ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Securing Data and Revocation of Users in Cloud Computing

Shiva Kumar Dasanthu[1], Dammavalam Srinivasa Rao[2]

M Tech, Dept. of I.T., CNIS, VNR VJIET, Bachupally, Hyderabad, Telangana, India

Associate Professor, Dept. of I.T., VNR VJIET, Bachupally, Hyderabad, Telangana, India

ABSTRACT: Cloud computing, a technology that helps in storing, manipulating and configuring data and applications over the internet. It eliminates the physical infrastructure of resources, which makes it a popular. Sundry schemes predicated on the attribute-predicated encryption have been suggested for providing security in cloud storage systems. 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 adscititiously 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 supplementally establishes the file access control with the privilege control. There the privileges of all operations on the cloud information. This can be managed in a fragile manner. Finally, we introduce the AnonyControl-F, which plenarily averts the individuality leakage and achieve the full anonymity. Our aegis 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. We have also implemented revocation of users which plays a vital role in cloud computing organisations.

KEYWORDS: Cipher text–policy, attribute based encryption, Anony Scheme, Privilege Tree, Key Exchange.

I. INTRODUCTION

CLOUD Computing[1] sets up widespread, appropriate, network access that is in high demand to a shared pool of configurable computing resources such as storage devices, servers, networks devices, applications and so on that can be immediately provision and relinquished with essential efforts for management or accommodation provider interaction. Its main objective is to distribute expeditious, secure, convenient data storage and net computing accommodation, with all computing resources envision as accommodations and distributed over the Internet. A number of computing concepts and technologies are cumulated in Cloud Computing to gratify the computing desiderata of users, it provides mundane business applications online through web browsers, while their data and software's are stored on the servers. This is an approach that is utilized to increase the scope or increase or to step up capabilities strongly without investing in incipient infrastructure, sustenance incipient personnel or licensing incipient software. It provides a very high storage space for data and a high speed of computing to customers such as users and organizations over the cyber world. [1]

Data security is one of the aspects of the cloud which preclude users from utilizing cloud accommodations. There is fear between the data owner's especially in immensely colossal organizations. They will have a Fear that their data gets possibly misusedand manipulated by the cloud service provider without their erudition or knowledge. User can get secured by employing Firewalls, Virtual Private Networks (VPN), Anti-viruses and ensuring security measures with policies within its Boundaries. Security is very crucial in any environment especially in cloud computing which organization confidentiality depends on. The access to the resources is provided by using login identification credentials and password which authorized users can have access to it. Privacy contravention and security of any kind is crucial with appropriate results. Due to this many rigorous regulations and policies are added so that users feel preserved in adapting to cloud. Data Security plays a vital role in cloud computing, it may be to a user or client or a huge organization. Data security at different calibres is the crucial point in this technology. It can be categorized into two categories:

- External level Security
- Internal Level Security

DOI: 10.15680/IJIRCCE.2016. 0409151

Security at External level states that data is unsecured that is opposed to third party, cloud accommodation provider or any one such as network intruder. Internal level security states that data is unsecured that is opposed to sanctioned users or employee of an organization.[2]

Revocation is a mechanism of restricting the users from accessing organisations information by removing them from access. Once an employee or a user leaves an organisation his login credentials should be erased so that he no longer can access organisations resources. This feature is provided by revocation. [3]

II. RELATED WORK

Subsisting System:

In this, we are addressing the user identity privacy by taking the user attributes and semi Anony control scheme. Besides the fact that we can express arbitrarily general encryption policy, our system additionally abides the compromise attack towards attributes ascendant entities, which is not covered in many subsisting works. We extend the subsisting schemes by establishing the access tree to a privilege tree. The main point of the leakage in identity information we had in our anterior scheme as well as every subsisting attribute predicated encryption schemes is that key engenderer issues attribute key predicated on the reported attribute, and the engenderer has to ken the user's attribute to do so.

