UGC Approved Journal

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2017

Attribute-based Hybrid Encryption in Cloud Computing Environment using Verifiable Delegation

Ashwini M Magadi[1], Prof. Vivekanandreddy[2]

PG Scholar, Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, India[1]

Faculty, Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, India[2]

Abstract: In cloud computing for the secure access of the data, data owners can go for the encryption that is based on the attributes to encrypt the data that has been stored in the data center. Users delegate the decryption part of work to the servers of cloud to reduce the cost of computing. So attribute based encryption technique comes into picture. But delegation by the servers of the cloud lead to the tampering of the data or not providing access to the eligible users for cost saving purpose.

Keywords: Verifiable delegation, Attribute based encryption, cipher text, outsourcing.

I. INTRODUCTION

Management of the information and the data by making use of available resources. The data centers and the servers store the humungous amount of data that is been shared among many users and is accessed by the users who are authorized .For Delegation computation servers could be used to handle and then be able to calculate large amount of the data when the users want to access the data.

CP-ABE and Verifiable Delegation are used to make sure the data confidentiality and verifiability . servers of cloud offer various data services like outsourced delegation computation. CP-ABE and VD are the combination of two techniques.

Attribute based encryption

There are two types of the attribute based encryption:

i) Key-Policy Attribute Based Encryption (KP-ABE): In this technique KP-ABE decision of access policy is made by the key distributor. This actually limits the practicability and usability.

ii) Ciphertext-Policy Attribute Based Encryption (CP-ABE): Here each of the cipher text is associated with an access structure and each private key is labelled with a set of descriptive attributes. If key's attributes matches with the access structure of the cipher text, then only user can decrypt the cipher text.

Delegation computing

Delegation computing is another main service provide by the cloud servers . Decryption process is outsourced to the cloud server rather than doing it locally. Delegation suffers two problems that is cloud server might fiddle with the data and could end up in giving access to the attackers. In order to save the computational cost cloud server could cheat the authorized users. Hence there is necessity to provide Confidentiality and Verifiability.

II. RELATED WORKS AND IMPLMENTATION

M. Armbrust, et.al [1]Dispersed way of computing alludes of two of the applications portrayed as administrative power on top of the Internet and the tools and the schemes encoding in the centres of data that provide individuals administrations. For pretty some period of time the administrations are now been considered to as the Programming as a Service (SaaS). The technology which gathers all the data and which has built in with necessary operations to mine through that stored data is called a cloud and the costumers can store the data here and then get back the data using available resources.

Sahai and waters proposed Attribute Based Encryption. They mainly focused on KP-ABE and the issue of what expressions they could use disadvantage is that they dint concentrate on CP-ABE[11].

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

ABE with verifiable delegation was proposed by Green et al, he designed first ABE with verifiable delegation scheme to reduce computation cost during decryption. Here the disadvantage was that data owners identity is revealed , so the untrusted server could forge the message he chooses.

The implementation includes the steps as mentioned, We modify CP-ABE with verifiable delegation and present VD-CPABE. To keep the data private and to achieve fine grained access control, our starting point is a circuit key – policy attribute based encryption. The cloud server may fiddle with the ciphertext or cheat the eligible user that he even does not have permissions to decryption. To validate the correctness, we extend the CP-ABE ciphertext into the attribute based ciphertext for two complementary policies and add a MAC for each ciphertext, so that whether the user has the permission.

III. 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.

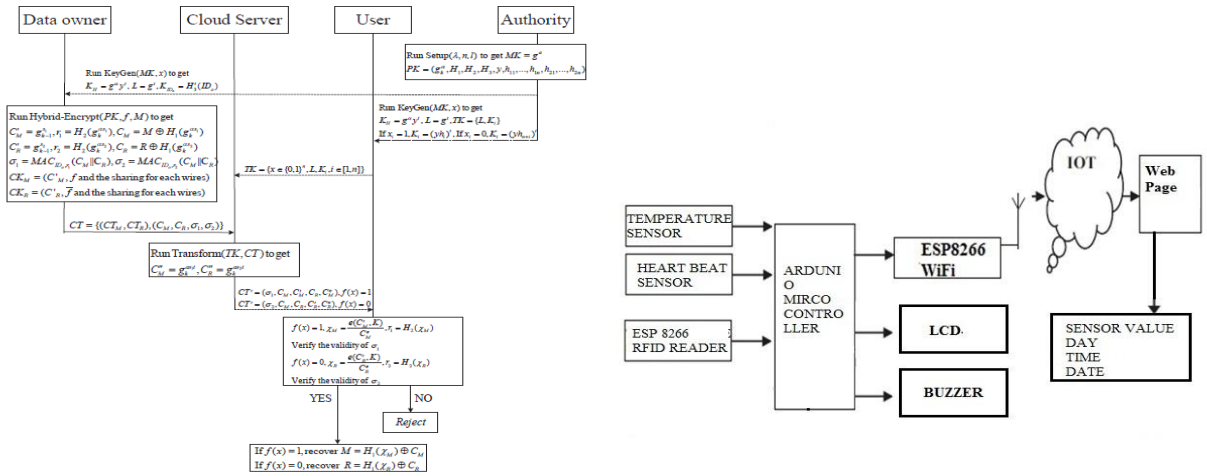

Fig 1 System Architecture

IV. OUR TECHNIQUES

The main aim of verifiable delegation is to protect authorized users from being derived during the delegation. Data owner encrypts his message M under access policy f. Then computes complement f' which outputs the opposite bit f and encrypts random element R of same length as M under the policy f' then users can outsource their complex access control policies decision and leave the decryption process to the cloud. The above extended encryption ensure that the users can obtain either the message M or the random element R.

Hybrid VD-CPABE

This is defined by a tuple of algorithms (setup, Hybrid-Encrypt, Key_Gen, Transform, Verify-Decrypt) these could be treated as the 5 phases of the algorithm. Authority generates private keys for the data owner and user. Data owner encrypts his data using hybrid encryption system. It generates privately verifiable MAC for each symmetric ciphertext then uploads the whole ciphertext to the cloud server. Data owner could go offline. User who wants access to the data interacts with the cloud server.

UGC Approved Journal

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2017

V. CONCLUSION

To the best of our insight, we right off the bat display a circuit ciphertext-strategy property based half breed encryption with obvious appointment conspire. General circuits are used in order to articulate the largely beached kind of obtain to control scheme. Joined obvious estimate and encode then-macintosh tool by means of our ciphertext rule superiority based half breed encryption, we may possibly assign the convinced unfinished separating overall view of data center. in addition, it projected contrive is over and done with and with reference to being safe and sound in luminosity of k-mulltilinear Decisional Difffie-Helllman distrust. Afterwards yet again, accomplish our sketch in excess of the facts the payment of the reckoning in addition to communication take advantage of put on show with the aim of the preparation is all along to terrain in the circulated compute. Surrounded by this come within reach of could conceivably subsist related it towards guarantee the in sequence labelling, the fine-grained get hold of on the way to supervise as well as the undeniable portrayal into cloud.

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 theDecryption of ABE Ciphertexts," in Proc. USENIX SecuritySymp., 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-VerlagBerlin, Heidelberg, 2011.

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

[6] B. Parno, M. Raykova and V. Vaikuntanathan, "Howto 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 Security and AnonymousPredicate 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 MultilinearMaps," in Proc. CRYPTO, pp.479-499, Springer-Verlag Berlin,Heidelberg, 2013.

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