Secure and Efficient Attribute-Based Access Control For Multi Authority Cloud Storage

Hema Lalitha Chittimuri[1], Nageswara Rao Putta[2], P.Rameswara Anand[3]
[1] Dept of CSE
[2]Associate Professor, Dept of CSE
[3]Professor, Dept of CSE
[1, 2] Swetha Institute of Technology & Science, Tirupathi, Andhra Pradesh-517561
[3]Jigjiga University, Ethiopia

Abstract- *Sharing our data over the internet using the facility providing by the cloud storage is cost effective. However, this also brings difficult challenges to the access control of shared data since few cloud servers can be fully trusted. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising approach that enables the data owners themselves to place fine-grained and cryptographically-enforced access control over outsourced data. In this paper, we present secure and cost-effective attribute-based data access control for cloud storage systems*

Keywords- Ciphertext Policy, Multi Authority, CP-ABE, Semi Trusted Cloud Server, Cloud Storage.

I. INTRODUCTION

Cloud computing is the use of computing resources that are delivered as a service over a network. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing. In this section we are discussing about existing systems Benefits of cloud computing:

- Achieve economies of scale.
- Reduce spending on technology infrastructure.
- Globalize your workforce on the cheap.
- Streamline processes..
- Reduce capital costs. Improve accessibility.
- Monitor projects more effectively.
- Less personnel training is needed..
- Minimize licensing new software. Improve flexibility.

Miss. Manasi Shet,Dr. S. N. Kini [1] 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. The security analysis shows that the scheme could effectively resist individual and colluded malicious users, as well as the honest-but-curious cloud servers.

N. Meddah , A. Toumanari , L. Fetjah [2] presented a efficient system that provide secure and fine-grained data access control in cloud Computing system based on KP-ABE and a new PRE system with CCA security, collusion resistance, and anonymity in the random oracle model . In future work, they have to propose a scheme to ensure fine-grained access control of Personal Health Records (PHR) allowing the doctors and patients to encrypt their PHRs and store them on semi-trusted cloud servers such that servers do not have access to sensitive PHR contexts.

JIALU HAO [3] proposed an efficient attribute-based access control with authorized search scheme (EACAS), which can meet the requirements for data sharing in cloud storage and protect the data confidentiality and attribute privacy effectively. Implemented it to demonstrate that EACAS is efficient and effective for practical applications. In the future work, they will introduce anonymous KP-ABE with flexible data sharing and efficient data storage for e-health cloud

Amit Wadhwa [4] discussed some of the existing authentication and access control techniques or models implemented over cloud architecture. Also, they discussed and define properties which could be considered for effectively comparing and analyzing the discussed technique or models. Further we also proposed and discussed a multi security level based model, MLBAAC, providing both access control and authentication level security over cloud. The model also made-up to provide protection from man in middle attacks, malicious insider attacks, and faking identity attacks and database hijacking attacks.

Chetan Bulla, Akshata R [5] proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was provable secure in the random oracle model. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

Yinghui Zhang, Member, IEEE, Dong Zheng, Robert H. Deng, Fellow, IEEE [6] efficiently addressed data security and user privacy issues in s-health by introducing PASH, privacy aware s-health access control system. The main building block of PASH is a CP-ABE scheme which supports large universe and partially hidden access policies. In PASH, sensitive attribute values involved in access policies are hidden and generic attribute names are public. They added an efficient decryption test before full decryption to improve efficiency.

II. PROPOSED SYSTEM DESIGN

In this section we are discussing about proposed system. The below Fig.1 shows that Structure of Proposed system

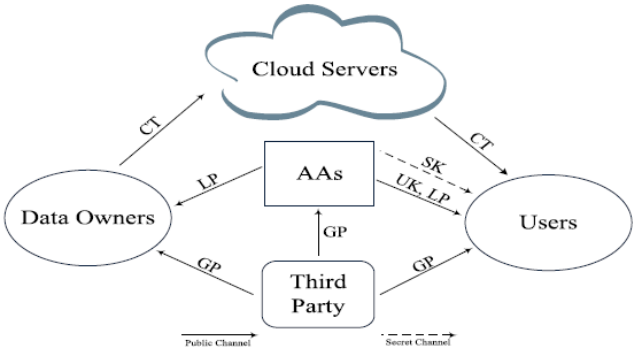

Fig.1 Structure of Proposed system

III. IMPLEMENTATION

Implementation of Proposed system based on five modules. Those are

- **Semi trusted third party**

It is just in charge of producing the global public parameter of the system, which is shared among all authorities and users in the system. Particularly, it does not keep any secret key, and also does not generate any secret keys for authorities and users. Thus, it makes no difference on the security of the system.

