Mixing Data Owner And Cloud Side Access Control For Encrypted Cloud Storage

Sucharitha Konduru[1], Nageswara Rao Putta[2], P.Rameswara Anand[3]
[1, 3] Dept of CSE
[2]Associate. Professor, Dept of CSE
[1, 2, 3] Swetha Institute of Technology & Science, Tirupathi, Andhra Pradesh-517561

Abstract- *Now a day's huge demand for cloud computing. But we cannot trust it for host Privacy Sensitive data due to absence of user to cloud controllability. Here for ensuring confidentiality data owners convert their data into encrypted format. To share the encrypted files with others, CP-ABE can be used for owner centric access control. Malicious Attackers attempts to download thousands of files to launch EDoS attcks. In this paper, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE.*

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. Fig.1 shows that Structure of cloud computing. In this section we are discussing about previous existing models. These services typically provide access to advanced software applications and high-end networks of server computers.

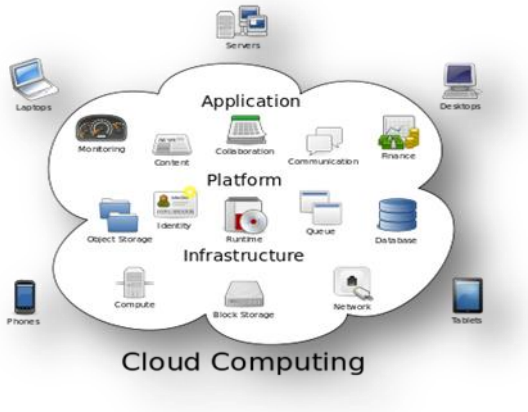

Fig.1 Structure of cloud computing

Characteristics of cloud computing

- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Sthitipragnya Sabat, Prof. Hingoliwala Hyder Ali [1] proposed a combined the cloud side and data owner-side access control in encrypted cloud storage, which is resistant to DDoS/EDoS attacks and provides resource consumption accounting. Our system supports arbitrary CP-ABE constructions. The construction is secure against malicious data users and a covert cloud provider.

Koluguri Shirisha, Mr.K.Raghupati [2] proposed and make use of the covert security, they used bloom filter and probabilistic check in the resource consumption accounting to reduce the overhead. Performance analysis shows that the overhead of our construction is small over existing systems
Miss. Manasi Shet, Dr. S. N. Kini [3] proposed another novel system to remove the single point execution bottleneck and increment the efficiency of the current CP-ABE scheme. By successfully reformulating CP-ABE cryptographic system into this novel structure, the proposed system gives a fine-grained, robust and secure access control with one-CA chosen among multi-AAs for public cloud storage.

Arati Kale, Sarika Kajale, Mansi Raj, Aishwarya Thakare [4] proposed a combined the cloud-side and knowledge owner-side access management in encrypted cloud storage, that is proof against attacks and provides resource consumption accounting. The event is secure against malicious information users and a covert cloud provider

Merahegn Alemayehu, Dr. K Suresh Babu [5] Cloud computing has raised a range of important privacy and security issues. Such issues are due to the fact that, in the cloud, users' data and applications reside at least for a certain amount of time on the cloud cluster which is owned and maintained by a third party.

II. PROPOSED SYSTEM DESIGN

In this section we are going do discuss about system architecture. The below Fig.2 shows that architecture of the proposed system and Fig.3 shows that Data flow diagram for Proposed System

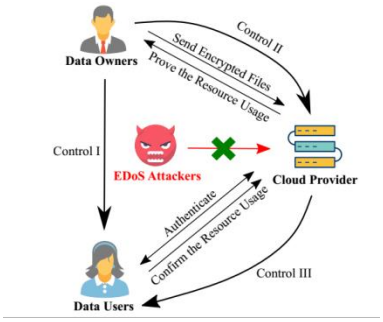

Fig.2 Architecture of the Proposed System

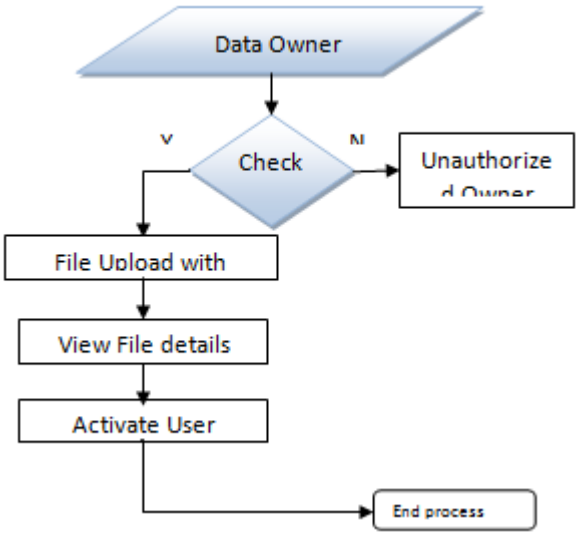

Fig.3 Data flow diagram for Proposed System

III. IMPLEMENTATION

MODULES:

- Data owners
- Data users
- Cloud provider
- Security against EDoS Attacks

Each module is explained as follows

Data owners:: In our proposed system we developed data owner module. Data owners are the owner and publisher of files and pay for the resource consumption on file sharing.

