IPHV8I2033X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

A SEMI-ANONYMOUS DECENTRALIZED DATA PRIVILEGE CONTROL SCHEME IN CLOUD COMPUTING

[#1]**Dr. K.RAMESHWARAIAH,** *HOD,*
[#2]**N. RAJENDER,** *Assistant Professor,*
[#3]**MUDDAM SRIDHAR REDDY**, *M.Tech Student,*
Department of CSE,
NALLA NARASIMHA REDDY GROUP OF INSTITUTIONS , RANGA REDDY, TELANGANA, INDIA.

Abstract:- Cloud computing is a computing concepts, which enables when required and low maintenance usage of resources, but the data is shares to some cloud servers and various privacy related concerns emerge from it. Various schemes like based on the attribute-based encryption have been developed to secure the cloud storage. Most work looking at the data privacy and the access control, while less attention is given to the privilege control and the privacy. Attribute-based Encryption (ABE) is a cryptographic conducting tool to guarantee data owner's direct control over their data in public cloud storage. ABE is an encryption method used by the user to store the data in the cloud. ABE is a public-key based one to many encryption methodologies which allows users to encrypt and decrypt data based on user attributes. In this paper we studied various schemes of ABE like KP-ABE, CP-ABE, Anony Control and Anony Control-F, also we analyzed how data access privilege and data sharing can be controlled by using various schemes of ABE. We present the Anonymity Control-F, which prevents the identity and achieve the anonymity. Our security analysis shows that both Anonymity Control and Anonymity Control-F are secure under the Diffie–Hellman assumption and our performance evaluation exhibits the feasibility of our schemes.

Keywords: Cloud Computing, Attribute-based Encryption, public keys, private keys, cipher text.

I.INTRODUTION

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a cloud. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently [9].Cloud computing provides a scalable, location-independent and high performance solution by delegating computation tasks and storage into the resource-rich clouds. This overcomes the resource limitation of users with respect to data storage, data sharing and computation various techniques have been proposed to protect the data contents privacy via access control Identity-based encryption (IBE) [4,7.12,14,15], Fuzzy Identity-Based Encryption Key-Policy Attribute-Based Encryption (KP-ABE) [5,6,10], Ciphertext-Policy AttributeBased Encryption (CP-ABE) [3,8,11.13] and AnonyControl and AnonyControl-F [1] to allow cloud servers to control user's access privileges without knowing their identity information. In the KP-ABE [5], a cipher text is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user's identity (e.g. IIT AND (Ph.D OR Master)). A user can decrypt the cipher text if and only if the access tree in his private key is satisfied by the attributes in the cipher text. However, the encryption policy is described in the keys, so the encrypter does not have entire control over the encryption policy [10]. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation.

On the other hand, those problems and overhead are all solved in the CP-ABE [3]. In the CP-ABE, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the cipher text if and only if his attributes in the private key satisfy the access tree specified in the cipher text. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots [11]. Unlike the data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. But it seems natural that users are willing to keep their identities secret while they still get their private keys. Therefore AnonyControl and AnonyControl-F [1] to allow cloud

servers to control users' access privileges without knowing their identity information. The schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The schemes are tolerant against authority compromise, and compromising of up to (N − 2) authorities does not bring the whole system down.

