Layered Access structure attribute based encryption scheme for cloud computing

Ms. GALI JHANSIRANI1, K.SRUJANA2

1 PG Scholar, Dept of CSE, Prakasam Engineering College, Prakasam(Dt), AP, India.

2 Assoc Professor , Dept of CSE, Prakasam Engineering College, Prakasam(Dt), AP, India.

ABSTRACT

Cloud computing is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Access control is paramount as it is the first line of defense that prevents unauthorized access to the shared data. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to- end data confidentiality assurance in the cloud and beyond. Clients risk key exposure that is hardly noticed but inherently existed in previous research. Furthermore, enormous client decryption overhead limits the practical use of ABE. The proposed collaborative Mechanism effectively solves not only key escrow problem but also key exposure. Meanwhile, it helps markedly reduce client decryption overhead. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying cipher text-policy, making the computation over encrypted data a very hard problem. The proposed scheme not only achieves scalability due to its hierarchical structure.

1. INTRODUCTION

With the growing of network technology and mobile terminal, online data sharing has become a new "pet", such as Facebook, Myspace, and Badoo. Meanwhile, cloud computing is one of the best assuring application platforms to solve the dangerous expanding of data sharing. In cloud computing, to protect data from lossing, users need to encrypt their data before being shared. Access control in dominant as it is the first line of defense that prevents unauthorized access to the shared data. Recently, attribute-based encryptions (ABE) have been attracted much more concentrated since it can keep data privacy and realize fine-grained, one-to-many, and non-interactive access control. Cipher text-policy attribute based encryption (CP-ABE) is one of appropriate schemes which has much more adjustability and is more applicable for most of applications.

2.IMPLEMENTATION

In this paper we present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery. For example, it is extremely scalable by allowing a data owner to grant data access privileges based on the data consumers' attributes (e.g., age, nationality, gender) rather than an explicit list of user names; and it ensures data privacy and exclusiveness of access of scalable media by employing attribute-based encryption. For this purpose, we introduce a File Hierarchy Ciphertext Policy Attribute Based Encryption (FH-CP-ABE) technique. FH-CP-ABE encrypts multilevel access structure within integrated cipher text, so as to enforce flexible attribute-based access control on scalable media. Specifically, the scheme constructs a content key which is used to FH-CP-ABE encryption, encrypts media units with the corresponding keys, and then creates Content Key Ciphertext (CT). User can decrypt the Content Key Ciphertext by using FH-CP-ABE decryption into decrypted content key. Then content keys can be decrypted using symmetric decryption algorithm (DES, AES). The scheme offloads computational intensive operations to cloud servers while without compromising user data privacy.

J. Bethencourt, Amit Sahai, Brent Waters [11], a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements. The system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. The system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. In the future, it would be interesting to consider attribute-based encryption systems with different types of expressibility.

Lightweight devices, such as radio frequency identification tags, have a limited storage capacity, which has become a bottleneck form any applications, especially for security applications. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic tool, where the encryptor can decide the access structure that will be used to protect the sensitive data. However, current CP-ABE schemes suffer from the issue of having long decryption keys, in which the size is linear to and dependent on the number of attributes. This drawback prevents the use of lightweight devices in practice as storage of the decryption keys of the CP-ABE for us ers. In this paper, we provide an affirmative answer to the above long standing issue, which will make the CP-ABE very practical. We propose a novel CP-ABE scheme with constant-size decryption keys independent of the number of attributes.[15]

System Framework of FH-CP-ABE:
As illustrated in Fig. 1, the system model in cloud comput-ing is given, which consists of four different entities:
authority,CSP, data owner and user. In this work, we assume that data owner has k files with k access levels and

M ={m1,..., mk }is shared in cloud computing. Here, m1 is the highest hierarchy and mk is the lowest hierarchy. If a user can decrypt m1,the user can also decrypt m2,..., mk .

1.Authority: It is a completely trusted entity and accepts the user enrollment in cloud computing. And it can also execute Setup and KeyGen operations of the proposed scheme.

2.Cloud Service Provider (CSP): It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible. In the proposed system, it provides ciphertext storage and transmission services. Data Owner: It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access structure and executing Encrypt operation. And it uploads ciphertext to CSP.

3.User: It wants to access a large number of data in cloud system. The entity first downloads the corresponding ciphertext. Then it executes Decrypt operation of the proposed scheme.