- **Attribute authority**

Each attribute authority independently manages its own attribute universe and sets up its own public parameter and master secret key. It is responsible for checking the validity of a user's attributes belonging to its domain. If yes, it issues a secret key component to the user according to his/her attributes. In addition, it is also in charge of periodically generating an update key for users that are not revoked in its domain. In our system, any string can be an attribute, and each attribute belongs to only one authority. Fig.2 shows that Flow diagram for Attribute authority

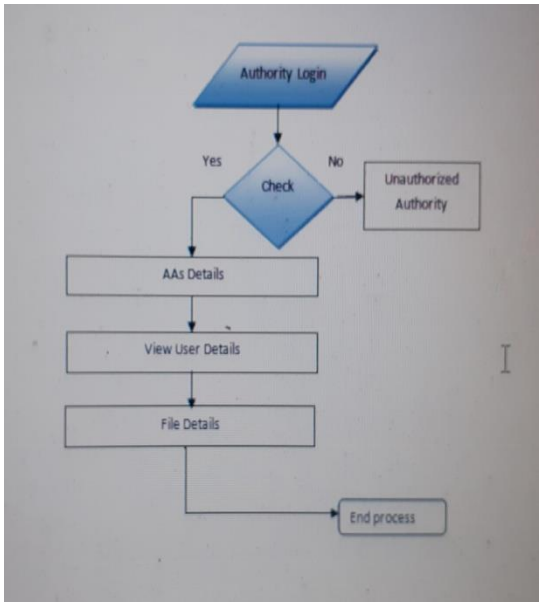

Fig.2 Flow diagram for Attribute authority

- **Data owner**

The data owner is an entity that owns data and would like to share his/her data by outsourcing them to cloud servers managed by cloud service providers. A data owner first defines an intended access policy over attributes, and enforces it over the data by calling the proposed multi authority CP-ABE scheme. Then, the owner sends the encrypted data to cloud servers. Fig.3 shows that Flow Diagram for Data owner

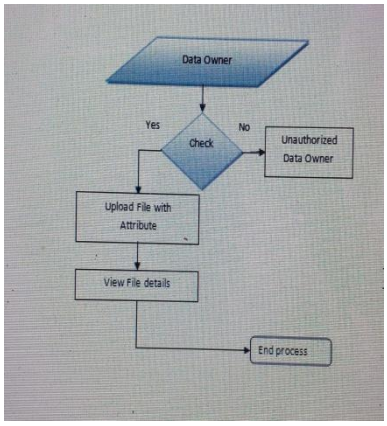

Fig.3 Flow Diagram for Data owner

- **User**

Each user owns a unique global identifier in the system, and possesses a set of attributes and the corresponding secret key, which consists of all secret key components issued by different attribute authorities (AAs). If a user is not revoked by an authority at some time period, he/she can utilize the published update key to update the corresponding secret key component. Fig.4 Flow Diagram for Data User

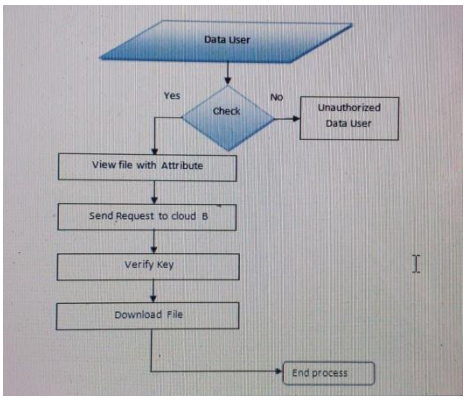

Fig.4 Flow Diagram for Data User

- **Semi trusted cloud server**

A cloud server is in charge of storing and updating those encrypted data from data owners. Here, we emphasize that the update procedure can be done by just using the public parameter of the system (including the global public parameter and the public parameter of all authorities), without the involvement of secret information. We assume that it is semi trusted (curious but honest), namely, it will honestly perform the valid assignments, but will attempt to learn information about the outsourced data as much as possible. Fig.5 shows that Flow Diagram for Semi trusted cloud server

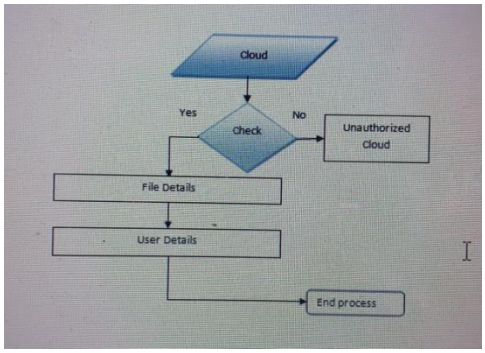

Fig.5 Flow Diagram for Semi trusted cloud server

IV. RESULTS AND DISCUSSIONS

In this section we are discussing about results of the proposed system. Fig.6 shows that data owners login page.

