SECURING DATA ON CLOUD USING CIPHERTEXT HYBRID ENCRYPTION WITH VERIFIABLE DELEGATION

Chaithra S P[1], Hooreya Najeeb[2], C K Vanamala[3]

[1]*Chaithra S P, Department of ISE, NIE, Mysore, Karnataka*
[2]*Hooreya Najeeb, Department of ISE, NIE, Mysore, Karnataka*
[3]*C K Vanamala, Department of ISE, NIE, Mysore, Karnataka*

ABSTRACT

For keeping data confidential and for achieving access control, data owners opt for attribute based encryption for the data stored on the cloud. Delegation of the decryption task arises when users have limited computing power. As a result of this, attribute based encryption with delegation emerged. But still the previous work is questioned due to various caveats. For example, with delegation, the delegated cipher text could be tampered or replaced by the cloud servers and respond a forged computing result with malicious intent and the eligible users could be cheated by saying that they are ineligible for the purpose of cost saving. Moreover, the access policies may not be flexible enough during the encryption. The data confidentiality, fine-grained access control and the correctness of the delegated computing results are well guaranteed by combining verifiable computation and encrypt-then-mac mechanism.

Keyword: - *Attribute-based encryption, Delegation, Access Control, Confidentiality, Cloud Computing*.

---

1. INTRODUCTION

Cloud Computing is the emerging trend in networking. Many different advantages are offered by the cloud to its users that lead to it being adopted in different fields. Within the computing environment, the various services offered by the cloud servers are remote data storage [1], outsourced delegation computation [2] etc. The following are used to ensure the data confidentiality and the verifiability of the delegation on dishonest cloud servers:

- Ciphertext policy attribute based encryption (CP-ABE): It is a type of public key encryption in which the secret key of a user and the ciphertext are dependent upon the attributes. E.g.: the country in which he lives. [3]
- Verifiable delegation (VD): Computation on outsourced data.

1.1 Existing System

In order to store, handle and calculate numerous data, the cloud servers are being used. Large number of applications moves on to cloud computing platforms which has to be handled. In order to ensure data confidentiality of such applications and verifiability of the delegation on dishonest cloud servers, ciphertext-policy attribute based encryption and verifiable delegation is used.

Disadvantages of Existing System:

- The data owners' original ciphertext might be tampered or replaced by the cloud servers for malicious attacks and then the cloud servers may respond with 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.
- The Cloud Computing platform itself suffers from many drawbacks such as funding, loss of internal control, Lack of standardization management etc.

1.2 Proposed System

The main aim is to use 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.

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.

1.3 Related Works

1] Attribute based Encryption

Authors: Sahai and Waters.

Sahai and Waters [4] proposed the notion of attribute-based encryption (ABE). In subsequent works [5], [6], they focused on policies across multiple authorities and the issue of what expressions they could achieve. Up

until recently, Sahai and Waters [7] raised a construction for realizing KPABE for general circuits. Actually, there still remain two problems. The first one is having no construction for realizing CPABE for general circuits, which is conceptually closer to traditional access control. The other is related to the efficiency, since the exiting circuit ABE scheme is just a bit encryption one. Thus, it is apparently still remains a pivotal open problem to design an efficient circuit CP-ABE scheme.

2] Hybrid Encryption:
Authors: Cramer and Shoup.
Cramer and Shoup [8], [9] 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 [10], [11], [12]. Such improved model has the advantage of achieving higher security requirements.

3] ABE with Verifiable Delegation
Authors: Green et al and Lai et al.
Green et al. [2] designed the first ABE with outsourced decryption scheme to reduce the computation cost during decryption. After that, Lai et al. [3] 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 $\perp$ to cheat that he/she is not allowed to access to the data.

2. DESIGN MODULES

- Attribute Authority
- Cloud Server
- Data Owner
- Data Consumer

2.1 Module Description

- **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.

- **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.

- **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.

- **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.

2.2 Data Flow Diagrams

The below DFD diagram shows the input data to the system, various processing carried out on this data, and the output data generated by this system. The components in the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system. The given DFD is partitioned into levels that represent increasing information flow and functional detail.