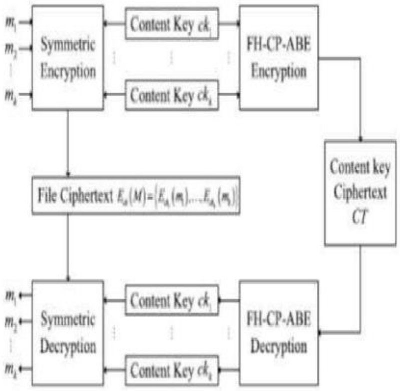

Fig.1.The system framework of FH-CP-ABE scheme.

4.Mathematical Model

- Set theory : Let S = I,P,R,O,K
- Where,
- S: Public integrity auditing system.
- I: Set of inputs.
- P: Set of processes.
- R: Rules or constraints.
- K: Keyword
- O: Set of outputs/Final output.
- I = i1, i2,.....,in
- Where,
- i1,i2,...,in = Files shared by the users.
- P=p1, p2, p3, p4, p5, p6, p7
- Where,
- p1: Key generation
- p2: Generate commitment string
- p3: Open
- p4: Verify
- p5: Update.
- p6: Proof Update.
- R = r1
- Where,
- r1: Revoked user should not be able to access files shared by users.
- r2: Proper keyword should be extracted.
- Where,
- O1: Valid user cloud access any file.

Output:-

- Result(Z) ={In,Pn,Rn}
- In->i1,i2,i3,.....in(Share file)
- Pn-> p1,p2,p3,....pn(process)
- Rn-> r1,r2,r3.........Rn(Revocation)
- Result(Z) = {pi, 0<I<k}........set of probability
- ~Result(Z) = {pi,(K,mi),{false otherwise}}
- here , K(Z) = {ki, 0<I<n} Set the keyword.

5.CONLUSION

We proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing. The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to be secure under DBDH assumption.

5. REFERENCES

[1] C.-K. Chu ,W.-T. Zhu, J. Han, J. –K. Liu, J. Xu, and J. Zhou, Security concerns in popular cloud storage services, IEEE Pervasive Computing., vol.12,no.4,pp.5057,Oct./Dec.2013.

[2]T. Jiang , X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, TIMER: Secure and reliable cloud storage against data re-outsourcing, in Proc. 10th Int. Conf. Inf. Secure.Pracr.Exper.,vol.8434.May 2014,pp.346358.

[3]K. Liang, J. K.. Liu, D. S. Wong, and W. susilo, An efficient cloud based revocable identity-based proxy re-

encryption scheme for public clouds data sharing, in Proc.19th Eur.Symp.Res.Comput.Secure.,vol.8712.Sep.2014,pp.257272.

[4]T.H. Yuen, Y. Zhang, S.M. Yio, and J.K. Liu, Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks, in Proc. 19th Eur.Symp. Res. Comput. Secure., col. 8712.Sep.2014,pp.130147.

[5] K. Liang et al., A DFA-based functional proxy re-encryption scheme for secure public cloud sharing, IEEE Trans. Inf. Forensics Security, vol.9, no.10, pp.16671680, Oct.2014.

[6]T.H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, k-times attribute-based anonymous access control for cloud computing, IEEE Trans.Comput.,vol.64,no.9,pp.25952608,Sep.2015.

[7] J.K. Liu, M.H. Au, X. Hiang ,R. Lu, and J. Li, Fine-grained two factor access control for Web-based cloud computing services, IEEE Trans. Inf. Forensics Security,vol.11,no.3,pp.484497,Mar.2016.

[8] A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp.457473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in Proc.13th ACM Conf. Comput. Commun. Secur., Oct.2006,pp.8998.

[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, Efficient attribute-based encryption from R-LWE, Chin. J. Electron., vol.23, no.4, pp.778782, Oct.2014.

Author's Profile

Ms. GALI JHANSIRANI

recevied B.Tech in Computer Science and Engineering from PRAKASAM Engineering college,kandukur affiliated to the Jawaharlal Nehru Technological University,Kakinada in 2015, and pursuring M.Tech in Computer Science and Engineering from PRAKASAM Engineering College affiliated to the Jawaharlal Nehru Technological University, Kakinada in 2015- 18 respectively.

K.SRUJANA

Working as a Assoc. Professor in Prakasam Engineering College, Kandukur, since jan 2011 to Tilldate.

Shee Is Dedicated To teaching Field From The Last 17 Years. She Has Guided 15 P.G Students And 25 U.G Students.

She Is Highly Passionate And Enthusiastic About her Teaching And Believes That Inspiring Students To Give Of Her Best In Order To Discover What She Already Knows Is Better Than Simply Teaching.