Proposed system:

Sundry schemes predicated on the attribute-predicated encryption are given for providing security to the systems of cloud storage. Sundry techniques[6] have been proposed to for fend the information contents secrecy via access control. We propose Anony Control 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 endeavour 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 Anony Control and no information is disclosed in AnonyControl-F. We firstly implement the authentic toolkit of a multiauthority predicated encryption scheme AnonyControl and AnonyControl-F.

III. IMPLEMENTATION

The implementation of the project deals with following entities given is as follows:

Attribute Ascendant entities: They are postulated to have puissant calculation facilities on some properties contain fractional user's information which can be personally identifiable. N disjoint sets are designed from the existing entire attribute set and controlled by each ascendancy, consequently each ascendancy is cognizant of only part of properties.

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

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 related with prerogative p. The server is authorized 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. The whole system should reboot to modify the private keys once generated in the initial phase of key generation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Privilege Trees: An 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 grades is 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. One privilege p is concerned with each and every operation. This is explained by a privilege tree Tp. If a user's properties gratify Tp, he is allowed to access the privilege p. hence by proceeding with the above operations we are controlling the file access in addition to controlling other executable operations. This makes the file controlling fine-grained and thus opportune for cloud storage accommodation.

The proposed architecture of the current work is as follows:

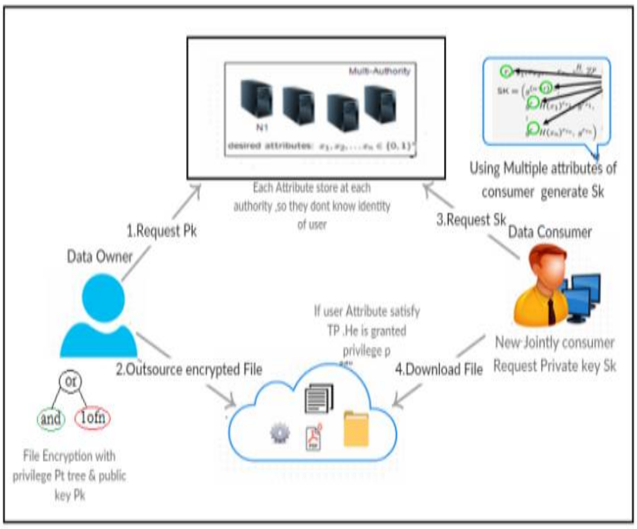

Multi-Authority
N1
desired attributes: $x_1, x_2, \ldots, x_n \in \{0,1\}^*$
Each Attribute store at each authority ,so they dont know identity of user
Using Multiple attributes of consumer generate Sk
1.Request Pk
3.Request Sk
Data Owner
Data Consumer
If user Attribute satisfy TP .He is granted privilege p
2.Outsource encrypted File
4.Download File
New Jointly consumer Request Private key Sk
or
and
1ofn
File Encryption with privilege Pt tree & public key Pk

Fig.3.1 Architecture of Proposed System

The architectural flow of the process starts from setup, encryption, decryption, re-encryption, revocation

IV. SIMULATION RESULTS

The user authentication screen shot is as shown in the below figure:

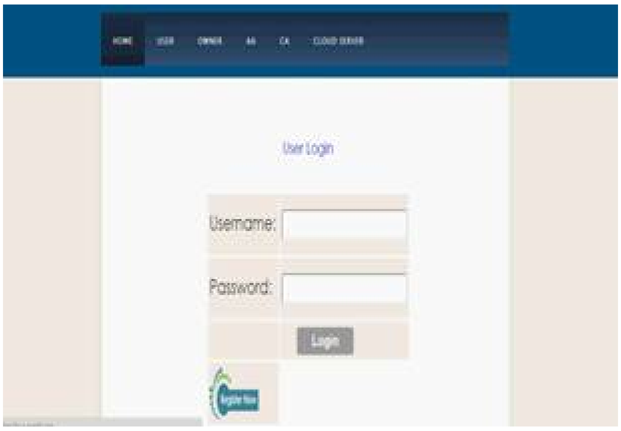
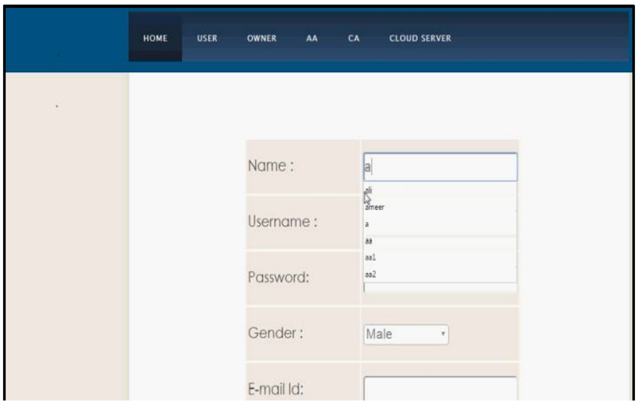