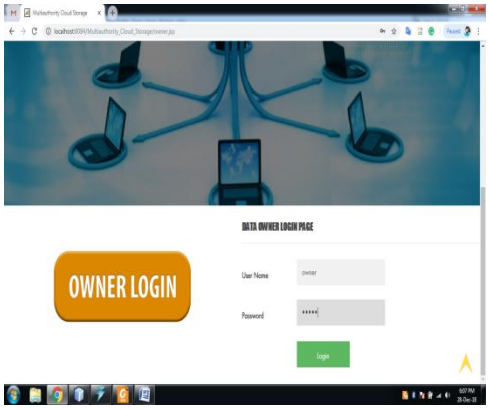

Fig.6 Data Owners Login Page.

- File uploading process is shown in the below Fig.7

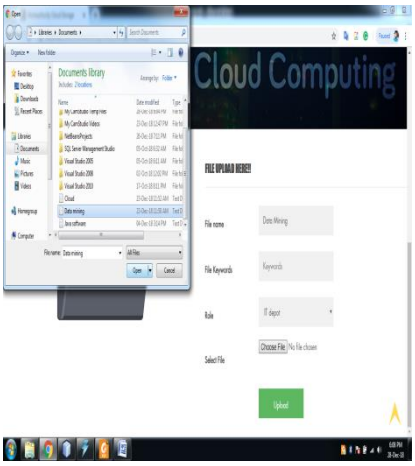

Fig.7 File uploading Process

- Uploaded files details are shown in the Fig.8

Fig.8 uploaded Files details

- Data user login page as shown in Fig.9

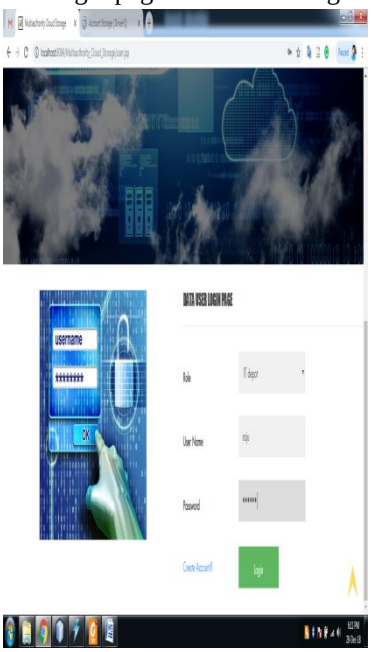

Fig.9 Data User Login Page

- AAs login page as shown in Fig.10

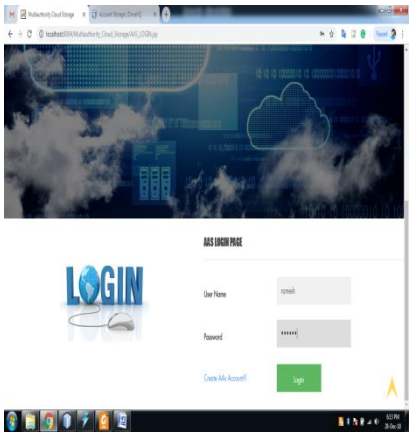

Fig.10 Aas Login Page

V. CONCLUSION

In this paper, to build a secure and cost-effective multi authority attribute-based access control scheme for data sharing in cloud storage systems, we proposed a multi authority CP-ABE scheme supporting scalable user revocation and public ciphertext update. The proposed scheme achieves the intended security properties of forward security and backward security, and can also withstand decryption key exposure. We proved the security of the proposed scheme in the random oracle model. Both performance discussions and implementation experiments show that our scheme is more desirable for practical applications.

REFERENCES

[1] 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

[2] N. Meddah , A. Toumanari , L. Fetjah "Anonymous Attribute based Access Control in Cloud Computing", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, IJERTV4IS040844 , Vol. 4 Issue 04, April-2015

[3] JIALU HAO, (Student Member, IEEE), JIAN LIU, HUIMEI WANG, LINGSHUANG LIU, MING XIAN, AND XUEMIN (SHERMAN) SHEN (Fellow, IEEE), "Efficient Attribute-based Access Control with Authorized Search in Cloud Storage", IEEE Access · March 2019

[4] Amit Wadhwa, Vinod Kumar Gupta, " Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017)

[5] Chetan Bulla, Akshata R. Patil, Priyanka B. Guttedar and Reshma G. Giddenavar, " Expressive, Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage", International Journal of Computer Science Trends and Technology (IJCST) – Volume 4 Issue 3, May - Jun 2016

[6] Yinghui Zhang, Member, IEEE, Dong Zheng, Robert H. Deng, Fellow, IEEE, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control", Published in IEEE Internet of Things Journal, 2018 April, Volume 3, Issue 1.