JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

Attribute-based Encryption System for Secured Data Storage

ABSTRACT:

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the cipher text-policy attribute-based encryption (CP-ABE)

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

scheme by Bethencourt *et al.* and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

ARCHITECTURE:

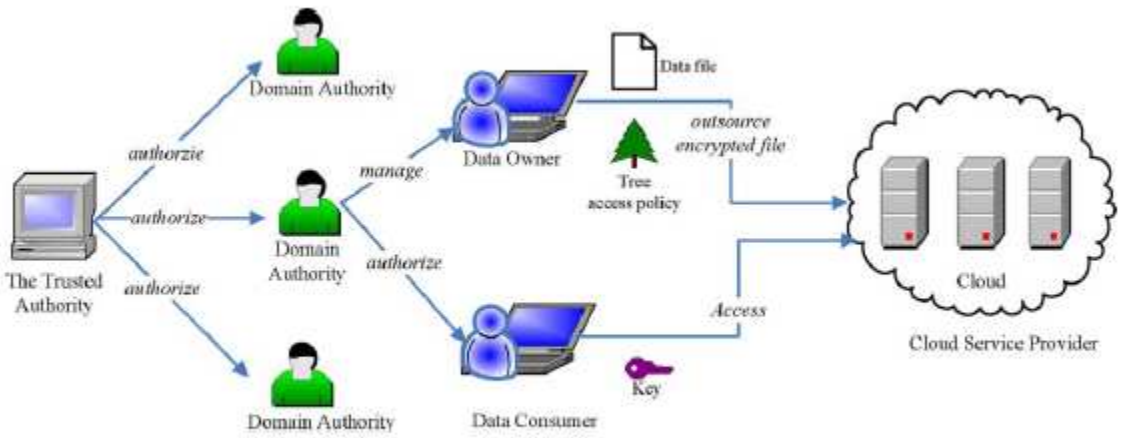

Fig. 1. System model.

EXISTING SYSTEM:

Our existing solution applies cryptographic methods by disclosing data decryption keys only to authorize users.

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well.

DISADVANTAGES OF EXISTING SYSTEM:

Software update/patches- could change security settings, assigning privilegestoo low, or even more alarmingly too high allowing access to your data by other parties.

Security concerns- Experts claim that their clouds are 100% secure - but it willnot be their head on the block when things go awry. It's often stated that cloudcomputing security is better than most enterprises. Also, how do you decidewhich data to handle in the cloud and which to keep to internal systems once decided keeping it secure could well be a full-time task?

Control- Control of your data/system by third-party. Data - once in the cloudalways in the cloud! Can you be sure that once you delete data from your cloudaccount will it not exist any more... ...or will traces remain in the cloud

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

PROPOSED SYSTEM:

This proposed system addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents.

We propose a hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. HASBE extends the ciphertext-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control.

ADVANTAGES OF PROPOSED SYSTEM:

- Low initial capital investment
- Shorter start-up time for new services

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

- Lower maintenance and operation costs

- Higher utilization through virtualization

- Easier disaster recovery

More specifically, we associate each data file with a set of attributes, and assign each user an expressive access structure whichis defined over these attributes. To enforce this kind of access control, we utilize KP-ABE to escort data encryption keys of data files. Such construction enables us to immediately enjoy fine-grainedness of access control. However, this construction, if deployed alone, would introduce heavy computation overhead and cumbersome onlineburden towards the data owner, as he is in charge of all the operations of data/user management. Specifically, such an issue is mainly caused by the operation of user revocation, which inevitably requires the data owner to re-encrypt all the data files accessible to the leaving user, oreven needs the data owner to stay online to update secret keys for users. To resolve this challenging issue and make the construction suitable for cloud computing, we uniquely combine PRE with KP-ABEand enable the data owner to delegate most of the computation intensive operations to Cloud Servers without disclosing the underlying file contents. Such a construction allows the data owner to control access of his data files with a minimal overhead in terms

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

of computation effort and online time, and thus fits well into the cloud environment. Data confidentiality is also achieved since Cloud Serversare not able to learn the plaintext of any data file in our construction. For further reducing the computation overhead on Cloud Servers andthus saving the data owner's investment, we take advantage of thelazy re-encryption technique and allow Cloud Servers to "aggregate "computation tasks of multiple system operations. As we will discuss in section V-B, the computation complexity on Cloud Servers is eitherproportional to the number of system attributes, or linear to the size of the user access structure/tree, which is independent to the number of users in the system. Scalability is thus achieved. In addition, our construction also protects user access privilege information againstCloud Servers. Accountability of user secret key can also be achieved by using an enhanced scheme of KP-ABE.

MODULES:

- Data Owner Module
- Data Consumer Module
- Cloud Server Module
- Attribute based key generation Module

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

MODULES DESCRIPTION:

- **Data Owner Module**

  In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

- **Data Consumer Module**

  In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Domain authority and the Data user's are controlled by the Domain Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges.

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

- **Cloud Server Module**

  The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

- **Attribute based key generation Module**

  The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.The trusted authority calls the algorithm to create system public parameters PK and master key MK. PK will be made public to other parties and MK will be kept secret. When a user sends request for data files stored on the cloud, the cloud sends the corresponding ciphertexts to the user. The user decrypts them by first calling decrypt(CT,SK) to obtain DEK and then decrypt data files using DEK.

JP INFOTECH
SOFTWARE DEVELOPMENT & RESEARCH DIVISION
www.jpinfotech.org
(0)9952649690

Chennai Office : JP INFOTECH, Old No.31, New No. 86, 1st Floor , 1st Avenue , Ashok Pillar , Chennai - 83.
Landmark : Next to Kotak Mahendra Bank.

Pondicherry Office : JP INFOTECH , #45 , Kamaraj Salai, Thattanchavady, Puducherry
Landmark : Next to VVP Nagar Arch.

jpinfotechprojects@gmail.com

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : - Windows XP.
- Coding Language : J2EE
- Data Base : MYSQL