Fig.4.1 Authentication Screen shot

DOI: 10.15680/IJIRCCE.2016. 0409151

The following is the Registration Screen shot:



Name : a

ali
ameer
a
aa
aa1
aa2

Username :

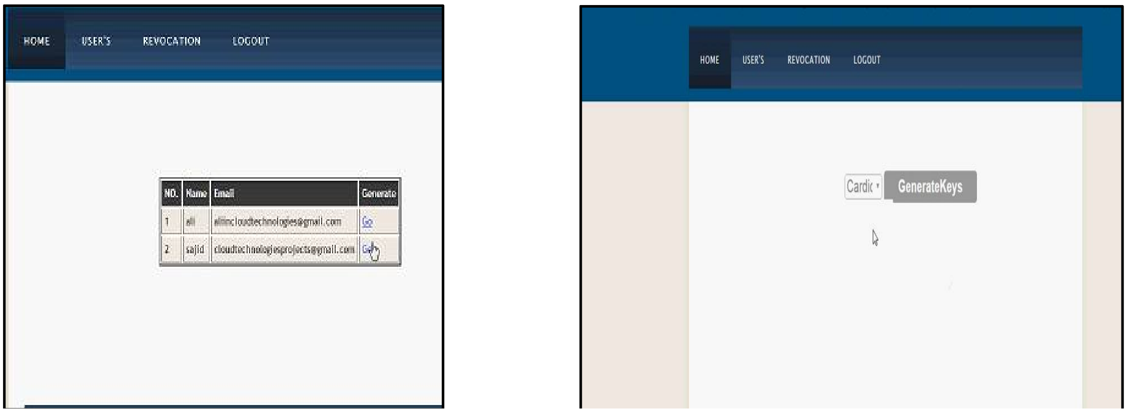
Password:

Gender : Male

E-mail Id:

Fig.4.2 Registration Screen Shot

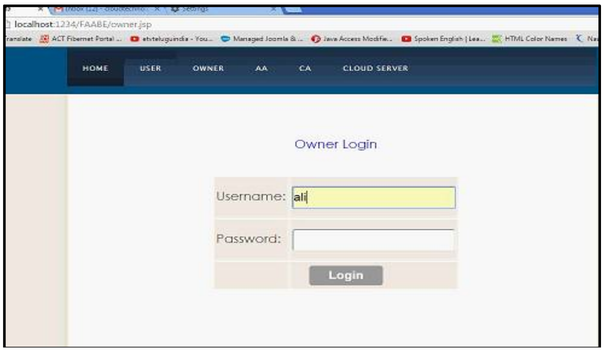
The generation of keys for users is given in below screen shot:



NO.	Name	Email	Generate
1	ali	aliincloudtechnologies@gmail.com	Go
2	sajid	cloudtechnologiesprojects@gmail.com	Go

