International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Attribute-Based Encryption for Control Access Privileges for Cloud Data with Anonymity

[1]Ch. Naresh,[2]T.Neetha

[1]M.Tech Student, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, Hyderabad, T.S, India.

[2]Associate Professor, Dept of CSE, Brilliant grammar school educational institutions group of institutions integrated campus, Hyderabad, T.S, 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. In this paper, we present a privilege control scheme Anonymity Control to address and the user identity privacy in existing access control. Anonymity Control decentralizes the central authority to limit the identity leakage and thus achieves partial anonymity. It also generates the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a proper manner. 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, Anonycontrol, Access control, Privilege control, Semi anonymity, fully anonymity.

INTRODUCTION:

CLOUD Computing set up pervasive, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be immediately provision and released with essential efforts for management or service provider interaction. Its main objective is to deliver quick, secure, convenient data storage and net computing service, with all computing resources envision as services and delivered over the Internet. A number of computing concepts and technologies are

combined in Cloud Computing to satisfy the computing needs of users, it provides common business applications online through web browsers, while their data and software's are stored on the servers. This is an approach that is used to maximize the scope or step up capabilities robustly without investing in new infrastructure, sustenance new personnel or licensing new software. It provides tremendous storage for data and rapid computing to customers over the internet. Data security is one of the aspects of the cloud which prohibit users from using cloud services. There is fear between the data owner's especially in large organizations that their data possibly misuse by the cloud provider without their knowledge. Data security of the user's can bce ensured by using the concept of virtual private networks, firewalls, and by enforcing other security policies within its own circumferences. Security is consequently an extensive element in any cloud computing environment, because it is crucial to assure that only authorized access is sanctioned and protected behaviour Is accepted. Any kind of security and privacy contravention is critical and can produce crucial results. As soon as the strict regulations and policies are taken against privacy in cloud, more and more personnel will feel save to adopt cloud computing. A client may be individual or a big organization but all are having same concern i.e. data security, so data security is dire consequence. Data security at different levels is the vital matter of this technology; it can be categorized into two categories: Security at External level and Security at Internal Level. Security at External level states that data is unsecure opposed to third party, cloud service provider or network intruder. Security at Internal level states that data is unsecure opposed To authorized users or employee of an organization.

RELATED WORKS:

There are numerous work carried in the field of data protection at cloud. Many models, schemes and techniques are proposed for data security. M. Sugumaran et al illustrates a couple of techniques that resolves the security of the data and proposes architecture to safeguard the data in cloud. In proposed architecture the encrypted data is stored in cloud using cryptography technique i.e. located on block cipher. Cindhamani.J et al proposed an enhanced frame work for data security in cloud which follows the security polices such as integrity, confidentiality and availability. Parameters they used are 128 bit encryption, RSA algorithm and Trusted Party Auditor (TPA). Before storing the data into the cloud, the data owner assigns the privileges

that who will access the data. After assigning the privileges they encrypt the data and stores into the cloud. Dharmendra proposed the unified data encryption architecture which ensures the data security and privacy with reasonable performance overhead of computing system. It is based on multilevel identity encryption approach with two level/factor identity verification process. Dr. L. Arockiam et al achieves the data confidentiality in cloud storage with two different techniques i.e. encryption and obfuscation. Encryption encrypts the alpha-numeric and alpha data while obfuscation encrypts the numeric data. Both are done on user side. First, the user has to encrypt the data using any technique then he stores the data into cloud storage. Taeho Jung et al use two schemes to control the data privacy and the identity privacy. One is the AnonyControl scheme i.e. semianonymous privilege control scheme which not only addresses the data privacy but also the user identity privacy in extant access control schemes. It decentralizes the central authority to restraint the identity leakage and thus achieves semianonymity. Another is the AnonyControl-F scheme that controls the identity leakage and achieves the full anonymity. Eman M.Mohamed et al Exhibits the data security model that is based on the analysis of cloud architecture and implemented software to intensify endeavor in data security model for cloud computing. Hu Shuijing described the enormous essentials in cloud computing, such as security key technology, regulation and standard etc and discussed manner in which they are addressed. In this Proposed model data is protected against all threats i.e. internal and external, thread during, transits as well as when data at rest.

PROPOSED SYSTEM:

Propose anonymity Control to allow cloud servers to control users' access privileges without knowing their identity information. 1. The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in anonymity Control and no information is disclosed in anonymity Control-F. 2. The proposed schemes are tolerant against authority compromise, and compromising of up to (N −2) authorities does not bring the whole system down. 3. Provided detailed analysis on security and performance to show feasibility of the scheme anonymity Control and anonymity Control-F. 4. First implement the real toolkit of a multi-authority based encryption scheme anonymity Control and anonymity Control-F. In this setting, each authority knows only a part of any user's attributes, which are not

enough to figure out the user's identity. However, the scheme proposed by Chase considered the basic threshold-based KP-ABE, which lacks generality in the encryption policy expression. Many attribute based encryption schemes having multiple authorities have been proposed afterwards, but they either also employ a threshold-based ABE or have a semi-honest central authority, or cannot tolerate arbitrarily many users' collusion attack.

CONCLUSIONS:

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fullyanonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. 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. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes who support efficient user revocation is one of our future works.

REFERENCES:

[1] a. Shamir, "identity-based cryptosystems and signature schemes," In advances in cryptology. Berlin, germany: springer-verlag, 1985, Pp. 47–53.

[2] a. Sahai and b. Waters, "fuzzy identity-based encryption," in advances In cryptology. Berlin, germany: springer-verlag, 2005, pp. 457–473.

[3] v. Goyal, o. Pandey, a. Sahai, and b. Waters, "attribute-based encryption For fine-grained access control of encrypted data," in proc. 13th Ccs, 2006, pp. 89–98.

[4] j. Bethencourt, a. Sahai, and b. Waters, "ciphertext-policy attribute based

Encryption," in proc. Ieee sp, may 2007, pp. 321–334.

[5] m. Chase, "multi-authority attribute based encryption," in theory of Cryptography. Berlin, germany: springer-verlag, 2007, pp. 515–534.

[6] m. Chase and s. S. M. Chow, "improving privacy and security in Multiauthority attribute-based encryption," in proc. 16th ccs, 2009, Pp. 121–130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Bozovi˘c,´ D. Socek, R. Steinwandt, and V. I. Villanyi,´ "Multi-authority attribute-based encryption with honest-butcurious central authority," IJCM, vol. 89, no. 3, pp. 268– 283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R.-W. Phan, "Low com-plexity multi-authority attribute based encryption scheme for mobile cloud computing," in SOSE. IEEE, 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "Dac-macs: Effective data access control for multi-authority cloud storage systems," in INFOCOM. IEEE, 2013, pp. 2895–2903.

[11] a. Lewko and b. Waters, "decentralizing attribute-based encryption," In advances in cryptology. Berlin, germany: springer-verlag, 2011, Pp. 568–588.

[12] s. Müller, s. Katzenbeisser, and c. Eckert, "on multi-authority Ciphertextpolicy 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 attribute-based encryption with accountability," In proc. 6th asiaccs, 2011, pp. 386–390.

[14] 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.

[15] s. Hohenberger and b. Waters, "attribute-based encryption with Fast decryption," in public-key cryptography. Berlin, germany: Springer-verlag, 2013, pp. 162–179.

[16] 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.