Secured Data Sharing and Access Control for Cloud Computing Systems using CP-ABE Algorithm with Verifiable Delegation

Kavya P, Manjula S, Neethu kuwar, Nikitha R, Gururaj K S*

Department of CSE, GSSSIETW, Mysuru, Karnataka, India

DOI: https://doi.org/10.21467/proceedings.1.10
* Corresponding author email: gururaj.ks@gsss.edu.in

Abstract

In the cloud, for achieving access control and data security, data owners adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are some problems like misrepresenting or replacing the delegated cipher text, access policy may not be flexible enough during encryption and cloud servers may cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been developed. This system is combined with verifiable delegation and encrypt-then-Mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated results are well guaranteed at the same time.

Index Terms- Access control Hybrid encryption, Attribute-based encryption, Cipher text-policy, Verifiable delegation.

1 INTRODUCTION

Cloud computing is innovation which uses advanced computational power as well as improved storage capabilities. Verifying delegation process using cipher text-policy attribute-based encryption (CP-ABE) is used to guarantee the data privacy and the verifiability of allocation on untruthful cloud servers. To make data sharing secure, attribute-based encryption is used. There are two forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the second is cipher text-policy attribute-based encryption. In this work, CP-ABE is considered. In CP-ABE system, each cipher text is containing an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a cipher text if and only if the key's attribute set satisfies the access structure associated with a cipher text. The cloud server provides another service which is a delegation computing. The VD CP-ABE scheme shows that the un-trusted cloud will not be able to learn anything

 ISBN: 978-81-936820-0-5

about the encrypted message and build the original cipher text. This work will attempt to refine the definition of CP-ABE with verifiable delegation in the cloud to consider the data confidentiality, the fine-grained data access control and the verifiability of the delegation.

2 LITERATURE SURVEY

A new requirement of ABE with outsourced decryption: is verifiability. Verifiability guarantees that a user can efficiently check if the transformation is done correctly. The system gives the formal model of ABE with verifiable outsourced decryption and provides new scheme which is both secured and verifiable [1]. A new methodology for realizing Cipher Text-Policy Attribute Encryption (CP-ABE) under concrete and no interactive cryptographic assumption has been considered. This solution can encrypt or specify access control in terms of any access formula over the attributes in the system [2][3].

A new methodology for attribute-based encryption schemes for circuits of any arbitrary polynomial size has been used, where the public parameters and the cipher text grow linearly with the depth of the circuit. The construction is secure under the standard learning with errors (LWE) assumption [4].

A new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption, has been used. The new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally [5]. A system for fine-grained sharing of encrypted data that is called Key-Policy Attribute-Based Encryption (KP-ABE) has been considered. In this system, cipher texts are labelled with sets of attributes and keys are associated with access structures that control which cipher texts a user is able to decrypt [6].

3 SYSTEM DESGIN

The system architecture is a conceptual model that defines the structure, behaviour and more views of a system.

Figure 1 represents system architecture consisting of four modules such as data owner, data consumer, authority and cloud.

