MJRET

Open Access

Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

ISSN:2348 - 6953

SURVEY ON ATTRIBUTE-BASED DATA SHARING SCHEME REVISITED IN CLOUD COMPUTING

Mr. Swapnil R. Patil, Prof. N. D. Kale

Computer Engineering Department, PVPIT,

Pune, India

Abstract: *Cloud storage is the best and proficient approach to handle our information remotely. In any case, since information proprietors and clients are more often than not outside the trusted area of cloud specialist co-ops the information security and get to control is the critical component at the season of delicate information put away in the cloud. Additionally, now days there are distinctive systems are accessible for information sharing and saving security of information proprietor and client. Key Escrow is the one of the significant issue now a day. We can't keep full trust over the key power focus since they might be abuse their benefits. This is unsatisfactory for data sharing circumstances. In this paper we concentrated the current procedure for sharing the information from information proprietor to information client. The methodology propose an enhanced two-party key issuing convention that can ensure that neither key power nor cloud specialist co-op can bargain the entire mystery key of a client exclusively. The method also present the idea of quality with weight, being given to upgrade the statement of characteristic, which cannot just extend the expression from paired to discretionary state, additionally help the intricacy of get to approach. In this manner, both capacity cost and encryption many-sided quality for a ciphertext are eased. Attribute based encryption is an open key based encryption that empowers get to control over encoded information utilizing access strategies and credited qualities.*

Keywords*: Data Confidentiality, Key Authority, Access Control policy, Data Sharing, Attribute-based encryption, Removing escrow, weighted attribute, Cloud computing.*

1. INTRODUCTION

In current era there are bunches of quickly developing patterns and cloud registering is one of them. Cloud gives simple, proficient stage to store information, secure information, and get to information at any area with the assistance of web. Additionally it gives client adaptable foundations, storage room and execution. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing [1], [10].

In a CP-ABE, client's mystery key is portrayed by a trait set, and ciphertext is connected with a get to structure. DO is permitted to characterize get to structure over the universe of traits. A client can unscramble a given ciphertext just if his/her trait set matches the get to structure over the ciphertext. Utilizing a CP-ABE framework specifically into a cloud application that may yield some open issues Firstly, all clients' mystery keys should be issued by a completely trusted key power (KA). This brings a security hazard that is known as key escrow issue. By knowing the mystery key of a framework client, the KA can unscramble the entire client's ciphertext, which remains altogether against to the will of the client. The weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but also to simplify access policy. Thus, the storage cost and encryption cost for a ciphertext can be relieved.

Assume there is a formal structure in college, in which instructors are characterized into showing partner, speaker, related teacher and full educator [1]. We circulate the heaviness of the characteristic for every kind of the instructors as 1, 2, 3, and 4. In this way, these qualities can be indicated as "Educator: 1", "Educator: 2", "Instructor: 3" and "Instructor: 4", individually. For this situation, they can be signified by one trait which has quite recently extraordinary weights. Specifically, it can be arbitrary state properties, for example, "Instructor: showing associate, teacher, relate educator, full teacher". We here accept that an get to arrangement is spoken to as: T {("Lecturer" OR "Partner Teacher" OR "Full Professor") AND "Male"}, and the current CP-ABE plans are executed on the type of get to strategy T . On the off chance that our proposed plan is sent, the T can be rearranged as T ′ {"Teacher: 2" AND "Male"}, since the characteristic "Instructor: 2" indicates the base level in the get to approach and incorporates {"Teacher: 2", "Instructor: 3" "Instructor: 4"} as a matter of course. In this manner, the capacity overhead of the comparing ciphertext and the computational cost utilized as a part of encryption can be lessened. These two structures are appeared in Fig. 1. Likewise, our technique can be utilized to express bigger quality space than any time in recent memory under a similar number of qualities. For instance, if both the property space and weighted set incorporate n components, the proposed plan can portray

n2 distinctive potential outcomes. Interestingly, the current CPABE plots just show 2n conceivable outcomes.

