International Journal of Advanced Engineering Research and Science (IJAERS) *[Vol-3, Issue-12, Dec- 2016]*
https://dx.doi.org/10.22161/ijaers/3.12.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

Attribute-Based Data Access Policy & Key Escrowing Problem: A Review Paper

Mr. Sourabha Vijaykumar Pashte, Prof.Mr. Chetan J. Awati

Department of Technology, M. Tech. Computer Science and Technology, Shivaji University, Kolhapur, Maharashtra, India

Abstract—*Cloud storage is the best & efficient way to handle our data remotely. However, since data owners and users are usually outside the trusted domain of cloud service providers the data security and access control is the important factor at the time of sensitive data stored in the cloud. Moreover, now days there are different mechanisms are available for data sharing & preserving privacy of data owner & user. Key Escrow is the one of the major issue now a day. We can't keep full trust over the key authority center because they may be misuse there privileges. This is unsuitable for information sharing situations. In this paper we studied the existing technique for sharing the data from data owner to data user.*

Keywords— Data Confidentiality, Key Authority, Attribute based schemes, Access Control policy, Data Sharing.

I. INTRODUCTION

N ow a days there are lots of fast growing trends & cloud computing is one of them. Cloud provide easy ,efficient platform to store data, secure data, & access data at any location with the help of internet. Also it provides user flexible infrastructures, storage space and performance.

Important factor in cloud storage are Data confidentiality & performance. To maintain data securely from unauthorized access lots of cryptographic algorithms are present. Trusted third parties are also playing main role in cloud computing which providing us secure channel for transferring the data from owner to other requested different users.

Existing system uses the cipher text policies based encryption in which confidentiality of the data are made by using data, encryption algorithm & the size of key.

Trusted third party like key authority, key generators & providers, digital certificate providers & verifiers etc used in this scenario. But we cannot keep fully trust over these service providers & trusted parties. Not all but some of them may be can try to steal our data & keys. Due to this key Escrow issue may be generated under this kind of system.

Normally all the tasks are done over the cloud such as authentication, file encryption, file decryption, key management and so on. There are lots of users are active concurrently from different location & performing lots of different operations. So performance of the cloud system may be degrading in future. To deal with these major issues of existing system I propose this system. In which we make small change in the Attribute-based policies & remove the key escrow problem completely.

Now we will go through some existing system related to data sharing & confidentiality over cloud in short & some of their disadvantages.

II. LITERATURE SURVEY

There are many policies are defined regarding cloud computing security & data sharing as per in the literature.

A. Revisit Attribute-based Data Scheme

Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, Weixin Xie [1] revisit attribute-based data sharing scheme in order to solve the key escrow issue but also improve the expressiveness of attribute, so that the resulting scheme is friendlier to cloud computing applications. They proposed an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. Moreover, they introduce the concept of attribute with weight, being provided to enhance the expression of attribute, which can not only extend the expression from binary to arbitrary state, but also lighten the complexity of access policy. Therefore, both storage cost and encryption complexity for a cipher text are relieved.

B. File Hierarchy Attribute-Based Scheme

An efficient file hierarchy attribute-based encryption scheme(FH-CP-ABE) is proposed by Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen and Weixin Xie [2]. The layered access structures are integrated into a single access structure, and then the hierarchical files are encrypted with the integrated access structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CPABE with a

https://dx.doi.org/10.22161/ijaers/3.12.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.

C. Two Factor Authentication

Introduced [3] a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfils the required predicate, but has no idea on the exact identity of the user.

D. User-Centric Data Creation Scheme

In [5] this paper author proposed a User-centric data secure creation scheme (UCDSC) for the security requirements of resource owners in cloud. In this scheme, a data owner first divides the users into different domains. The data owner encrypts data and defines different secure managing policies for the data according to domains. To encrypt the data in UCDSC, they present an algorithm based on Access control conditions proxy re-encryption (ACC-PRE), which is proved to be master secret secure and Chosen-cipher text attack (CCA) secure in random oracle model. The ACC-PRE can reduce the computational overhead of the user's encryption and difficultly of key management, and satisfy the users' requirements for dynamical adjustment of permission descriptions as well.

