IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 1, January 2020

Survey of Access Control Techniques Based on CP-ABE Scheme to Ensure Secure Access of Multimedia Data in Cloud Storage

Kavyasri M N[1], Ramesh B[2]

Assistant Professor, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India[1]

Professor, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India[2]

Abstract: With the development and benefits of cloud computing more and more users outsources their data to third party cloud storage for ease of sharing and cost saving. Security of the outsourced data has become the core problem of cloud computing. Many security models have been proposed, in which Cipher Text-Policy Attribute Based Encryption is considered as an efficient tool for fine grained data access in the cloud storage system. The practical applications of CP-ABE in cloud has own inherent challenges regarding user revocation, cipher text size, and number of user attributes, access structures and many more. There are many works proposed to address these problems from various researches. This paper gives the overview of various research works based on CP-ABE. The performance analysis of these works is carried out.

Keywords: Collaborative Key Management, Distributed Key Management System, Access Control, Conjunctive Keyword Search, Dispensability Matrix

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. As a promising computing paradigm, it has drawn extensive attention from both academia and industry in recent years. There is an emerging trend that more customers increasingly began to use the public cloud storage for online data storing and sharing. However, these data applications in cloud storage are obstructed by some security issues, such as data confidentiality and information leakage. Once the users outsource their private data to the public cloud Large scaled That threatens the privacy of data owner. As number of user increase challenges like data security and access control arise. To maintain confidentiality of data some cryptographic technique can be used. Encryption and decryption introduce heavy computational overhead on data owner and users. To achieve effective privacy preserving and data sharing service in cloud new technique is introduce called Attribute Based Encryption (ABE) scheme .Attribute Based encryption technique provide solution to secure and flexible data sharing. ABE use fine grained access control scheme. In which each user is associated with access structure. Access structure defines the scope of files user allowed to access. Attribute Based Encryption (ABE) has one- to-many inherent property. ABE Comes in two classes called Ciphertext Policy (CP-ABE) & Key Policy (KP-ABE). In a KP-ABE scheme, the ciphertext is associated with a set of attributes and the user's private key is associated with an access structure. In a CP-ABE scheme, the ciphertext is associated with an access structure and the user' private key is associated with a set of attributes. Since the access policy is determined by the data owner in CP-ABE, which is conceptually closer to traditional access control methods such as role-based access control that provides fine-grained access control over encrypted data, it is more suitable for access control applications in cloud environment. There is more work proposed with respect to CP-ABE scheme. This paper presents survey of techniques which proposed methods to overcome disadvantages posed by basic CP-ABE scheme

II. ACCESS CONTROL SCHEMES

A. Collaborative Key Management scheme: Paper presented new collaborative key management scheme in Ciphertext Policy Attribute Based Encryption for Cloud is proposed to enhance security and efficiency in key management. Which uses the concept of distribute key generation, issue and storage of private key. Which minimize the problem of key exposure which is hardly address by previous research. Specialized attribute group are used to build private key update and immediate attribute revocation. Decryption server is used to optimize user experience by minimizing decryption load. Thus systems perform better in cloud data sharing system with respect to security and efficiency.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 1, January 2020

B. An Efficient CP-ABE scheme for Big Data Access Control in Cloud Computing: The work is proposed to design efficient CP-ABE method for big data access control in the cloud by the following. Privacy: Sensitive personal information is not disclosed to others. Access control: Only authorized users of the system are able to access the data. Efficiency: Less computation overhead should be achieved for encryption and decryption process by designing the short ciphertext and minimize the pairing operations required. It proposes the efficient ciphertext policy attribute based encryption scheme for big data access control in cloud computing with the access tree as an access policy. Sheme achieves less computation overhead in encryption by designing short ciphertext and decryption process by reducing the number of pairing operations required. The security of this scheme is proved against chosen-plaintext and the collusion attacks.

C. Hidden Policy Ciphertext-policy Attribute Based Encryption with Conjunctive Keyword Search: The work presents designing of novel CP-ABKS scheme which supports conjunctive keyword search and preserves the privacy of the access policy. Proposed scheme can resist KGA. A server is designated by the data owner to perform the test operation in our scheme. The test algorithm could not function without the server's private key., the security of scheme can be proved in the standard model rather than the random oracle model. Proposed work guarantees the privacy of access structure and enrich the search functionality in ABKS, it proposes hidden policy ciphertext-policy attribute based encryption with conjunctive keyword search (HP-CPABCK) scheme. The data owner realizes a fine-grained authorization of the data users by specifying a hidden access policy in the keyword ciphertext. By designating the test server, the proposed HP-CPABCK scheme achieves resisting KGA. Additionally, the HP-CPABCK scheme can be shown to be secure in the standard model. The performance analysis demonstrates the applicability of the HP-CPABCK scheme.

D. Privacy Preserving Ciphertext Policy Attribute based Encryption Scheme with Efficient and Constant Ciphertextsize: Work presents an efficient construction of privacy preserving CP-ABE with constant ciphertext size that enforces meaningful data access policies irrespective of the number of user attributes. This work explores redundant user attributes from the set of user attributes defined by the data access policy through the construction of dispensability matrix. It proposed, a privacy-preserving CP-ABE scheme with constant size ciphertext has given. The major advantage of the proposed system is that it reduces the ciphertext length to a constant ciphertext size with any number of the user given attributes in a meaningful manner. Which is the major drawback in existing CP-ABE schemes. Further, it achieves the properties of data privacy and fine-grained access provision through the implementation of dispensability matrix. Though this work provides the better solution to the problem of user Access policy specification in CP-ABE schemes, it does not consider the issue of user attribute management. In future, this work can be extended to provide efficient user attribute management processes.

