data confidentiality and the verifiability of the delegation on mendacious cloud servers. The incrementing volumes of medical images and medical records, the healthcare organisations put a substantial amount of data in the cloud for reducing data storage costs and fortifying medical cooperation. There are two complementary forms of attribute predicated encryption.

One is key-policy attribute-predicated encryption (KP-ABE) and the other is ciphertext-policy attribute-predicated encryption (CPABE).

2.2Proposed System

We firstly present a circuit ciphertext-policy attribute-predicated hybrid encryption with verifiable delegation scheme. General circuits are acclimated to express the most vigorous form of access control policy. the proposed scheme is proven to be secure predicated on k-multi linear Decisional Diffie-Hellman postulation. On the other hand, we implement our scheme over the integers. During the delegation computing, a utilized could validate whether the cloud server responds a correct transformed cipher text to avail him/her decrypt the cipher text immediately and correctly

3. IMPLEMENTATION

3.1Attribute 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.

3.2Data 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.

3.3Cloud 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.

3.4Data 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. EXPERIMENTAL RESULTS

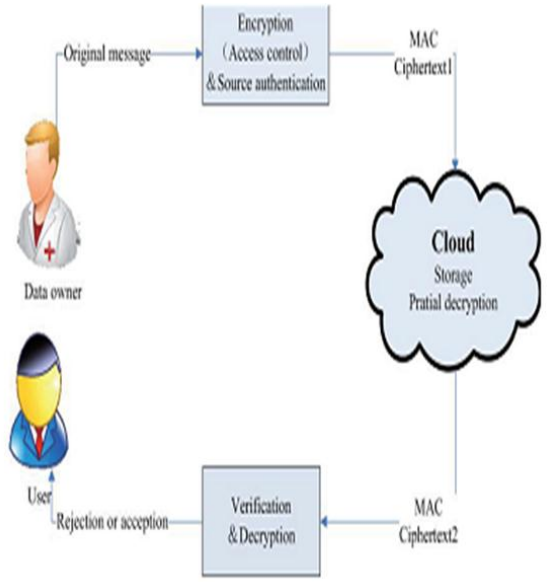

Fig 1 Architecture Diagram

Fig 2 Registration Page

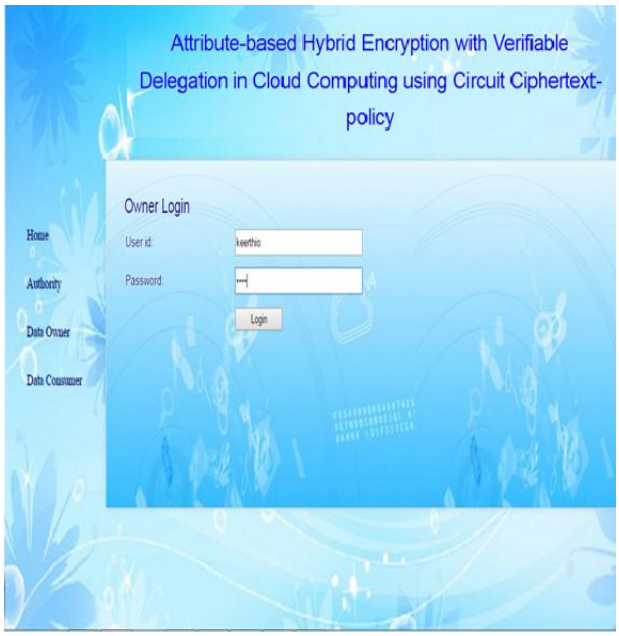

Fig 3 Login Page

Fig 4 File uploads Page

Fig 5 Key Generation Page

Fig 6 File Download Page

5. CONCLUSION

To the best of our erudition, we firstly present a circuit ciphertext-policy attribute-predicated hybrid encryption with verifiable delegation scheme. General circuits are acclimated to express the most vigorous form of access control policy. Coalesced verifiable computation and encrypt-then-mac mechanism with our ciphertext policy attribute-predicated hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. In additament, the proposed scheme is proven to be secure predicated on k-multilinear Decisional Diffie-Hellman posit. 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 ascertain the data confidentiality, the fine-grained access control and the verifiable delegation in the cloud.

6. REFERENCE

[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.