Data users: In this module users want to obtain some files from the cloud provider stored on the cloud storage. They need to be authenticated by the cloud provider before the download (to thwart EDoS attacks). The authorized users then confirm (and sign for) the resource consumption for this download to the cloud provider.

Cloud provider: Cloud provider hosts the encrypted storage and is always online. It records the resource consumption and charges data owners based on that record.

Security against EDoS Attacks: EDoS attackers are those that do not satisfy the access policy (i.e., unauthorized users) but want to trigger the cloud provider to send something through the network, as a result the resource consumption increases.

IV. RESULTS AND DISCUSSIONS

Mixing Data Owner and Cloud Side Access Control for Encrypted Cloud Storage results are shown in below figures. The below Fig.4 shows that owner registration page.

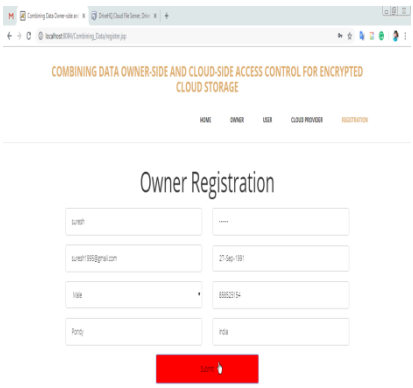

Fig.4 owner registration page

After successful registration of theowner. He / She can directly go for login page shown in below Fig.5

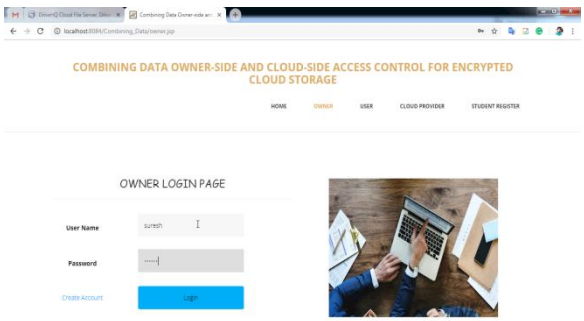

Fig.5 Owner Login Page

After logged in he / she can upload files as shown in the below Fig.6

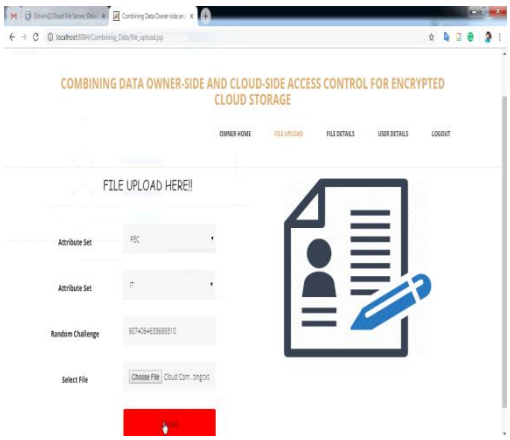

Fig.6 Process of Uploading Files

Uploaded file details are shown in below Fig.7

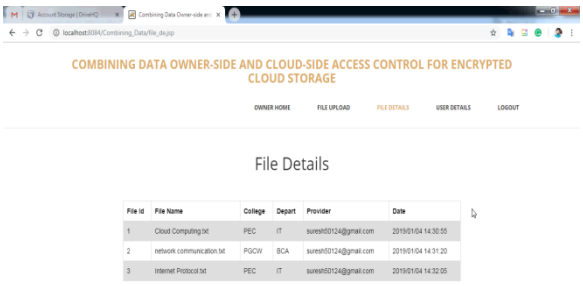

Fig.7 Uploaded File Details

If any students registered means owner can check active students details as shown in Fig.8

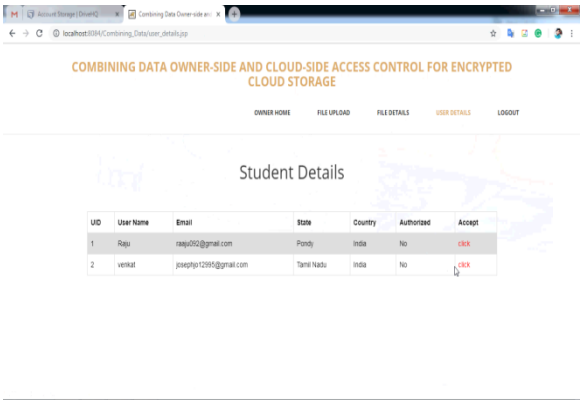

Fig.8 Registered Students Details

Users also registered and logged in to check the File Attributes as shown in Fig.9

