DOI: http://dx.doi.org/10.26483/ijarcs.v9i3.6118

ISSN No. 0976-5697

Volume 9, No. 3, May-June 2018

International Journal of Advanced Research in Computer Science

SURVEY PAPER

Available Online at www.ijarcs.info

AN EXTENSIVE STUDY TOWARDS ACHIEVING FINE GRAINED ACCESS CONTROL ON ENCRYPTED CLOUD DATA

M.Amsaveni, R.Shankar and S.Duraisamy
PG and Research Department of Computer Science
Chikkanna Govt Arts College Tirupur,Tamil Nadu,India.

Abstract: Outsourcing of business, Scientific and engineering data application on the Third party administrative cloud server have been increasing from the past decade. Unfortunately many servers disregard the security requirement which entails serious security concerns. To provide Confidentiality on the shared sensitive data, many cryptographic technique are usually applied in large numbers though it has lead to serious challenges in the cloud storage against data sharing.In this paper, we study on achieving fine grained access control on encrypted cloud data against several kinds of attacks propagating to the cloud servers such as key leakage attack, Cipher text attack by deducing the key for encryption and decryption. Fine grained access control is employed against encrypted data. In addition to more advantage, the access control mechanism also faces several issues in terms of automatic revocation. In order to handle implication of this study, we plan to propose an Ensemble operator on the Fine grained access control through Time, Location and Profile constrainst on the access policy to the attribute set defined. In this notion, expensive access policy generation for decryption of the cipher text is offloaded to the cloud to some extent. Even obtaining encryption key and decryption key, attacker will not help in decrypting the ciphertext. The proposed notion is used as key encapsulation mechanism to the data outsourced to cloud via third party application. Through extensive analysis on different fine grained access control mechanism on the outsourced data, the ensemble operator model can gain significant performance to highlight the scalability and efficiency.

Keywords: Secure Data Sharing Models, Fine Grained Access Control, Key Leakage Attack, Cipher Text Attack, Cloud Computing, Outsourced data Security

1. INTRODUCTION

Cloud services are growing exponentially through various sizes of cloud service providers, cloud storage service acts primary requirement to user of the cloud, however Security of outsourced data to the cloud represents a key concern for users[1][2]. There exists much risk to outsourced data in terms of data leakage. To secure outsourced data, the cryptographic schemes are usually applied to provide data integrity and data confidentiality. Among many scheme Attribute based Encryption is used in large extent. Attribute based Encryption is used to protect the confidentiality and integrity of outsourced data and further it is used to provide fine-grained access control against various access policy defined with constrainst. It may become one of the promising candidates to address the security concern in cloud computing. The security of cryptographic schemes initiates from the providing privacy to data through cryptographic key. Nowadays cryptography keys been exposed by cryptanalyst which is termed as key exposure problem [3]. There exist many techniques to prevent the key exposure such as key-insulated public key technique [4] and parallel key insulated public key technique [5]. In Particular, Key insulated solution fails by imposing employing brute force attack or pollution attack. To the best of our knowledge, the key exposure protection and automatic revocation solution in cloud storage is not employed.

The proposed model can be been defined in terms of ensemble operator in terms of Time, Location and Profile as access constrainst for data decryption and automatic revocation of user. The defined model can be mentioned as key encapsulation mechanism. The model can reduce expensive access policy generation for decryption of the cipher text. The rest of the section is organized as follows, section 2 describes the review of literature followed by section 3 to define the proposed methodology as outline and finally section 4 concludes the study of the paper.

.

2. REVIEW OF LITERATURES

In this section, we describe the existing methods applied to cloud data security by incorporating the access control mechanism through usage of Attribute based encryption technique. Further review of literature is sectioned into Methods on Key Exposure Prevention Technique and Automatic Revocation Technique

2.1.Key Exposure Prevention Techniques

The key Exposure Techniques is developed utilizing multiple conceptual processes, each method is described in detail

2.1.1. Attribute based encryption with efficient verifiable outsourced decryption

In this literature, Fine grained access control is enabled in terms of attribute-based encryption (ABE) in order to prevent the outsourced data against the malicious attack propagating in the cloud through inclusion of outsourced decryption. The ABE Scheme reduces cipher text size and decryption cost on the developed encryption model. In particular, ABE scheme transforms the outsourced data into EI Gamal Type Cipher text using public key cryptosystem with data owner supplied keys so that decryption process can be made simple and secure. However, a shortcoming of the outsourced data through ABE scheme is that the implementation of the secure protocol on the cloud server's towards data transformation cannot be verified by the user of the data. Also data user can be compromised with wrongly transformed output.