E. Modified Hierarchical Attribute-Based Encryption: The work proposed a modified HABE scheme by taking advantages of Attributes Based Encryption (ABE) and Hierarchical Identity Based Encryption (HIBE) access control processing. The proposed access control method using M-HABE is designed to be utilized within a hierarchical multi-user data-shared environment, which is extremely suitable for a mobile cloud computing model to protect the data privacy and defend unauthorized access. Compared with the original HABE scheme, the novel scheme can be more adaptive for mobile cloud computing environment to process, store and access the enormous data and files while the novel system can let different privilege entities access their permitted data and files. The scheme not only accomplishes the hierarchical cloud computing model, but protects the data from being obtained by an untrusted third party.

Table I: Table Showing Nature of Encryption Key and Access Policy Used in Various Works

Scheme	***Objective***	***Encryption key***	***Access policy***	***advantages***
Collaborative Key Management in Ciphertext Policy Attribute Based Encryption	To enhance security and efficiency in key management. Addresses escrow problem	Distributed key generation	Based on specialized attribute group	Minimizes the problem of key exposure
An Efficient Ciphertext Policy-Attribute Based Encryption for Big Data Access Control	is to design efficient CP-ABE method for big data access control in the cloud by providing security, access control and confidentiality	Short cipher text	Access tree	scheme achieved less computation overhead in encryption by designing short ciphertext and decryption process by reducing the number of pairing operations required

Hidden Policy Ciphertext-policy Attribute Based Encryption with Conjunctive Keyword Search	scheme which supports conjunctive keyword search and preserves the privacy of the access policy	Conjunctive keyword search	hidden policy ciphertext-policy	It supports conjunctive keyword search and preserves the privacy of the access policy and can resist KGA
Privacy Preserving Ciphertext Policy Attribute based Encryption Scheme with Efficient and Constant Ciphertextsize x	define an efficient construction of privacy preserving CP-ABE with constant ciphertext size that enforces meaningful data access policies irrespective of the number of user attributes	Constant cipher text size	construction of dispensability matrix.	proposed system is that it reduces the ciphertext length to a constant ciphertext size with any number of the user given attributes in a meaningful manner
A Modified Hierarchical Attribute-Based Encryption Access Control Method	proposed a modified HABE scheme by taking advantages of attributes based encryption (ABE) and hierarchical identity based encryption (HIBE) access control processing	Variable cipher text size	Access structure determines what cipher text can be obtained by which user	scheme can be more adaptive for mobile cloud computing environment to process, store and access the enormous data and files while the novel system can let different privilege entities access their permitted data & files.

III. CONCLUSION

With concern of data security many organizations are worried about that so main task is to provide security and privacy of confidential data. Our main aim is to provide security during access of data. Various methods were proposed based on various techniques like those being explained in the paper. Analyses of those methods are done and the results are given in the table.

REFERENCES

[1]. S. S. Muthukumaran & T. Ramkumar “An Approach forEnhancing Secure Cloud Storage Using Vertical Partitioning Algorithm”, Middle-East
[2]. N. N. Pathak , M. Nagori “Enhanced security for multi cloud storage usingnAES algorithm”, International Journal of Computer Science and Information Technologies, vol. 6 , pp. 5313-5315, 2015. Journal of Scientific Research, vol.23,no. 2, pp. 223-230, 2015.
[3]. Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Security and Privacy Challenges in Cloud Computing Environments." IEEE Security & Privacy 8.6 (2010): pp. 24-31.
[4]. Xiaojie Niu. “Fine Grained access control scheme based on cloud storage, international conf on computer network, Electronic & Automation
[5]. AYA: an efficient access controlled storage and processing for cloud based sensed data
[6]. Wang, F., Chang, C.-C., Harn, L., “Simulatable and secure certificate-based threshold signature without pairings,” Security and Communication Networks, 2013, 7, (11), pp. 20942103.
[7]. Fournaris, A.P., “A distributed approach of a threshold certificate-based encryption scheme with no trusted entities,” Inf. Secure. J. Glob. Perspect., 2013, 22, (3), pp. 126139
[8]. Kate, A., Goldberg, I., “Distributed key generation for the internet,” Proc. 29th IEEE Int. Conf. on Distributed Computing Systems (ICDCS 90) [9] Montreal, Quebec, Canada, June 2009, pp.119-128.
[9]. Pakniat, N., Noroozi, M., Eslami, Z., “Secret image sharing scheme with hierarchical threshold access structure,” J. Vis. Commun. Image Represent., 2014, 25, (5), pp. 10931101
[10]. Nasrollah Pakniat, Mahnaz Noroozi, Ziba Eslami., “Distributed key generation protocol with hierarchical threshold access structure,” 2014, ISSN 1751-8709
[11]. H. Yan; J. Li; J. Han; Y. Zhang, "A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage," in IEEE Transactions on Information Forensics and Security , vol.PP, no.99,pp.1-1 doi: 10.1109/TIFS.2016.2601070
[12]. G. Murali and R. S. Prasad, "CloudQKDP: Quantum key distribution protocol for cloud computing," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai,2016, pp. 1-6.
[13]. J. Prakash, V. R. Uthariaraj and B. L. Elizabeth, "Efficient KeyManagement Protocol with Predictive Rekeying for Dynamic Networks," 2016 2nd International Conference on Green High PerformanceComputing (ICGHPC), Nagercoil, 2016, pp. 1-6.