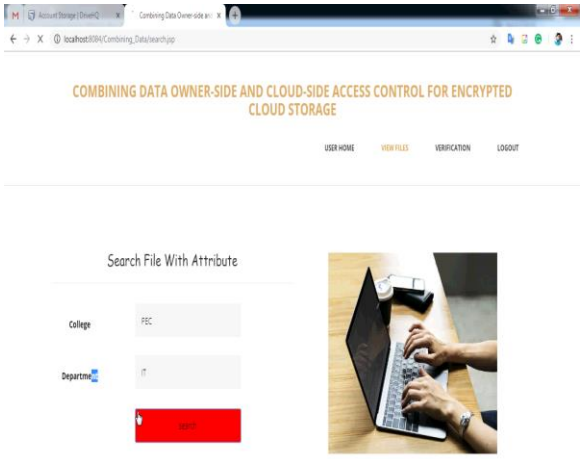

Fig.9 File Attributes Searching Process

After searching the Searched files are appeared as shown in below Fig.10

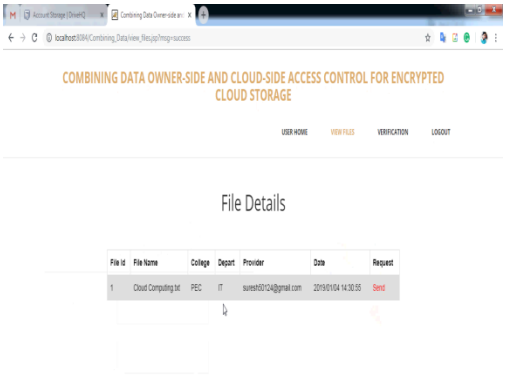

Fig.10 Searched File Details

Cloud Providers can login as shown in below Fig.11

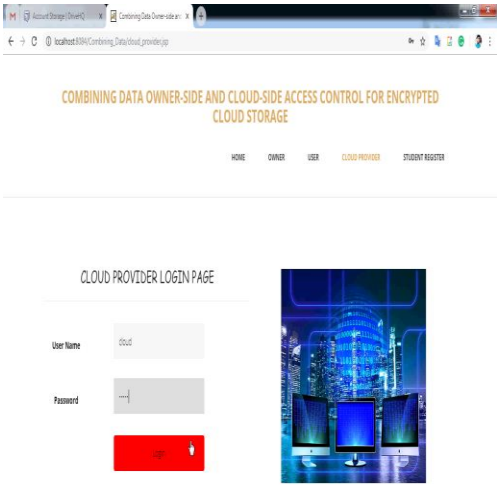

Fig.11 Cloud Provider Login Page

Cloud Provider has the right to check the requests by the users. He can approve users request and finally generate the security key as shown in Fig.12

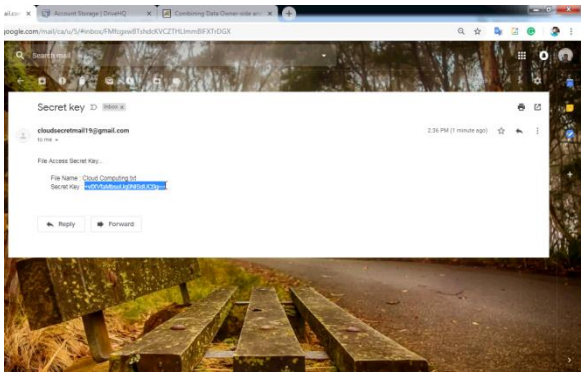

Fig.12 Security Key

V. CONCLUSION

Mixing Data Owner and Cloud Side Access Control for Encrypted Cloud Storage implemented successfully. By using this system we can control malicious attacks and provides resource consumption accounting

REFERENCES

[1] Sthitipragnya Sabat, Prof. Hingoliwala Hyder Ali, "Efficient Two Sided Access Control System in Cloud Storage", International Journal of Innovative Research in Computer And Communication Engineering, Vol. 6, Issue 10, October 2018

[2] Koluguri Shirisha, Mr.K.Raghupati, "Collaborating Data Owner-Side and Cloud-Side Access Control For Cryptcloud Storage, International Journal For Recent Developments In Science & Technology, Volume 03, Issue 09, Sept 2019 ISSN 2581 – 4575

[3] Miss. Manasi Shet, Dr. S. N. Kini, "Secure and Efficient Data Access Control for Public Cloud Storage with Multiple Attribute Authorities", International Journal Of Advance Scientific Research And Engineering Trends, Volume 3 || Issue 6 || June 2018 || ISSN (Online) 2456-0774

[4] Arati Kale, Sarika Kajale, Mansi Raj, Aishwarya Thakare, "Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage", IJRAST, volume 7, issue 6, june 2019

[5] Merahegn Alemayehu, Dr. K Suresh Babu, "IMPROVING CLOUD SECURITY TRUST BY DATA OWNER AND CLOUD-SIDE ACCESS CONTROL FOR SECURE CLOUD STORAGE", Journal of Information and Computational Science, ISSN: 1548-7741, Volume 9 Issue 12 – 2019