E. Attribute-Based Proxy Re-Encryption

Kaitai Liang and Willy Susilo proposed [6] a searchable attribute-based proxy re-encryption system. When compared to existing systems only supporting either searchable attribute-based functionality or attribute-based proxy re-encryption, this new primitive supports both abilities and provides flexible keyword update service. Specifically, the system enables a data owner to efficiently share his data to a specified group of users matching a sharing policy and meanwhile, the data will maintain its searchable property but also the corresponding search keyword(s) can be updated after the data sharing. The server however knows nothing about the keyword(s) and the data. The new mechanism is applicable to many real-world applications, such as electronic health record systems.

F. Constant-size Cipher Text Policy

Zhijie Wang, Dijiang Huang,Yan Zhu, Bing Li, and Chun-Jen Chung proposed a new efficient framework named Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE) [7] with the support of negative attributes and wildcards. It embeds the comparable attribute ranges of all the attributes into the user's key, and incorporates the attribute constraints of all the attributes into one piece of ciphertext during the encryption process to enforce flexible access control policies with various range relationships. Accordingly, CCP-CABE achieves the efficiency because it generates constant-size keys and ciphertext regardless of the number of involved attributes, and it also keeps the computation cost constant on lightweight mobile devices.

G. Attribute-Based Hybrid Encryption

Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in this work [8]. 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. Besides, this scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption.

H. Verifiable Outsourced ABE

In the original outsourced ABE scheme correctness of the cloud server's transformation can not be verified by the user. That is, an end user could be cheated into accepting a wrong or maliciously transformed output. Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma [9] first formalize a security model of ABE with verifiable outsourced decryption by introducing a verification key in the output of the encryption algorithm. Then, they presents an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. This new approach is simple, general and almost optimal. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user's and the cloud server's computation costs except some non-dominant operations (e.g., hash computations), nor expands the ciphertext size except adding a hash value (which is less than 20 byte for 80-bit security level).

I. ID-Based Ring Signature

Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. This paper [10] shows enhancement security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has been compromised.

J. *Multi Authority Attribute Based Encryption*

The extended CP-ABE mechanism with multi-authorities (MA-ABE) is designed [20] for the practical application. In this paper, authors proposed an efficient and secure multi-

https://dx.doi.org/10.22161/ijaers/3.12.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

authority access control scheme transfer the computing to the cloud server. This scheme implements partial decryption operation in cloud server and improves the user's decryption efficiency, which can be applied to the scenario of access to the Internet using mobile devices.

K. *Fully Homomorhphic Encryption*

This paper [21]shows that how to reduce a communication overhead between cloud server and data owner using public key compression technique for fully homomorphic encryption scheme over the integers. Whenever we use the cloud, user expects Data privacy, search accuracy & less communication overhead from the cloud service providers. In order tackle this TRSE (Two Round Searchable Encryption) scheme has been proposed which achieved high data privacy through homomorphic encryption and search accuracy through vector space model. This proposed scheme used Modified FHEI (fully homomorphic encryption over the integers) which generates the public key of large size. This large key is used for encryption of keywords to hide access pattern & search pattern.