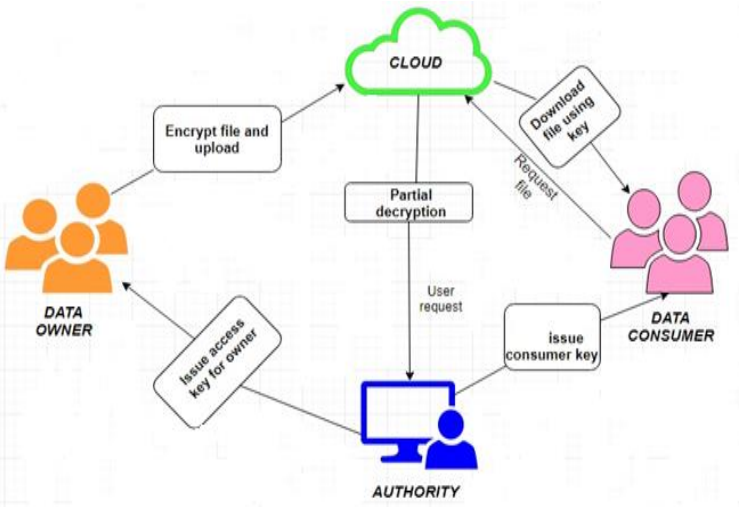

Fig 1: System Architecture

ISBN: 978-81-936820-0-5
Proceedings DOI: 10.21467/proceedings.1

Series: AIJR Proceedings

Authority: Attribute key generator centre (trusted third party).
Data owner: Encrypting party who uploads his encrypted data to the cloud.
Data consumer: Decrypting party who outsources the most overhead computation to the cloud.
Cloud server: The party who provides storage and outsourced computation services.

A use case corresponds to a sequence of transactions, in which each transaction is invoked from outside the system (actors) and engages internal objects to interact with one another and with the system surroundings. Fig 2 represents the use case diagram for owner, consumer and authority as actors in which actors can perform various operations like login, file upload, key request and file download.

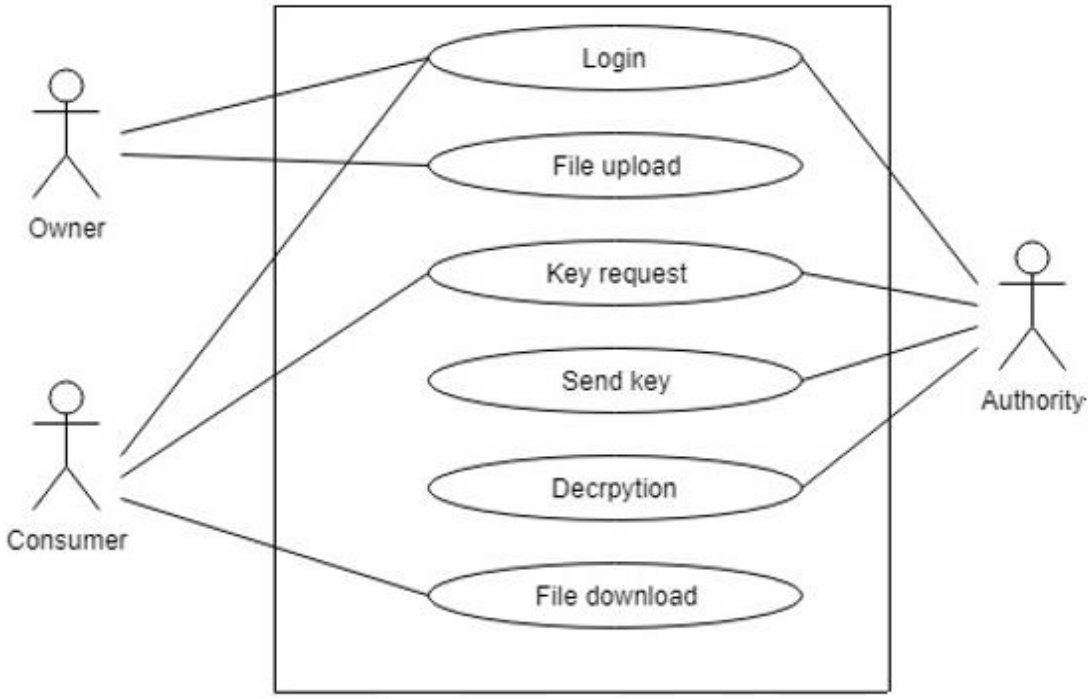

Fig 2: Use-case diagram

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. Fig 3 represents sequence diagram for consumer scenario. Consumer logs into, gets authenticated, requests key, decrypts and downloads the file.

