International Journal of Research
Available at https://edupediapublications.org/journa
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Data sharing Suing ABE Verifiable Delegation Authentication Confidentiality

T. MD Sharief[1] & Ms.M.Meenakshi [2]

[1]M-Tech,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

[2]HOD&Asst.Professor,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

Abstract: -Data owner encrypt their data before outsourcing into the cloud for the purpose of privacy preserving. Additionally, the attribute based encryption method is used to enhance the confidentiality and access control. Delegation is a process which is performed by the users who are containing the less computing power. They delegate their decryption process to the cloud server to reduce the computation cost. This time the cloud server may change the given cipher text and sends the modified one to the data user for malicious attack. This time the access control cannot be malleable. To enhance the access control, we propose a circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation method. For the authentication purpose, mac mechanism is added with the symmetric encryption technique. By this mechanism, we can certify the confidentiality of data, accuracy of the delegated computing results and enhance the access control. Our paper uses the k-multi linear Decisional Diffie-Hellman algorithm to improve the security to the encrypted data. This scheme takes only less computational and communication cost so it will be done at practically.

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

1. INTRODUCTION

The emergence of cloud computing brings a revolutionary innovation to the management of the info resources. 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, ciphertext-policy attribute-based encoding (CP-ABE) and verifiable delegation (VD) area unit

accustomed make sure the information confidentiality and also the verifiability of delegation on dishonest cloud servers. Taking medical information sharing as associate, with the increasing volumes of medical pictures and medical records, the care organizations place an oversized quantity {of 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 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. RELATED WORK

Existing System

The cloud servers could tamper or replace the delegated ciphertext 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.

Proposed System

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. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-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

3. IMPLEMENTATION

International Journal of Research
Available at https://edupediapublications.org/journa
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

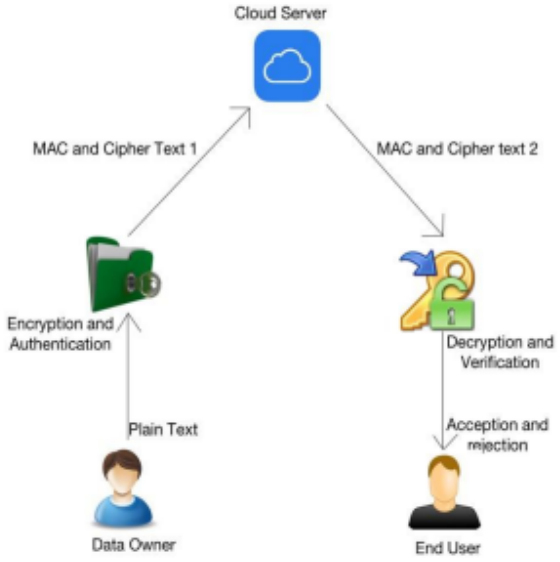

Fig:-1 Project Architecture

Cloud Storage

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data.

Security Model

Since we use key encapsulation mechanism (KEM) and authenticated encryption (AE) to build our hybrid VD-CPABE scheme, we describe the security definition separately at first. The confidentiality property (indistinguishability of encryptions under selective chosen plaintext attacks (IND-CPA)) required for KEM is captured by the following games against adversary A. Game.KEMInit. The adversary gives a challenge access structure f∗, where it wishes to be challenged. Setup. The simulator runs the Setup algorithm and gives the public parameters PK to the adversary.KeyGen Queries I. The adversary makes repeated private key queries corresponding to the sets of attributes x1, ..., xq1 . We require that ∀i ∈ q1 we have f∗(xi) = 0.

Encrypt. The simulator encrypts K0 under the structure f∗, random chooses K1 from key space and flips a random coin b. Then the simulator sends Kb and the ciphertext CK∗ to the adversary. KeyGen Queries II. The adversary makes repeated private key queries corresponding to the sets of attributes xq1 , ..., xq where f∗(x) = 0. • Guess. The adversary outputs a guess b′ of b. We define the advantage of an adversary A in this game is Pr[b′ = b] − 1 2 . Then a KEM scheme is secure against selective chosen plaintext attacks if the advantage is negligible. The confidentiality property

(indistinguishability of encryptions under selective chosen ciphertext attacks (IND-CCA)) required for AE is captured by the following games against adversary A. Game.AE • Init. The adversary submits two equal length messages M0 and M1. • Setup. The simulator runs the Setup algorithm and generators the symmetric key KAE. • Encrypt. The simulator flips a random coin b, encrypts Mb under the symmetric key KAE, generates the ciphertext C∗ and gives it to the adversary. • Decrypt Queries. The adversary makes repeated decryption queries. When the given ciphertext C/= C∗, the simulator will return DKAE(C) and σKAE(C) to the adversary.

Ciphertext-policy attribute-based encryption

In this section, we present the definition and security model of our hybrid VD-CPABE. In such a system, a circuit ciphertext-policy attribute-based encryption scheme, a symmetric encryption scheme and an encrypt-then-mac mechanism are applied to ensure the confidentiality, the fine-grained access control and the verifiable delegation

A hybrid VD-CPABE scheme is defined by a tuple of algorithms (Setup, Hybrid-Encrypt, Key- Gen, Transform, Verify-Decrypt). The description of each algorithm is as follows. • Setup(λ, n, l). Executed by the authority, this algorithm takes as input a security parameter λ, the number of attributes n and the maximum depth l of a circuit. It outputs the public parameters PK and a master key MK which is kept secret. more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPDS.2015.2392752, IEEE Transactions on Parallel and Distributed Systems XU et al.: circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing 5 • Hybrid-Encrypt(PK,M, f). This algorithm is executed by the data owner. It could be conveniently divided into two parts: key encapsulation mechanism (KEM) and authenticated symmetric encryption (AE). – The KEM algorithm takes as input the public parameters PK and an access structure f for circuit. It computes the complement circuit f and chooses a random string R. Then it generates KM = {dkm, vkm}, KR = {dkr, vkr} and the CP-ABE ciphertext (CKM,CKR). – The AE algorithm takes as input a message M, the random string R, the symmetric key

International Journal of Research
Available at https://edupediapublications.org/journa
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Hybrid encryption

Hybrid encryption. Cramer and Shoup proposed the generic 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 is one of an important direction. Green etaldesigned the first ABE with outsourced decryption scheme to reduce the computation cost during decryption. After that, Lai et al. 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.

