International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-147 PAGE NO: 879-885

Cipher text policy Using attribute based encryption Data Storage in Cloud

V.PRATHIBHA [1]& Ms.M.Sharmila Devi[2]

1M-Tech,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

2Asst.Professor,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

Abstract-Cloud computing is a revolutionist computing paradigm, which enables flexible, on-demand, and low-cost utilization of computing imaginations, but the information is outsourced to some cloud hosts, and sundry secrecy concerns emerge from it. Sundry schemes predicated on the attribute-predicated encryption have been proposed to secure the cloud storage. However, most work fixates on the information contents secrecy and the access control, while less care is paid to the privilege control and the individuality secrecy. In this paper, we present a semi incognito privilege control scheme AnonyControl to address not only the information secrecy, but additionally the utilizer individuality secrecy in subsisting access control schemes. AnonyControl decentralizes the central ascendancy to inhibit the individuality leakage and thus achieves semi anonymity. Besides, it additionally generalizes the file access control to the privilege control, by which privileges of all operations on the cloud information can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which plenarily averts the individuality leakage and achieve the full anonymity. Our protection analysis shows that both AnonyControl and AnonyControl-F are secured under the decisional bilinear Diffie–Hellman posit, and our functioning evaluation exhibits the feasibility of our schemes

Keywords: Ciphertext–policy; attribute based encryption, Anony Scheme.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-147 PAGE NO: 879-885

1. 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

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-147 PAGE NO: 879-885

2. RELATED WORK

Existing system

We present a semi anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes.Besides the fact that we can express arbitrarily general encryption policy, our system also tolerates the compromise attack towards attributes authorities, which is not covered in many existing works.

We extend existing schemes by generalizing the access tree to a privilege tree.We extend existing schemes by generalizing the access tree to a privilege tree.The key point of the identity information leakage we had in our previous scheme as well as every existing attribute based encryption schemes is that key generator issues attribute key based on the reported attribute, and the generator has to know the user's attribute to do so.

Proposed system

Sundry schemes predicated on the attribute-predicated encryption have been proposed to secure the cloud storage. Sundry techniques have been proposed to forfend the information contents secrecy via access control. We propose AnonyControl and Anony Control- to sanction cloud hosts to control users' access privileges without kenning their individuality information. They will follow our proposed protocol in general, but endeavor to ascertain as much information as possible individually. The proposed schemes are able to bulwark user's secrecy against each single ascendancy. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. We firstly implement the authentic toolkit of a multiauthority predicated encryption scheme AnonyControl and AnonyControl-F.

3. IMPLEMENTATION

Attribute Authorities:

They are postulated to have puissant calculation facilities on some properties partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each ascendancy, consequently each ascendancy is cognizant of only part of properties.

Information Owner:

A Information Owner is the entity who wishes to outsource encrypted information file to the Cloud Hosts.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-147 PAGE NO: 879-885

Cloud Server:

The Cloud Server, who is surmised to have adequate storage capacity, does nothing but store them.

Information Consumers:

All Information Consumers are able to download any of the encrypted information files, but only those whose private keys slake the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp.

Incipiently joined Information Consumers request private keys from all of the ascendant entities, and they do not ken which properties are controlled by which ascendant entities. When the Information Consumers request their private keys from the ascendant entities, ascendant entities jointly engender corresponding private key and send it to them.

CP-ABE Algorithm:

In the CP-ABE, cipher texts are engendered with an access structure, which designates the encryption policy, and private keys are engendered according to users' properties. A utilizer can decrypt the cipher text if and only if his properties in the private key gratify the access tree designated in the cipher text. By doing soothe encrypted holds the ultimate ascendancy about the encryption policy. Withal, the already issued private keys will never be modified unless the whole system reboots.

Privilege Trees Tp:

A information file has several operations executable on itself, and each of them is sanctioned only to sanction users with different caliber of qualifications. For example, {Read_mine, Read_all, Efface, Modify, Engender} is privileges set of students' grades. Then, reading Alice's gradesis sanctioned to her and her edifiers, but all other privileges should be sanctioned only to the edifiers, so we require to grant the "Read mine" to Alice and all other to the edifiers. Every operation is associated with one privilege p, which is described by a privilege tree Tp. If a user's properties gratify Tp, he is granted the privilege p. By doing so, we not only control the file access but additionally control other executable operations, which makes the file controlling fine-grained and thus opportune for cloud storage accommodation.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-147 PAGE NO: 879-885

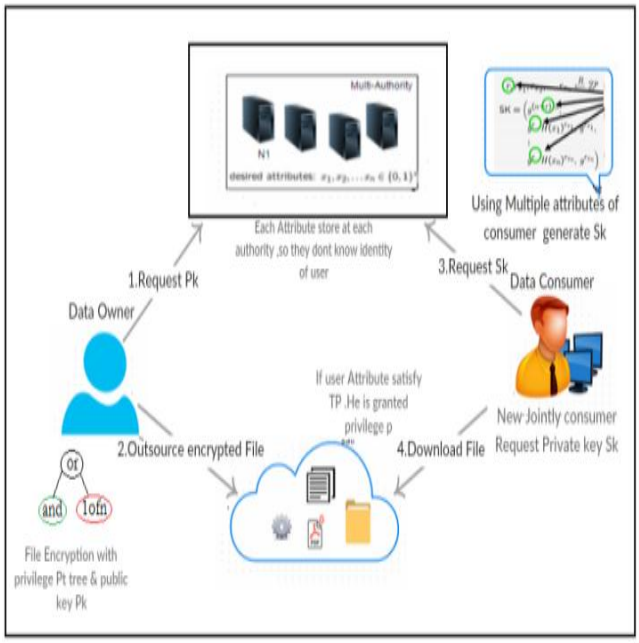

Fig:-1 Proposed System Architecture Model.