Fig.4.2 Key Generation Screen shots

The Owner logins with his credentials which is shown by the figure below:



localhost:1234/FAABE/owner.jsp

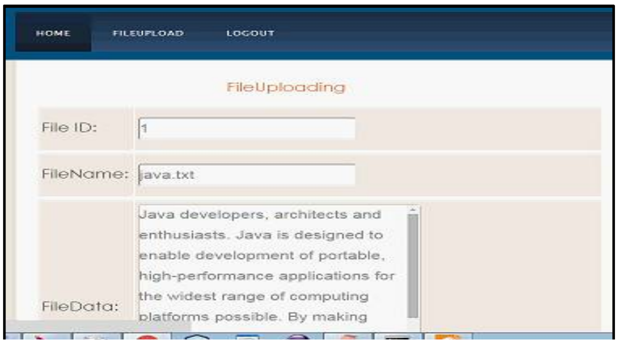
Owner Login

Username: ali

Password:

Fig. 4.4 Owner Login

The file uploading in a cloud server Screen shot is shown in figure below:



FileUploading

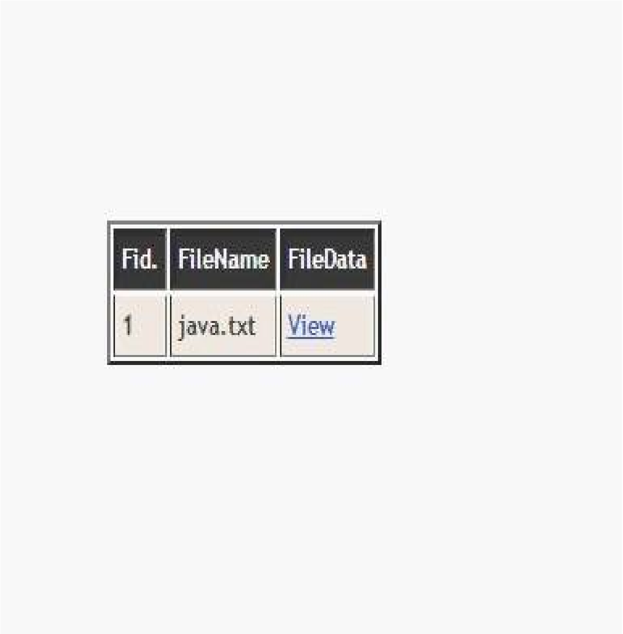
File ID: 1

FileName: java.txt

FileData: Java developers, architects and enthusiasts. Java is designed to enable development of portable, high-performance applications for the widest range of computing platforms possible. By making

Fig.4.5 File Uploading

The User Revocation is shown in the Screen Shot below:



Fid.	FileName	FileData
1	java.txt	View

Fig.4.6 Revocation

The revocation mechanism helps only the authorized people to access files. The cloud server can revoke user if his authorization expires. The revocation mechanism plays a commendable role in providing secured file transfers.

V. CONCLUSION AND FUTURE WORK

This paper proposes a semi-in nominate attribute-predicated privilege control scheme AnonyControl and a planarity-incognito attribute-predicated 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, the system we proposed achieves gentle privilege control in addition to 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 adscititiously leaded detailed bulwark and functioning analysis which shows that AnonyControl is efficient and secured. The AnonyControl-F directly inherits the bulwark of the AnonyControl and thus is equipollent secures as it, but extra communication overhead occurs during the regime of 1-out-of-n incognizant transfer. The future work of our project can be implementation of revocation of users in cloud in a more effective way. Fortifying utilizer revocation is a paramount issue in the authentic application, and it poses a great challenge in applications systems that are using ABE schemes. We should make our revocation mechanism superior to the existing systems so that they can be useful.

.

REFERENCES

[1]https://www.tutorialspoint.com/cloud_computing/cloud_computing_pdf_version.htm
[2] https://en.wikipedia.org/wiki/Attribute-based_encryption
[3] S. S. M. Chow and M. Chase "improving security and privacy in multi authority ABE", in CCS 16th
[4] B.Waters and A.Lewko, "decentralizing ABE" Advances in Cryptology, Germany, Berlin, 2011
[5] https://eprint.iacr.org/2010/351.pdf
[6] B. Lynn. Pairing Based Cryptography (PBC) Website http://crypto.stanford.edu/pbc.

DOI: 10.15680/IJIRCCE.2016. 0409151