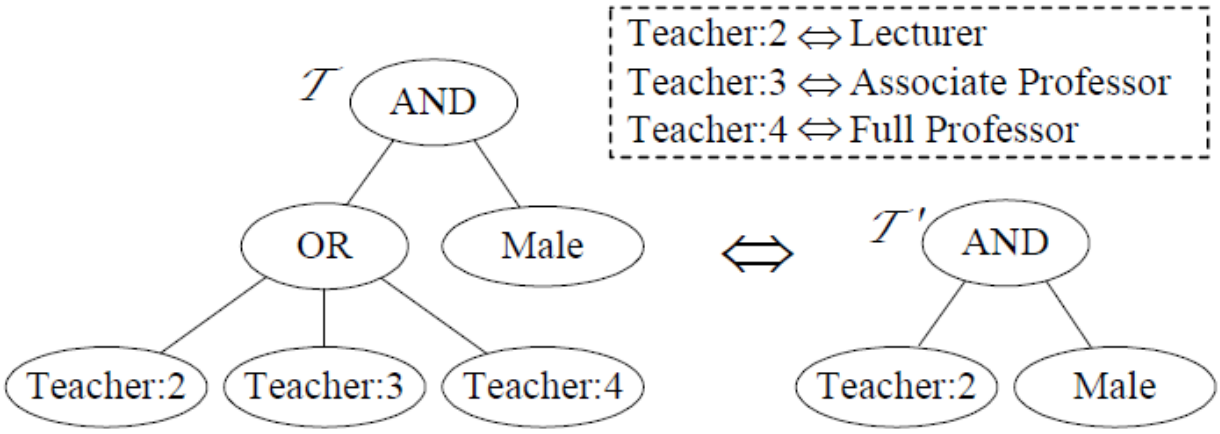

Fig. 1.Two equivalent access structures of a ciphertext. T represents a general access policy in the existing CP-ABE schemes. T ′ denotes an improved access policy in the proposed scheme [1].

2. LITERATURE SURVEY

The literature survey that containing study of differentschemes available in Attribute Based encryption(ABE).Thatare KP-ABE,CP-ABE, Attribute-based Encryption Schemewith Non-Monotonic Access Structures, ABE andMABE.Also include advantage, disadvantage and acomparison table of each scheme based on fine grainedaccesscontrol,efficiency, and computational overhead andcollusion resistant.

Shulan Wang, Kaitai Liang, Joseph K. Liu, JianyongChen,Jianping Yu, WeixinXie [1] revisit attribute-based datasharing scheme in order to solve the key escrow issue but alsoimprove the expressiveness of attribute, so that the resultingscheme is friendlier to cloud computing applications. Theyproposed an improved two-party key issuing protocol that canguarantee that neither key authority nor cloud service providercan 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, whichcan not only extend the expression from binary to arbitrarystate, but also lighten the complexity of access policy.Therefore, both storage cost and encryption complexity for acipher text are relieved.

An efficient file hierarchy attribute-based encryptionscheme (FH-CP-ABE) is proposed by Shulan Wang, JunweiZhou, Joseph K. Liu, Jianping Yu, Jianyong Chen and WeixinXie [2]. The layered access structures are integrated into asingle access structure, and then the hierarchical files areencrypted with the integrated access structure. The cipher textcomponents related to attributes could be shared by the files.Therefore, both cipher text storage and time costs of encryption are saved. Moreover, the proposed scheme is proved

to besecure under the standard assumption. In this study, anefficient encryption scheme based on layered model of theaccess structure is proposed in cloud computing, which isnamed file hierarchy CP-ABE scheme (or FH-CP-ABE, forshort). FH-CP-ABE extends typical CPABE with ahierarchical structure of access policy, so as to achieve simple,flexible and fine-grained access control.

Kaitai Liang and Willy Susilo proposed [3] a searchableattribute-based proxy re-encryption system. When comparedto existing systems only supporting either searchable attributebasedfunctionality or attribute-based proxy re-encryption, thisnew primitive supports both abilities and provides flexiblekeyword update service. Specifically, the system enables adata owner to efficiently share his data to a specified group ofusers matching a sharing policy and meanwhile, the data willmaintain its searchable property but also the correspondingsearch keyword(s) can be updated after the data sharing. Theserver however knows nothing about the keyword(s) and thedata. The new mechanism is applicable to many real-worldapplications, such as electronic health record systems.