This mechanism formalizes a security model of ABE scheme by integrating the verifiable decryption mechanism on the outsourced data with presence of a verification key. It is verified on the generated ciphertext. The re-formalized model is to transform ABE scheme along verifiable decryption in order to consider it as optimal solution [6]..

2.1.2 k-times attribute-based anonymous access control for cloud computing

In this literature, k-times attribute-based anonymous access control is analysed for outsourced data in cloud. The model authenticates the user k times for data disclosure to demanding user. Access policy is defined through iterative condition to reduce the burden of the decryption cost[9]. The Access policy iterates the anonymously on attributes to authenticate the user to data access. K limit is provided for anonymous access. That is, the server may limit a particular set of users (i.e., those users with the same set of attribute) to access the system for a maximum k-times within a period or an event. Further additional access will be denied.

2.1.3. An Efficient Privacy-Preserving Outsourced Calculation Toolkit with Multiple Keys

In this literature, an efficient privacy Preserving Outsourced Calculation Toolkit with Multiple Keys is been analysed [11]. Using EPOM, a large scale of users can securely outsource their data to a cloud server for storage using ABE scheme. Moreover, encrypted data belonging to multiple users can be processed without compromising on the security of the individual user's (original) data and the final computed results in terms of fine grained access control principles. To reduce the associated key management cost and private key exposure risk in EPOM, we discuss a distributed two-trapdoor public-key cryptosystem, the core cryptographic primitive. We also present the toolkit to ensure that the commonly used integer operations can be securely handled across different encrypted domains. We then prove that the EPOM achieves the goal of secure integer number processing without resulting in privacy leakage of data to unauthorized parties. Last, we demonstrate the utility and the efficiency of EPOM.

2.1.4 Enabling Cloud Storage Auditing With Key-Exposure Resistance

In this literature, author discusses a new secure mechanism named as enabling storage auditing mechanism through inclusion of h Key-Exposure Resistance on the cloud server will be discussed. The new aspect of the cloud storage auditing against key disclosure is performed. The solution reduces the damage of the client's key exposure. The Solution incorporates the preorder traversal technique for data indexing and binary tree structure is been used for data transformation towards strengthening the data auditing. The solution leads as firewall to data access as key-exposure resilience [12]. The authenticator also enabled in this auditing mechanism in order to support the forward security and to blockless verification of the data in cloud. The security and performance analysis describes that analysed system is more secure and efficient against various direct attacks.

2.2.User Revocation Scheme against Access Violation

Automatic revocation against the access violation is been modelled using various models is described below

2.2.1. Hierarchical Attribute Based Access Control Mechanism

In this literature, a hierarchical attribute-based access control in cloud computing is been analysed in detail to model a secure data sharing model on the outsourcing data in terms of flexibility and scalability [7]. More frequently ABE scheme is employed to secure the outsource data. However ABE implementation without optimization fails against the complex access control policies. Through incorporation of hierarchical attribute-set-based encryption by extending ciphertext-policy attribute-set-based encryption in order to achieve hierarchical structure to the data outsourced and to the cloud users, it is possible to increase to scalability and flexibility. The scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE.In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by analyzing its performance and computational complexity.

2.2.2. Extended proxy-assisted approach: A Revocable fine-grained encryption Method

In this literature, extended proxy assisted approaches mitigates Automatic user revocation within the ABE Scheme remains a challenging issue to overcome with large number of user. The proposed model incorporates all or nothing transformation approach to in order to prevent the cloud data server from data colluding attack with incorporation of third party auditor to simplify the user revocation functionality [8].

2.2.3. Fully secure revocable attribute-based encryption

In this literature, fully secure revocable Attribute based encryption is been analysed against the complex access control upon the attributes to protected and fixing the access policies. The System uses adaptive model for security to the outsourced data by enabling and enforcing ABE to generate the encrypted data based on access constrainst. The Solution also produces the automatic revocation based on number of usage violation. Though extensive analysis, it proved that system produces high efficiency and flexibility against the public parameters [9].

