International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Implemented Hybrid Encryption Algorithm with Variable Delegation for Data Security in the Cloud

Katpadi Baby Shalini[1], Vuyyuru Lakshma Reddy[2]

[1]PG Scholar, Department of CSE, PACE Institute of Technology and Sciences,Vallur, Prakasam, Andhra Pradesh, India

[2]Assistant Professor, Department of CSE, PACE Institute of Technology and Sciences, Vallur, Prakasam, Andhra Pradesh, India

ABSTRACT

In the cloud, for accomplishing access control and information security, the information proprietors could utilizes ascribe based encryption to scramble the put away information. To decrease the cost, the users which has a restricted processing power are by the by more prone to assign the cover of the unscrambling errand to the cloud servers. The outcome appears, quality based encryption with appointment turn out. In any case, there are a few issues and inquiries with respect to past related works. For instance, amid the assignment or discharge, the cloud servers could distort or supplant the appointed ciphertext and react a phony outcome with vindictive expectation. And in addition with the end goal of cost sparing the cloud server may likewise extortion the qualified clients by reacting them that they are unworthy. Indeed, the entrance approaches may not be adaptable amid the encryption. Since strategy for general circuits are utilized to accomplish the most grounded type of access control, a development to configuration circuit ciphertext-approach quality based cross breed encryption with irrefutable assignment has been produced. This framework is blended with certain calculation and encode then-Mac component, the information classification, the fine-grained get to control and additionally the rightness of the appointed processing comes about are very much ensured in the meantime. And in addition this plan accomplishes security against picked plaintext assaults under the k-multilinear Decisional Diffie-Hellman presumption. Besides, this plan accomplishes plausibility and in addition effectiveness.

Keywords : Ciphertext-Policy Attribute-Based Encryption, Circuits, Verifiable Delegation, Multi Linear Map, Hybrid Encryption.

I. INTRODUCTION

Cloud computing is novel processing system that is based on virtualization, parallel and distributed computing, utility processing, and service oriented architecture. In the past decades, distributed computing has developed as a standout amongst the most compelling ideal models in the IT business, and has pulled in broad consideration from both the academia and industry. Nonetheless, the individual client prerequisites might be differing and require diverse types of outsourced calculation, while current PVC plans support only a single structure. Customers might wish to demand estimations from a specific server or to issue a solicitation to a huge pool of servers. The access policy is totally in view of authorization relationship where the relationship is between user attributes and asset properties. The properties might be any data of the client's profession, work parts that is given and is utilized to concede the access. However, all together to outline an access strategy component there are numerous difficulties to conquer some of them are

(1) User can transfer any sort of information such as content, media etc.
(2) Any can give any number of attributes and thus two or more clients might have same characteristics.
(3) Any individual might fabulous any sort of access to any number of clients.

CSEIT11726302 | Received : 01 Dec 2017 | Accepted : 26 Dec 2017 | November-December-2017 [(2)6: 1014-1017]

This methodology permits the client to actualize the access control on their information specifically in content sharing service instead of central administrator. To give an intricate access policy component, we require adaptable and versatile cryptographic key administration estimations. For enhancing these disservices, we are utilizing attribute based encryption. Subsequently, we employed CP-ABE (Cipher Text Policy schema – Attribute Based Encryption) method as a solution for the aforementioned problem. In CP-ABE, the beneficiary can unscramble the information just when the client attribute fulfill the access policy.

II. PROBLEM STATEMENT

A. Securely Outsourcing Attribute-Based Encryption with Check ability:

In this paper [1], Attribute-Based Encryption (ABE) is a promising cryptographic crude which essentially improves the flexibility of access control components. Because of the high expressiveness of ABE strategies, the computational complexities of ABE key-issuing a decoding are getting restrictively high. We propose another Secure Outsourced ABE framework, which bolsters both secure outsourced key-issuing and decoding.

B. Privacy-preserving decentralized key-policy attribute-based encryption:

In this paper [2], they have proposed privacy-preserving decentralized key-policy ABE scheme where each authority can issue secret keys to a user independently without knowing anything about his GID. Therefore, even if multiple authorities are corrupted, they cannot collect the user's attributes by tracing his GID

c. Decentralizing attribute-based encryption:

In paper [5], We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority.

d.Universally Composable Secure Channel Based on the KEM-DEM Framework:

In paper [6], For ISO gauges on open key encryption, Show up presented the structure of KEM (Key Encapsulation Mechanism), and DEM (Data Encapsulation Mechanism), for formalizing and acknowledging one-directional half breed encryption; KEM is a formalization of uneven encryption indicated for key dissemination, and DEM is a formalization of symmetric encryption. This paper examines a more broad half and half convention, secure channel, utilizing KEM and DEM, to such an extent that KEM is utilized for dissemination of a session key and DEM, alongside the session key, is utilized for various bi-directional encoded exchanges in a session. This paper demonstrates that KEM semantically secure against adaptively picked figure content assaults (IND-CCA2) and DEM semantically secure against adaptively picked plaintext/figure content assaults (IND-P2-C2) alongside secure marks and perfect accreditation specialist are adequate to understand an all around composable (UC) secure channel.