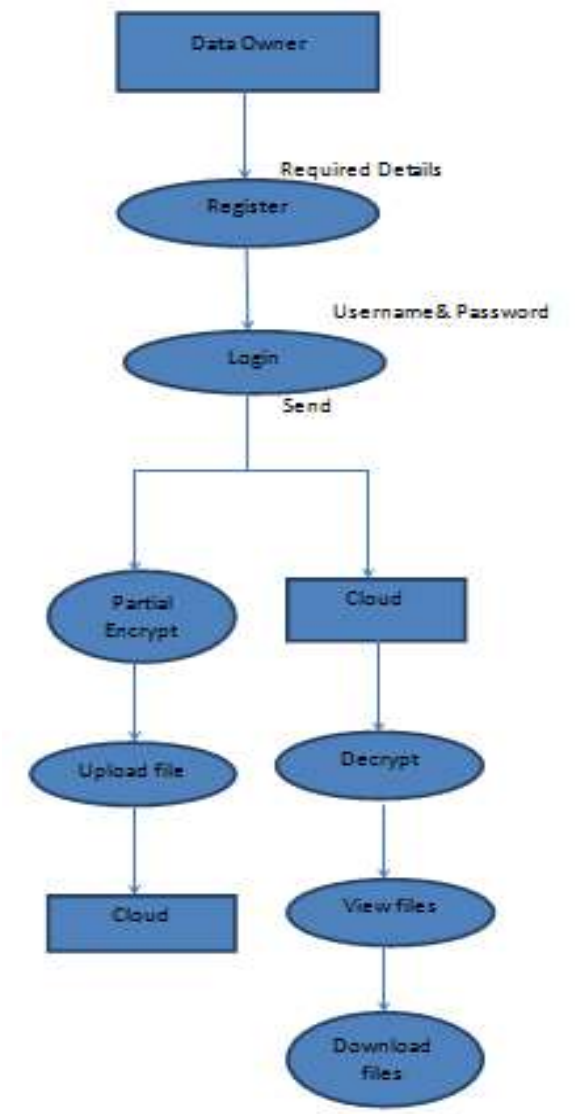

Fig-2.2.a: Data Flow Diagram 1

Data owner will register and login to the cloud server. He will partially encrypt the data and upload the files on the server as shown in fig-2.2.a.

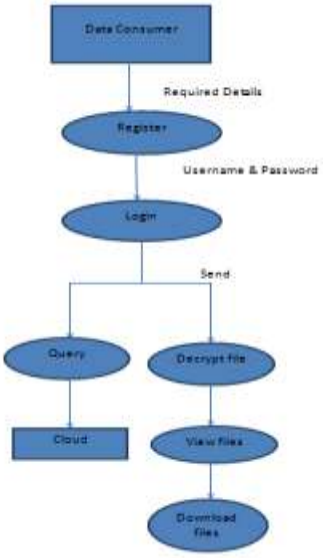

Fig-2.2.b: Data Flow Diagram 2

Data consumer will register and login to the cloud server. He will request cloud for the data. Third party certifying authority will issue a key using which the data user can access data and view or download files as shown in fig-2.2.b.

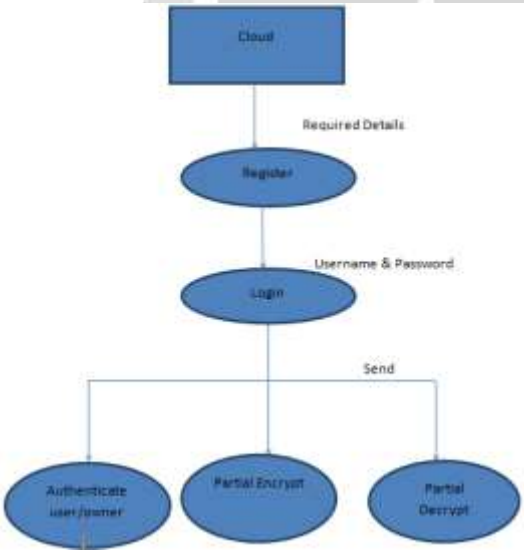

Fig-2.2.c: Data Flow Diagram 3

The cloud server will also register and login and partially encrypt and store the data as shown in fig-2.2.c.