4. EXPERIMENTAL RESULTS

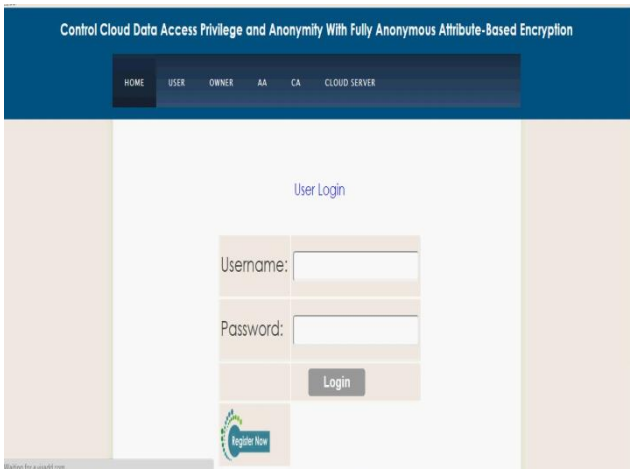

Fig:-2 User authentication and authorization

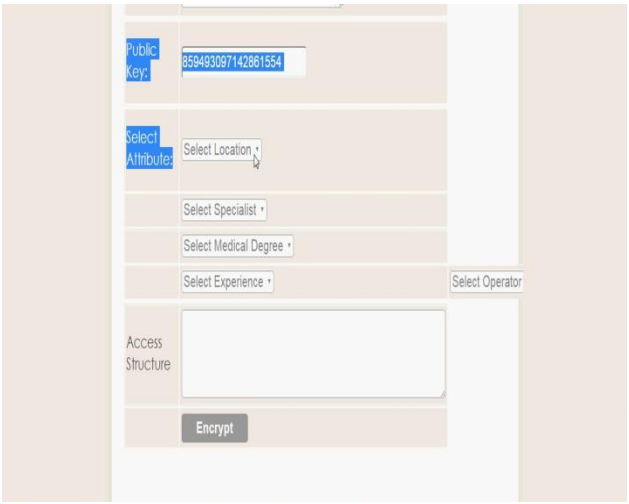

Fig:-3 Cipher text–policy attribute based encryption

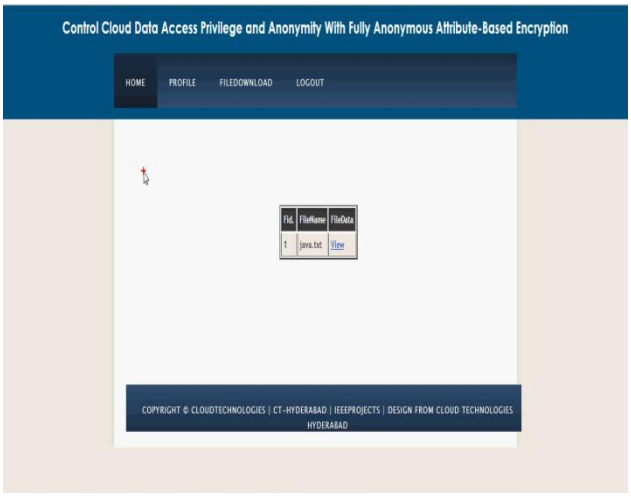

Fig:-4 File Data

5. CONCULSION

This paper proposes a semi-in nominate attribute-predicated privilege control scheme AnonyControl and a planarity-incognito attribute-predicated

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-147 PAGE NO: 879-885

privilege control scheme AnonyControl-F to address the utilizer secrecy quandary in a cloud storage server. Utilizing multiple ascendant entities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but withal individuality anonymity while leading privilege control predicated on users' individuality information. More importantly, our system can abide up to N − 2 ascendancy compromise, which is highly preferable especially in Internet-predicated cloud computing environment. We additionally leaded detailed protection and functioning analysis which shows that AnonyControl both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the protection of the AnonyControl and thus is equipollent 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 utilizer revocation mechanism on top of our incognito ABE. Fortifying utilizer revocation is a paramount issue in the authentic application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with subsisting ABE schemes that support efficient utilizer revocation is one of our future works.

6. 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 attributebased 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 multi-authority 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," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Božovi´ c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 7, 2016. ISSN: 2348-6600
Reference ID: IJCS-147 PAGE NO: 879-885

with honest-but-curious central authority," Int. J. Comput.Math., vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE, Mar. 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 Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.http://www.sourcefordgde.com