4. EXPERIMENTAL RESULTS

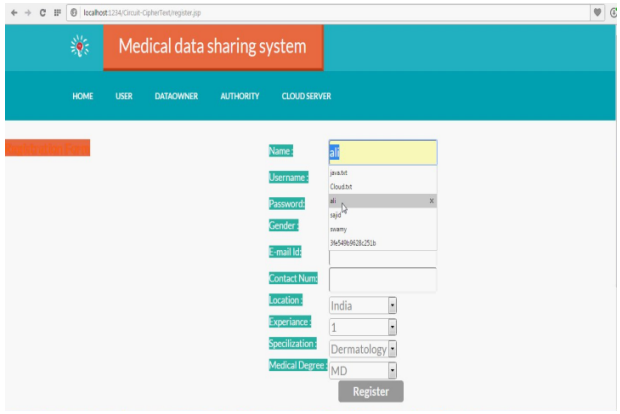

Fig:-2 User Registration with ABE

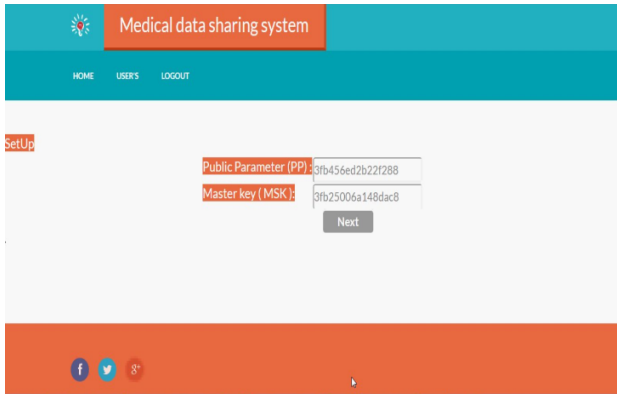

Fig:-3 keys Generation

International Journal of Research
Available at https://edupediapublications.org/journa
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

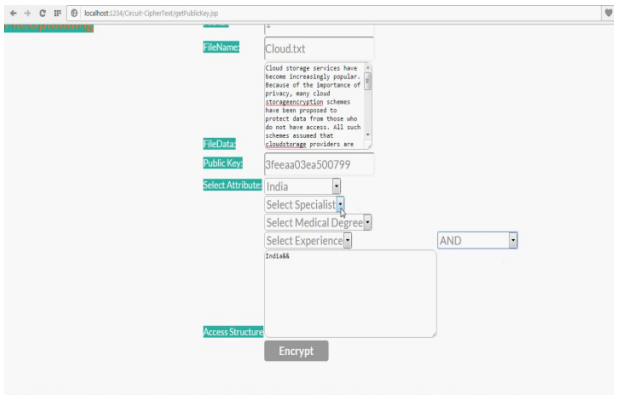

Fig:-4 Data Encryption using ABE

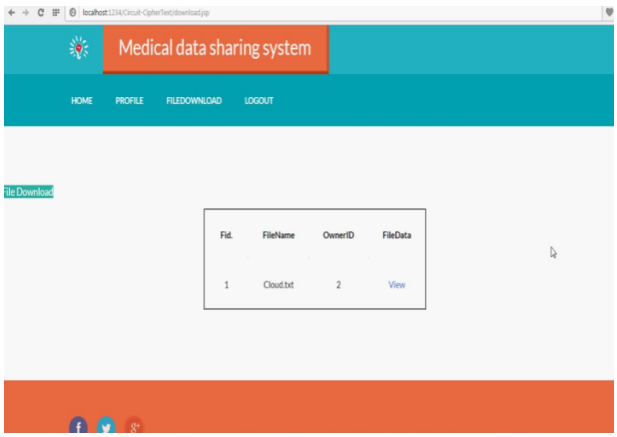

Fig:-5 File Download

5. CONCLUSION

In the cloud, for accomplished admission association and keeping vision confidential, {the knowledge|theinfo|the information} homeowners could accept attribute-based cryptography to encipher the grasp on data. decoding task to the cloud servers to cut back the computing value. Our ciphertext strategy attribute-based hybrid cryptography, we incline to could representative the verifiable partial decoding to the cloud server

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. USENIXSecuritySymp., 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, Efficient, and Provably SecureRealization," 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 computationfrom 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 Securityand Anonymous Predicate Authentication,” in Proc. PKC, pp.243-261, Springer-Verlag Berlin, Heidelberg, 2012.

[8] S. Garg, C. Gentry and ShaiHalevi,” CandidateMulitilinear Maps from Ideal Lattices and Applications,”in Proc. EUROCRYPT, pp.1-17, Springer-Verlag Berlin,Heidelberg, 2013.

[9] Melissa Chase and Sherman S. M. Chow. Improvingprivacy and security in multiauthority attribute-basedencryption. In ACM Conference on Computer andCommunications Security, pages 121–130, 2009.

[10] Jonathan Katz, AmitSahai, and Brent Waters.Predicateencryption supporting disjunctions, polynomial equations,and inner products. In EUROCRYPT, pages 146–162,2008