II. RELATED WORK

The concept of ABE for Fine Grained Access Control of Encrypted Data in 2006. He introduces the new cryptosystem for fine grained sharing of encrypted data that is called Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. Secret-sharing schemes (SSS) are used to divide a secret among a number of parties. Matthew Pirretti and Brent Waters introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. A performance analysis of ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Through this, demonstrates that the attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. Decryption decrypts a ciphertext encrypted by the Encryption. This process begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the ciphertext in order to obtain the AES and HMAC key. John Bethencourt, AmitSahai, Brent Waters introduces Ciphertext-Policy Attribute-Based Encryption in 2008. They employ a trusted server to store the data and mediate access control. In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In addition, they provide an implementation of the system and give performance measurements. The primary challenge in this line of work is to find new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010. It illustrates the basic principles on which architecture for combining access control and cryptography can be built. Then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. It also described an approach for policy evolution that takes into account the main features of the scenario and is able to guarantee in most cases confidentiality of the information in the presence of significant policy updates, clearly identifying the exposure to collusion when this risk may arise. Other issues to be investigated include the integration with the Web paradigm, and the efficient execution of queries. Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Bjorn Tackmann, Daniele Venturi introduced Anonymity-preserving PublicKey Encryption: A Constructive Approach where publickey cryptosystems with enhanced security properties have been proposed. it investigate constructions as well as limitations for preserving receiver anonymity when using public-key encryption (PKE). They use the constructive cryptography approach by Maurer and Renner and interpret cryptographic schemes as constructions of a certain ideal resource (e.g. a confidential anonymous channel) from given real resources (e.g. a broadcast channel) and defined appropriate anonymous communication resources and show that a very natural resource can be constructed by using a PKE scheme which fulfills three properties that appear in cryptographic Literature. Results do not only support the trust in existing schemes and constructions; they also show that the simpler and more efficient weakly robust schemes can be used safely. Junbeom Hur, Dong Kun Noh introduces the concept of Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions. The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups. The other extra function is the ReEncrypt(CT;G) which is a reencryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it. R.Ranjith and D.Kayathri Devidescribes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication in 2013. It is implemented with secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination.

IPHV8I2033X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches. Mr. ParjanyaC.A and Mr. Prasanna Kumar describe the concept of Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in March 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.

III. PROBLEM FORMULATION

A. Framework Model: In our framework, figure 1 there are five sorts of elements: N Attribute Powers (signified as A), central authority, Cloud Server, Data Owners and Data Consumers. A client can be a Data Owner and a Data Customer all the while. Attribute authority and central authority are accepted to have intense calculation capacities, what's more, they are regulated by government workplaces in light of the fact that a few traits incompletely contain clients' by and by identifiable data. The entire attribute set is partitioned into N disjoint sets and controlled by every attribute authority, along these lines every attribute authority knows about just piece of information. Central authority is the trusted party where data owner and data consumer are communicated to attribute authority through central authority. A Data Owner is the substance who wishes to outsource encoded information record to the Cloud Servers. The Cloud Server, why should expected have sufficient capacity limit, does only store them. Recently joined Data Consumers ask for private keys from all of the Attribute authority , and they don't know which Attribute are controlled by which Attribute authority. At the point when the Data Consumers demand their private keys from the Attribute authority, Attribute authority together make relating private key and send it to them. All Data Consumers can download any of the scrambled information documents, however just those whose private keys fulfil the privilege tree Tp can execute the operation connected with benefit p. The server is designated to execute an operation p if and just if the client's accreditations are checked through the privilege tree Tp.

IV. PROPOSED METHOD: ACHIEVING FULL ANONYMITY

It is assumed that semi-honest authorities in AnonyControl and they will not conspire with each other. This is a essential supposition in AnonyControl because each authority is in control of a subset of the whole attributes set, and for the attributes that it is in charge of, it knows the exact information of the key requester.

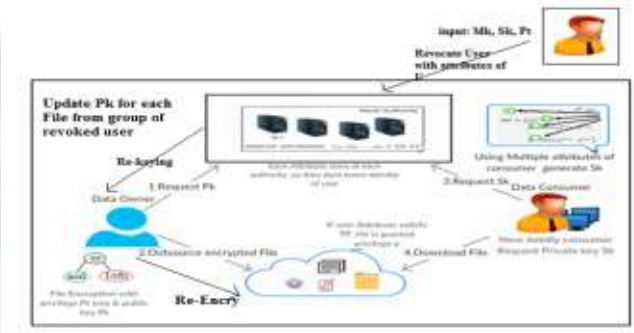

Fig. Proposed Architecture

If the information from all authorities is collected totally, the complete attribute set of the key requester is recovered and thus his identity is disclosed to the authorities. In this sense, AnonyControl is semi anonymous since partial identity information. (represented as some attributes) is released to each authority, but we can achieve a full-anonymity and also permit the collusion of the authorities.[12] The key point of the identity information leakage we had in earlier system as well as every present attribute based encryption systems is that key generator (or attribute authorities in our system) issues attribute key based on the[13] stated attribute, and the generator has to know the user's attribute to do so. We need to host a new technique to let key generators issue the correct attribute key without knowing what attributes the users have. A naive solution is to give all the attribute keys of all the attributes to the key requester and let him pick whatsoever he wants. By this procedure, the key generator does not know which attribute keys the key requester chosen, but we have to completely trust the key requester that he will not pick any attribute key not allowed to him. [14].