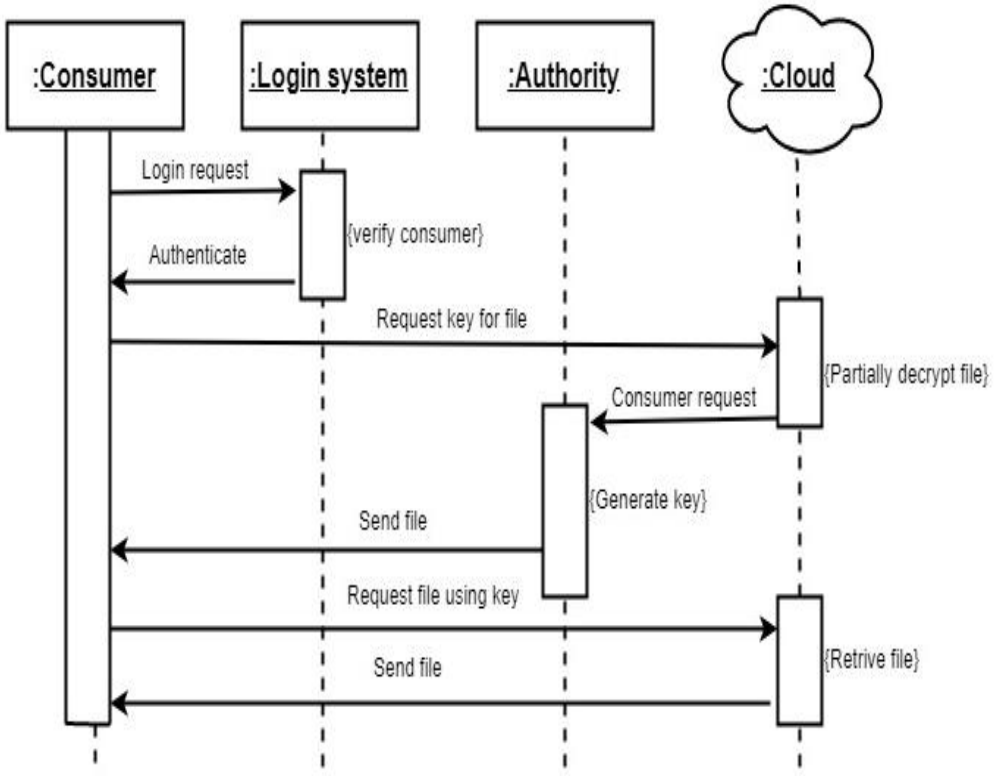

Fig 3: Sequence diagram for Consumer scenario

4 CONCLUSIONS

In this work, we have presented a circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-Mac mechanism with our cipher text policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. 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.

References

[1] J. Lai, Deng, R. H., Guan, C., and Weng, J., "Attribute-based encryption with verifiable outsourced decryption", IEEE Transactions on information forensics and security, vol. 8, pp. 1343–1354, 2013".

[2] Waters B. (2011) Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In: Catalano D., Fazio N., Gennaro R., Nicolosi A. (eds) Public Key Cryptography – PKC 2011. PKC 2011. Lecture Notes in Computer Science, vol 6571. Springer, Berlin, Heidelberg".

[3] Parno B., Raykova M., Vaikuntanathan V. (2012) How to Delegate and Verify in Public: Verifiable Computation from Attribute-Based Encryption. In: Cramer R. (eds) Theory of Cryptography. TCC 2012. Lecture Notes in Computer Science, vol 7194. Springer, Berlin, Heidelberg".

ISBN: 978-81-936820-0-5
Proceedings DOI: 10.21467/proceedings.1

Series: AIJR Proceedings

[4] Garg S., Gentry C., Halevi S., Sahai A., Waters B. , Attribute-Based Encryption for Circuits from Multilinear Maps. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013.

[5] Jin Li,Xinyi Haung,Jingwei Li "Securely Outsourcing Attribute-Based Encryption with Checkability" 21 October 2013.

[6] Ye J., Zhang W., Wu S., Gao Y., Qiu J. (2014) Attribute-Based Fine-Grained Access Control with User Revocation. In: Linawati, Mahendra M.S., Neuhold E.J., Tjoa A.M., You I. (eds) Information and Communication Technology. ICT-EurAsia 2014.