2.3. Tabular View of the Review of literatures

SI.No	Problem	Title	Objective	Advantages
1	Data transformation cannot be verified by the user of the data	Efficient verifiable outsourced decryption using ABE	Verifiable outsourced decryption can verify the transformed data on the data user end	Reduced Cipher text size and less computation cost
2	Complex Access policy may provide gateway to the attacker	Hierarchical attribute-based solution	System inherits flexibility and fine-grained access control in supporting compound attributes of Attribute Set Based Encryption	Multiple value assignment provides access expiration time for access provider
3	Access Specification against the data disclosure leads to huge decryption time	k-times attribute-based anonymous access control	K limit provision on the access policy modelling provide to anonymous data access	It reduces the decryption cost
4	Access policy fails with large number	Extended proxy-assisted approach	all or nothing transformation	Prevents authorized

	of data user		approach is used against the Colluding attack	access against through access key exposure
5	complex access control upon the attributes to protected and fixing the access policies	Fully secure revocable attribute-based encryption	Automatic revocation based on number of usage violation	System increase the scalability and flexibility based on periodic withdraw of access.
6	Large users scenario leads to key management and key exposure risk	An Efficient Privacy-Preserving Outsourced Calculation with Multiple keys	Distributed two-trapdoor public-key cryptosystem	Utility rate of this particular model is high
7	Client key exposure in cloud storage auditing is high as it not updated	Enabling Cloud Storage Auditing With Key-Exposure Resistance	Binary tree structure and the preorder traversal technique method included to secure the keys shared.	System is secure and efficient with periodic key updates automatically.

3. OUTLINE OF THE PROPOSED MODEL

The proposed model is outlined from the implication of this extensive study through imposing an Ensemble operator on the Fine grained access control through Time, Location and Profile constrainst on the access policy to strengthen the ABE scheme towards achieving the automatic revocation and key exposure resilience. The proposed idea is considered as key encapsulation mechanism for outsourced data to cloud. This model acts as resistant to the possible attacker's scenario along learning-with errors assumption. The primary technical hurdles can be addressed through implementation of proposed model.

4. CONCLUSION

In this study, we have carried out extensive study towards achieving fine grained access control on the outsourced cloud data by incorporation of the cryptographic primitives. The Cryptographic primitives uses ABE scheme to generate the access policy to mitigate key management issues and computation issue has been analysed in detail. In addition, solutions to Key exposure attack, Guessing attack and brute force attack has been discussed. In particular, automatic revocation and key exposure resilience solution has been defined as ensemble operator to describe it as a novel proposed solution. Though extensive analysis, it is verified that cloud security mechanism has to be focused much on several aspects to provide service with data confidentiality, scalability and data integrity.

5. REFERENCES

[1] W. Yau, R. Phan, S. Heng, B. Goi, "Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester, 2013" in International Journal of Computer Mathematics, ,volume 90, Issue: 2, pp. 2581-2587

[2] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, "Toward secure and dependable storage services in cloud computing," Services Computing, IEEE Transactions on, vol. 5, no. 2, pp. 220–232, 2012.

[3] Y. Zhu, H. Hu, G.-J. Ahn, M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Transactions on Parallel Distributed Systems, vol. 23, no. 12, pp. 2231–2244, 2012.

[4] Y. Dodis, J. Katz, S.Xu,M. Yung, "Key-insulated public key cryptosystems," in Advances in Cryptology–EUROCRYPT 2002 in Springer, volume.2332 ,pp. 65–82.

[5] B. Libert, J.J.Quisquater, M. Yung, "Parallel key-insulated public key encryption without random oracles," in Public Key Cryptography 2007, Springer, pp. 298–314.

[6] Baodong Qin, Robert H Deng, Shengli Liu, Siqi Ma" Attribute based encryption with efficient verifiable outsourced decryption" 2015. In IEEE Transactions on Information Forensics and Security, volume.10, issue 7,pp:1384–13935.

[7] Zhiguo Wan, Jun'e Liu, and Robert H Deng. Hasbe: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE transactions on information forensics and security, 7(2):743–754, 2012.

[8] Yanjiang Yang, , Jianyong Zhou. Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data. 2015, In Computer Security - ESORICS 2015, pp 146–166.

[9] Hon Yuen, Joseph K Liu, Man Ho Au, Xinyi Huang, Willy Susilo, Jianying Zhou. k-times attribute-based anonymous access control for cloud computing. IEEE Transactions on Computers, 64(9):2595–2608, 2015.

[10]. J.Qian X.Dong,"Fully secure revocable attribute-based encryption"2011,Journal of Shanghai Jiaotong University (Science), vol. 16, pp. 490–496.

[11] Ximeng Liu,Robert H. Deng ,Kim-Kwang Raymond Choo , Jian Weng"An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys"IEEE Transactions on Information Forensics and Security in Volume: 11, Issue: 11, Nov. 2016

[12]. Jia Yu, Kui Ren, Cong Wang,Vijay Varadharajan "Enabling Cloud Storage Auditing With Key-Exposure Resistance" IEEE Transactions on Information Forensics and Security in Volume: 10, Issue: 6, June 2015