2.3. Activity Diagram

The following diagram is drawn with four main activities:

- Upload and partial encryption by owner
- Full encryption by cloud server

- Third party authority request by user.
- Decryption and data access on cloud by user

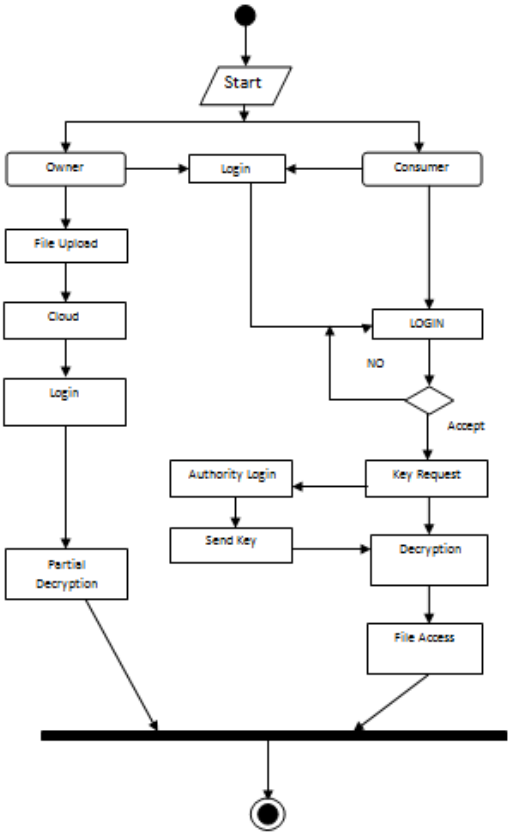

Fig-2.3: Activity diagram

2.4 Use Case Diagram

The below use case diagram fig-2.4.a shows the relation between owner and cloud created from a use case analysis. It shows the dependencies between the two main actors the owner and cloud.

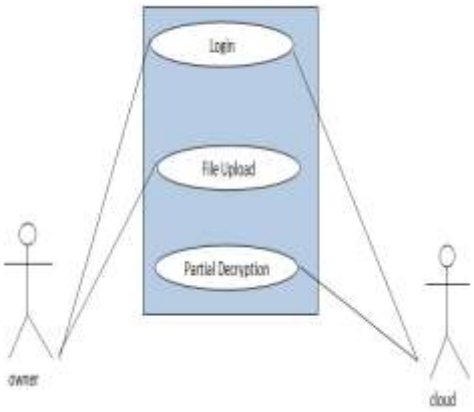

Fig-2.4.a: Use case diagram for Data Owner and Cloud

The below use case diagram fig-2.4.b shows the relation between the authority and consumer from a use case analysis. It shows the dependencies between the actors namely authority and consumer.

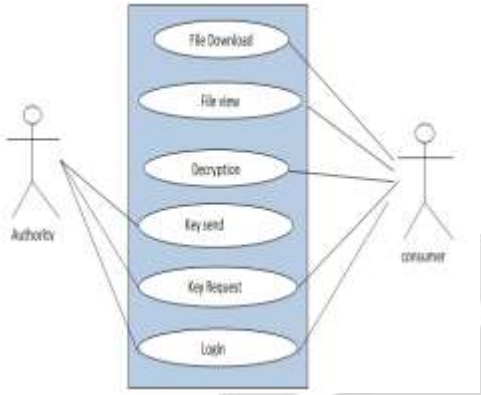

Fig-2.4.b: Use case diagram for Data Consumer and Authority

4. CONCLUSIONS

The overall goal of the project is to develop high security and cost effective storage and retrieval of data on cloud servers. The main aim of this project is to overcome the drawbacks of the existing system where the data is not very secure and the customers could be cheated for cost saving.
The Proposed System provides hybrid encryption with verifiable delegation. There is two way encryption and decryption of data for maximum security and integrity of data. 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.

5. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoicaand 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.Sahai and B. Waters, ”Fuzzy Identity Based Encryption,” in Proc. EUROCRYPT, pp.457-473, Springer-Verlag Berlin, Heidelberg, 2005.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] D. Hofheinz and E. Kiltz R, ”Secure hybrid encryption from weakened key encapsulation,” in Proc. CRYPTO, pp.553-571, Springer-Verlag Berlin, Heidelberg, 2007.

[11] 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.

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