V. PERFORMANCE EVALUATION

It is presented here regarding the performance evaluation based on the assessment about executing prototype system of AnonyControl-F. This is the first implementation of a multi-authority attribute based encryption system. This prototype system offers five command line tools.[12]

(i) anonycontrol-setup: Jointly generates a public key and N master keys.

(ii) anonycontrol-keygen: Generates a part of private key for the attribute set it is responsible for.

(iii) anonycontrol-enc: Encrypts a file under r privilege trees.

(iv) anonycontrol-dec: Decrypts a file if possible.
(v) anonycontrol-rec: Decrypts a file and re-encrypts it under different privilege trees.[17]

This toolkit is based on the CP-ABE toolkit [4] which is available online and the whole system is implemented on a Linux system with Intel i7 2nd Gen @ 2.7GHz and 2GB RAM. It is furthermore employed three similar works under the same condition for the comparison purpose. Particularly, it is set only one privilege for the file access, and measured the time to create one privilege tree and calculate its verification parameter. In general, the computation overhead of is much higher than others because their system involves many more exponentiations and bilinear mappings due to the accountability [15],[18]. The encryption/decryption under different file sizes did not show big differences when file sizes are large (≥20MB), because the run times are dominated by the symmetric encryption (AES-256). Finally, only run times are plotted because the privilege creation is the Unique process in the system.

VI.CONCLUSION

In Cloud computing system for multiple authorities, our proposed schemes achieve not only fine-grained privilege control and identity privacy but also user revocation using attribute revocation schemeover AnonyControl-F scheme which is can tolerate up to N − 2 authority compromise. Future scope of our scheme is to reduce communication overhead in this user revocation over AnonyControl-F system. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that Anony- Control both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer.

REFERENCES

[1] Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption 190 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015 .
[2] A Privilege Based Attribute Encryption System For Secure and Reliable Data Sharing. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 5, May 2014
[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertextpolicy attribute based encryption,” in Proc. IEEE SP, May 2007, pp. 321–334.
[4] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
[5] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th
[7] Identity-Based Encryption with Outsourced Revocation in Cloud Computing IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 2, FEBRUARY 2015
[8] Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption Jinguang Han, Member, IEEE, Willy Susilo, Senior Member, IEEE, Yi Mu, Senior Member, IEEE,
[9] Jianying Zhou, and Man Ho Allen Au, Member, IEEE K. Yang, X. Jia, K. Ren, and B. Zhang, “DAC-MACS: Effective data access control for multi-authority cloud storage systems,” in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.
[10] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS’10), 2010, pp. 261–270.
[11] J. Bethencourt, A. Sahai, and B. Waters. CiphertextPolicy Attribute-Based Encryption. In Proc. of SP’07, Washington, DC, USA, 2007.
[12] D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” CRYPTO ’01: Proc. Advances in Cryptology, J. Kilian, ed., pp. 213-229, Aug. 2001.
[13] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policy attribute based encryption,” in ICALP’08. Springer, 2008, pp. 579–591.
[14] Y. Dodis, N. Fazio, A. Lysyanskaya, and D.F. Yao. IDBased Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption. In ACM conference on Computer and Communications Security (ACM CCS), pages 354, 363, 2004.
[15] M. K. F. Dan Boneh: \Identity-based encryption from the weil pairing", In: Proceedings of The 21st Annual International Cryptology Conference on Advances in Cryptology CRYPTO'01, Santa Barbara, California, USA, Springer LNCS, Vol.2139, pp. 213-229 (2001).
[16] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.
[17] S. Müller, S. Katzenbeisser, and C. Eckert, “On multi-authority ciphertext-policy attribute-based encryption,” Bull.

Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009. [13] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attributebased encryption with accountability," in Proc. 6th ASIACCS, 2011, pp. 386–390.

[18] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," J. Comput. Inf. Syst., vol. 9, no. 7, pp. 2793–2800, 2013.

[19] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public-Key Cryptography. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[20] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.