III. Aim

a) To avoid User identity revealed.
b) To avoid Access Control is not distributed giving rise to single point of failure
c) Increased complexity because policies are embedded in user's key.

IV. SYSTEM ARCHITECTURE

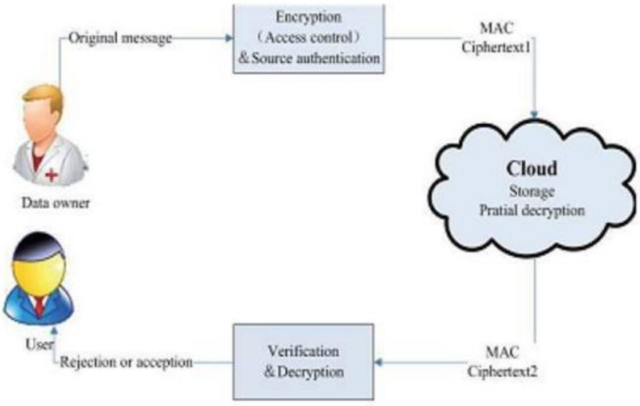

Figure 1. System Architecture

The system contains four modules,

1. Cloud Storage Module
2. Data Owner Module
3. Data User Module
4. Authority Module

Cloud Storage:

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.

Data Owner:

The data owner encrypts his message under access policy, then computes the complement circuit, which outputs the opposite bit of the output of f, and encrypts a random element R of the same length to under the policy

Data User:

The users can outsource their complex access control policy decision and part process of decryption to the cloud. Which extended encryption ensures that the users can obtain either the message M or the random element R, which avoids the scenario when the cloud server deceives the users that they are not satisfied to the access policy, however, they meet the access policy actually.

Authority:

Authority generates private keys for the data user.

V. CONCLUSION

In this paper, we addressed an important issue of attribute revocation for attribute based systems. In particular, semi-trustable proxy servers are available, and proposed a scheme supporting user's attribute revocation schema. A unique property of our proposed scheme is that it places minimal load on authority upon the events in user's revocation. We achieved this by uniquely combining the proxy re-encryption technique with CPSBAE and enabled the authority to delegate most laborious tasks to proxy servers. Our proposed scheme is provably secure against chosen cipher-text attacks. In addition, we also showed the applicability of our method to the KP-ABE scheme. An experimental design shows the effectiveness and efficiency of our proposed work.

VI. REFERENCES

[1]. J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, "Securely Outsourcing Attribute-based Encryptionwith Checkability," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2013.

[2]. 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.

[3]. J. Hur and D. K. Noh,"Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2011.

[4]. 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.

[5]. A. Lewko and B. Waters, "Decentralizing Attribute- Based Encryption," in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[6]. W. Nagao, Y. Manabe and Tatsuaki Okamoto, "AUniversally Composable Secure Channel Based on the KEM-DEM Framework," in Proc. CRYPTO, pp.426-444, Springer-Verlag Berlin, Heidelberg, 2005.

Author's Profiles:

Ms.KATPADI.BABY SHALINI received B.Tech in Computer Science and Engineering from Malineni Lakshmaiah Engineering College, Singarayakonda affiliated to the Jawaharlal Nehru technological university, Kakinada in 2012, and pursuing M. Tech in Computer Science and Engineering from PACE Institute Of Technology and Sciences affiliated to the Jawaharlal Nehru technological university, Kakinada in 2015-17, respectively.

Mr.VUYYURU.LAKSHMA REDDY Has Received MCA And M.Tech PG.He Is Dedicated To teaching Field From The Last 7 Years. He Has Guided 6 P.G Students And 17 U.G Students. At Present He Is Working As Asst.Professor In PACE Institute Of Technology and Sciences,Vallur, Prakasam(Dt), AP, India.He Is Highly Passionate And Enthusiastic About His Teaching And Believes That Inspiring Students To Give Of His Best In Order To Discover What He Already Knows Is Better Than Simply Teaching.