

HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing

Shubham Dayanand Amane

*Department of Computer Science and Engineering, SVERI's College of Engineering,
Pandharpur*

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 cipher text-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) 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.

SYSTEM ANALYSIS

EXISTING SYSTEM:

Our existing solution applies cryptographic methods by disclosing data decryption keys only to authorize users. 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 will not be their head on the block when things go awry. It's often stated that cloud computing security is better than most enterprises. Also, how do you decide which 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 cloud always in the cloud! Can you be sure that once you delete data from your cloud account will it not exist any more... ..or will traces remain in the cloud

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 cipher text-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
- 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 which is defined over these attributes. However, this construction, if deployed alone, would introduce heavy computation overhead and cumbersome online burden 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, or even 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-ABE and enable the data owner to delegate most of the computation intensive operations to Cloud Servers without disclosing the underlying file contents.

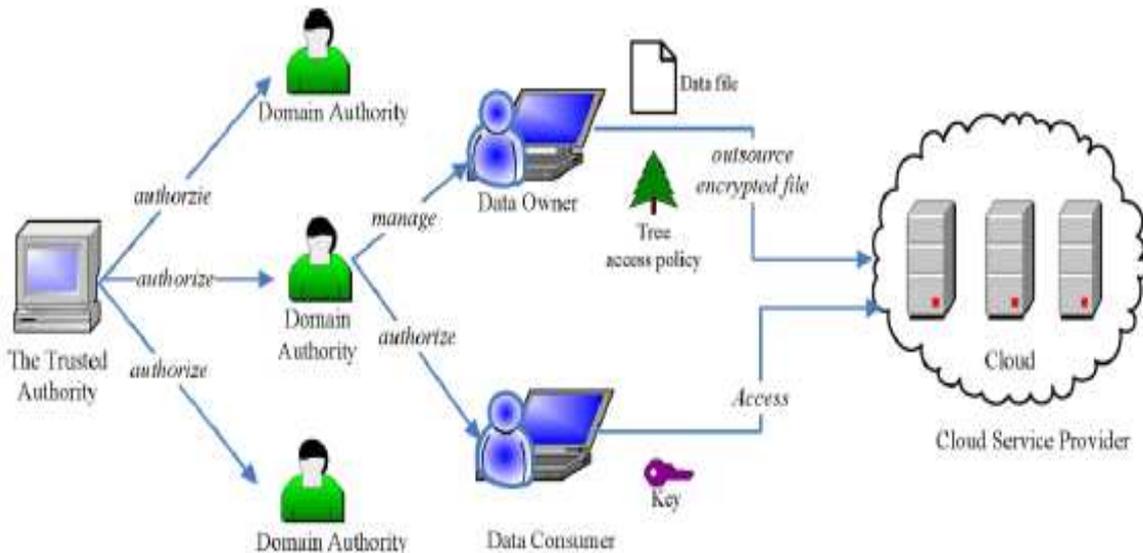
ARCHITECTURE:

Fig. 1. System model.

IMPLEMENTATION MODULES:

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

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.

- **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.

CONCLUSION:

In this paper, we introduced the HASBE scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. The HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. We formally proved the security of HASBE based on the security of CP-ABE by Bettencourt *et al.*. Finally, we implemented the proposed scheme, and conducted comprehensive performance analysis and evaluation, which showed its efficiency and advantages over existing schemes.

REFERENCES

- [1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Comput. Syst.*, vol. 25, pp. 599–616, 2009.
- [2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: <http://aws.amazon.com/ec2/>
- [3] Amazon Web Services (AWS) [Online]. Available: <https://s3.amazonaws.com/>
- [4] R. Martin, "IBM brings cloud computing to earth with massive new data centers," *InformationWeek* Aug. 2008 [Online]. Available: [http:// www.informationweek.com/news/hardware/data centers/209901523](http://www.informationweek.com/news/hardware/data_centers/209901523)