III. COMPARISONS BETWEEN EXISTING ALGORITHMS

A. Comparison Of ABE Schemes

Table.1.1 : Comparison Of ABE Schemes

Techniques / Parameter	**ABE**	**KP-ABE**	**CP-ABE**
Fine Grained Access Control	Low	Low, High if there is re-encryption technique	Average Realization of complex Access Control
Efficiency	Average	Average, High for broadcast type system	Average, Not efficient for modern enterprise
Computational Overhead	High	Most of computational overheads	Average computational overheads
Flexibility	Average	Average	Average
Security	Medium	Medium	Average

Table.1.2 : Comparison Of ABE Schemes

Techniques / Parameter	**FH-CP-ABE**	**MA-ABE**
Fine Grained Access Control	Good Access Control	Better Access Control
Efficiency	Flexible	Scalable
Computational Overhead	Some of overhead	Average
Flexibility	Average	Average
Security	Average	Low

B. Drawbacks Of ABE Schemes

i. ABE Drawbacks -
- Data owner needs to use every authorized user's public key to encrypt data.
- Restricted in the real environment.

ii. KP-ABE Drawbacks -
- Encryptor cannot decide who can decrypt the encrypted data.
- it is unsuitable in some application because a data owner need to trust the key issuer.

iii. CP-ABE Drawbacks -
- Not fulfilling the enterprise requirements of access control which require considerable efficiency & flexibility .
- Restriction occurs in terms of specifying policies and managing user attributes.

iv. HABE Drawbacks -
- Practically it is not good for implementation.
- Since all attributes in one conjunctive clause may be administered by the same domain authority also the same attribute may be administered by multiple domain authorities.

v. MA-ABE Drawbacks -
- Required each authority's attribute set be disjoint & that is somewhat complicated.

C. Authentication Techniques with their advantages & disadvantages

Method /Scheme	**Advantages**	**Disadvantages**
Voiceprint biometric authentication	Size of codebook database depends on number of users.	Overhead increase if number of users increase.
A strong user authentication framework for cloud computing	Identity management, Session key management &agreement, Mutual authentication.	Password and smartcard Verification is done by the local system.
Face Recognition System (FRS) on	simple and easy to implement.	Camera always required & some lighting condition also

https://dx.doi.org/10.22161/ijaers/3.12.5 *ISSN: 2349-6495(P) | 2456-1908(O)*

Cloud Computing for User Authentication		required for better result
Consolidated authentication model	Secure & easy to use	Vulnerable in some attacks
Remote authentication on secret splitting	secure from authentication factor attacks.& network attacks	Threat of the template leakage
Authentication in the Clouds: A Framework and its Application to Mobile Users	Authentication is done on the clients‟ behavior hence theft of the device is not a threat.	Best result depends on application.
Single Sign On	Different application can authenticate using one server	Single point of failure
Multidimensional Password Generation	Multiple levels of authentication	Overhead is more in multilevel authentication
Two Factor Authentication	It is robust and efficient against phishing and replay attacks.	Theft of mobile phone leads to breach of security.

IV. PROPOSED WORK

We go for implementation of cloud based system which deals with the key escrow problem in data security & make direct communication happens between the different users using cloud service providers (CSP) & also try to reduce the server side load. Access control is one of the most important security mechanisms in cloud computing. In this propose Attribute-based access control scheme we provides a flexible approach that allows data owners to integrate data access policies within the encrypted data. Also in propose system we will build up the system to deal with the major disadvantages of existing system like key escrow problem in data sharing & performance degradation issue.

V. CONCLUSION

Cloud computing is most preferable trend for user which provides many beneficial services. But somewhere, there is some privacy or protection is required against the data stored or activity done over the cloud. This paper provides a review of different authentication mechanisms for cloud computing in which a number of security features are provided. Also we review the different attribute based access control mechanisms used in existing systems. It consist five different attribute-based encryption schemes such as ABE (Attribute-Based Encryption), KP-ABE (Key-policy attribute-based encryption), CP-ABE (ciphertext-policy attribute-based encryption), HABE (Hierarchical Attribute Based Encryption), MA-ABE (Multi-Authority Attribute Based Encryption). Attribute based policies are associated with data and attributes. These data & attribute are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data else no one can decrypt it. In ABE scheme, there are both the ‘secret key’ and ‘ciphertext’ are associated with a set of attributes. ABE is further modified into different that provides fine grained access control. In ABE scheme, there are both the ‘secret key’ and ‘ciphertext’ are associated with a set of attributes. ABE is further modified into KP-ABE that provides fine grained access control. ABE used in cloud security for the purposes of providing guarantees towards the provenance the sensitive data. These scheme provides more scalable, flexible and fine-grained access control than any other schemes in cloud computing.