Circuit ciphertext-policy attribute-based hybrid encryptionwith verifiable delegation has been considered in this work[4]. In such a system, combined with verifiable computationand encrypt-then-mac mechanism, the data confidentiality, thefine-grained access control and the correctness of thedelegated computing results are well guaranteed at the sametime. Besides, this scheme achieves security against chosenplaintextattacks under the k-multilinear Decisional Diffie-Hellman assumption.

The extended CP-ABE mechanism with multi-authorities(MA-ABE) is designed [5] for the practical application. Inthis paper, authors proposed an efficient and secure multiauthority access control scheme transfer the computing to thecloud server. This scheme implements partial decryptionoperation in cloud server and improves the user's decryptionefficiency, which can be applied to the scenario of access tothe Internet using mobile devices.
An attribute based encryption scheme introduced by Sahaiand Waters in [6] and the goal is to provide security andaccess control shows that how to reduce a communicationoverhead between cloud server and data owner using publickey compression technique for fully homomorphicencryptionscheme over the integers. Whenever we use the cloud, userexpects Data privacy, search accuracy & less communicationoverhead from the cloud service providers. In order tackle thisTRSE (Two Round Searchable Encryption) scheme has beenproposed which achieved high data privacy throughhomomorphic encryption and search accuracy through vectorspace model. The problem with attribute based encryption (ABE) schemeis that data owner needs to use every authorized user's publickey to encrypt

data. The application of this scheme isrestricted in the real environment because it use the access of monotonic attributes to control user's access in the system.

3. CONCLUSION& FUTURE SCOPE

In this paper, we break down various property based encryption plans: ABE, KP-ABE, CP-ABE, ABE with non-monotonic get to structure, HABE and MA-ABE. The fundamental get to policies are KP-ABE and CP-ABE, advance plans are acquired in light of these arrangements. In light of their kind of get to structure the plans are sorted as either monotonic or non-monotonic. CH-ABE an adjustment of Attribute Based Encryption (ABE)for the reasons for giving certifications towards the provenance the delicate information, and in addition towards the namelessness of the information proprietor; Our plan additionally empowers dynamic alteration of get to approaches o underpins proficient on-request client/property denial and break-glass access under crisis situations.

REFERENCES

[1] *Shulan Wang, Kaitai Liang, Joseph K. Liu, JianyongChen, Jianping Yu, WeixinXie ,"Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEETransactions on Information Forensics and Security, 2016.*

[2] *Shulan Wang, Junwei Zhou, Joseph K. Liu, JianpingYu,Jianyong Chen, WeixinXie ,"An Efficient File HierarchyAttribute-Based Encryption Scheme in CloudComputing", IEEE Transactions on Information Forensicsand Security, 2016*

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

[4] *JieXu, Qiaoyan Wen, Wenmin Li and ZhengpingJin,"Circuit Ciphertext-policy Attribute-based HybridEncryption with Verifiable Delegation in CloudComputing", IEEE TRANSACTIONS ON PARALLELAND DISTRIBUTED SYSTEMS ,2015*

[5] *Danwei Chen, Liangqing Wan, Chen Wang, Su Pan,YutingJi, "A Multi-authority Attribute-based EncryptionScheme with Pre-decryption", 2015 IEEE SeventhInternational Symposium on Parallel Architectures,Algorithms and Programming*

[6] *J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attributebased encryption "in Proceedings of IEEE Symposium on Security andPrivacy, pp. 321V334, 2007.*

[7] *V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multiauthorityattribute-based encryption with honest-but-curious centralauthority" International Journal of Computer Mathematics, vol. 89,pp. 3,2012.*

[8] *V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-basedencryption for fine-grained access control of encrypted data," inProceedings of the 13th ACM conference on Computer andcommunications security, pp. 89{98, 2006}*

[9] *Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryptionscheme for secure data sharing in a cloud environment," InformationSciences .In Press, 2012.*

[10] *M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. "Secureattribute-based systems". In Proceedings of the 13th ACM conference onComputer and communications security, pages 99{112. ACM Press NewYork, NY, USA, 2006*