REFERENCES

[1] Shulan Wang, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, Weixin Xie ,"Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security, 2016

[2] Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, Weixin Xie ,"An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, 2016

[3] Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu and Jin Li , “Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services” ,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 3, MARCH 2016

[4] Xinfeng Ye, "Privacy Preserving and Delegated Access Control for Cloud Applications", TSINGHUA SCIENCE AND TECHNOLOGY (c) IEEE, ISSN l1007-0214l l04/10l lpp40-54 Volume 21, Number 1, February 2016

[5] SU Mang, LI Fenghua, SHI Guozhen, GENG Kui and XIONG Jinbo ,"A User-Centric Data Secure Creation Scheme in Cloud Computing", Chinese Journal of Electronics Vol.25, No.4, July 2016

[6] Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, 2015

[7] Zhijie Wang, Dijiang Huang,Yan Zhu, Bing Li, and Chun-Jen Chung, "Efficient Attribute-Based Comparable Data Access Control", IEEE Transactions on Computers, 2015

[8] Jie Xu, Qiaoyan Wen, Wenmin Li and Zhengping Jin,"Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS ,2015

[9] Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma ,"Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2015

[10] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu and Jianying Zhou , "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security" ,IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 4, APRIL 2015

[11] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma ,"Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation" , IEEE Transactions on Computers ,2015

[12] Ruei-Hau Hsu & Jemin Lee , "Group Anonymous D2D Communication with End-to-End Security in LTE-A" ,2015 IEEE Conference on Communications and Network Security (CNS)

[13] Guang-liang Guo, Quan Qian*, Rui Zhang ,"Different Implementations of AES Cryptographic Algorithm", 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on Embedded Software and Systems (ICESS)

[14] Shohreh Hosseinzadeh, Sami Hyrynsalmi, Mauro Conti† and Ville Leppanen "Security and Privacy in Cloud Computing via Obfuscation and Diversification: a Survey" ,2015 IEEE 7th International Conference on Cloud Computing Technology and Science

[15] Jindan Zhang, Xu An Wang, Jianfeng Ma "Data Owner Based Attribute Based Encryption", 2015 International Conference on Intelligent Networking and Collaborative Systems

[16] Xiaolong Xu & Qun Tu ,"Data deduplication mechanism for cloud storage systems" ,2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery

[17] HUANG Qinlong, MA Zhaofeng, YANG Yixian, FU Jingyi and NIU Xinxin ,"EABDS: Attribute-Based Secure Data Sharing with Efficient Revocation in Cloud Computing" ,Chinese Journal of Electronics Vol.24, No.4, Oct. 2015

[18] Cheng Hongbing, Rong Chunming, Hwa ng Kai, Wang Weihong, LI Yanyan ,"Secure Big Data Storage and Sharing Scheme for Cloud Tenants" ,SECURITY SCHEMES AND SOLUTIONS China Communications • June 2015

[19] Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing" ,IEEE Transactions on Parallel and Distributed Systems ,2014

[20] Danwei Chen, Liangqing Wan, Chen Wang, Su Pan, Yuting Ji, "A Multi-authority Attribute-based Encryption Scheme with Pre-decryption", 2015 IEEE Seventh International Symposium on Parallel Architectures, Algorithms and Programming

[21] Mr. Sunil A. Kumbhar, Mr. Chetan J. Awati , "Improving Efficiency of TRSE Scheme by Employing Public Key Compression Technique for Fully Homomorhphic Encryption over the Integers", International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 1, January – 2014 ISSN: 2278-0181