Adaptive Delegation Authority Enhancement to Hasbe for Efficient Access Control in Distributed Cloud Computing

N. R .SINDHU PRIYA[1] M.KUMARESAN[2]
[1]M. E. [2]Assistant Professor
[1,2]PGP College of Engineering and Technology, Namakkal

Abstract— Cloud computing have high demand due to waste and huge data usage of clients. The privacy and security become major concern on the outsourced cloud data storage. The attribute based encryption schemes are used recently for access control of outsourced cloud data. It has highly inflexible in implementing complex access control policies. The existing work presented Hierarchical attribute set based Encryption (HASBE) that extended cipher-text policy attribute set based encryption (ASBE) with hierarchical structure of users. It used achieve scalability, inherits flexibility, fine grained access control, and employs multiple value assignments for access expiration time, and deal with user revocation efficiently. The performance analysis is made to evaluate the computational complexity of access control for outsourced data in cloud computing. However varying of cloud service provider complicates the hierarchical access control policies. The proposal presented an Adaptive Delegation Authority model enhancement to HASBE. It is used to minimize the complexity of access control policies in changing cloud service provider. The delegation authority coordinates the data owners and consumer for easy and quick data access control. It intimates the data owners and consumers about the authority delegation.
The delegation authority sends encryption standards to be followed thereafter. The simulation is carried with Cloud simulator using java to testify in the effectiveness of Adaptive Delegation Authority enhancement to HASBE.

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 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 improves not only the speed, but also the quantity and quality of resources available to your organization. Going beyond the limits of traditional IT infrastructure and data centers offers you more choice, flexibility and agility and becomes your competitive advantage**.**
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.

Fig. 1: Cloud Computing

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 ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt and analyze its performance and computational complexity. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing.
It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Despite the tremendous benefits, security is the primary obstacle that prevents the wide adoption of this promising computing model, especially for customers when their confidential data are consumed and produced during the computation. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc.
Distributed computing in cloud is nothing more than utilizing many networked computers to partition (split it into many smaller pieces) a question or problem and allow the network to solve the issue piecemeal. Another instance of distributed computing, for storage instead of processing

power, is bit torrent. A torrent is a file that is split into many pieces and stored on many computers around the internet. When a local machine wants to access that file, the small pieces are retrieved and rebuilt. P2P network that send communication/data packages into multiple pieces across multiple network routes. Then assemble them in receivers end. Distributed computing on cloud is nothing but next generation framework to utilize the maximum value of resources over distributed architecture

An Adaptive Delegation Authority model to enhance the HASBE model is used to delegation authority is based on the criteria of user demand in changing cloud computing storage service providers. The attribute encryption authority is delegated to the new domain authority or trusted authority. The variation of trust authority changes is attribute encryption key model. Data consumers adapt to the new authority of access control automatically without any delay. Newly delegated authority updates the data consumers and owners regarding access control key policies in quicker time. Peer cloud computing models delegates authority of access control management on user demand and location. The simulation is carried out in distributed cloud computing scenario to testify authority delegation to HASBE.

II. LITERATURE SURVEY

Information and Communications Technology (ICT) over the last half century, there is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, gas, and telephony). This computing utility, like all other four existing utilities, will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community [1]. A GSAKMP policy token is a highly flexible data structure used to define the behavior of a group. The token defines an exhaustive list of policies (there are over 150 different fields supporting a wide range of policies and mechanisms). With small exception, the group is free to define policies containing as many (or as few) of these fields as is desirable. Thus, groups with varying abilities and requirements can be defined through the policy token [2].

Each statement identifies context-sensitive session requirements. A reconciliation algorithm attempts to identify a policy instance compliant with the stated requirements. The correctness of efficient two-policy reconciliation algorithm is proved, and show by reduction that three or more policy reconciliation is intractable [3]. UniPro, a unified scheme is introduced to model protection of resources, including policies, in trust negotiation. UniPro improves on previous work by modeling policies as first-class resources, protecting them in the same way as other resources, providing fine-grained control over policy disclosure, and clearly distinguishing between policy disclosure and policy satisfaction, which gives users more flexibility in expressing their authorization requirements [4].

In automated trust negotiation (ATN), two parties exchange digitally signed credentials that contain attribute information to establish trust and make access control decisions. Because the information in question is often sensitive, credentials are protected according to access control policies. In traditional ATN, credentials are transmitted either in their entirety or not at all [5]. In the cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. The applicability of our construction to sharing of audit-log information is demonstrated and broadcast encryption. This construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) [6].

To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, 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 [7]. In a ciphertext policy attribute based encryption system, a user's private key is associated with a set of attributes (describing the user) and an encrypted ciphertext will specify an access policy over attributes. A user will be able to decrypt if and only if his attributes satisfy the ciphertext's policy [8].

Identity-Based Encryption (IBE) scheme is introduced which is based on Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, to decrypt a cipher text encrypted with an identity, if and only if the identities are close to each other as measured by the "set overlap" distance metric [9]. Cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and productivity enhancements by using cloud-based services to manage projects, to make collaborations, and the like [10].

Ciphertext-Policy Attribute-Set Based Encryption (CP-ASBE) is a form of CP-ABE that addresses the above limitations of CP-ABE by introducing a recursive set based structure on attributes associated with user keys. Specifically CP-ASBE allows, User attributes to be organized into a recursive family of sets and Policies that can selectively restrict decrypting users to use attributes from within a single set or allow them to combine attributes from multiple sets.

III. ADAPTIVE DELEGATION AUTHORITY ENHANCEMENT TO HASBE FOR EFFICIENT ACCESS CONTROL IN DISTRIBUTED CLOUD COMPUTING

1. Cloud Computing Services
2. Access Control
3. Hierarchical attributes set encryption
4. Authority delegation
5. Dynamic access control policy

A. Cloud Computing Services

Cloud Computing systems comprises of cloud service provider and manages cloud to provide data storage. The data owners encrypt their data files and store in cloud. Data consumers are downloading and decrypt data files from cloud for their usage. The domain authorities are managed by its parent domain authority or trusted authority.

Trusted authority is issue authentication to data in the cloud.

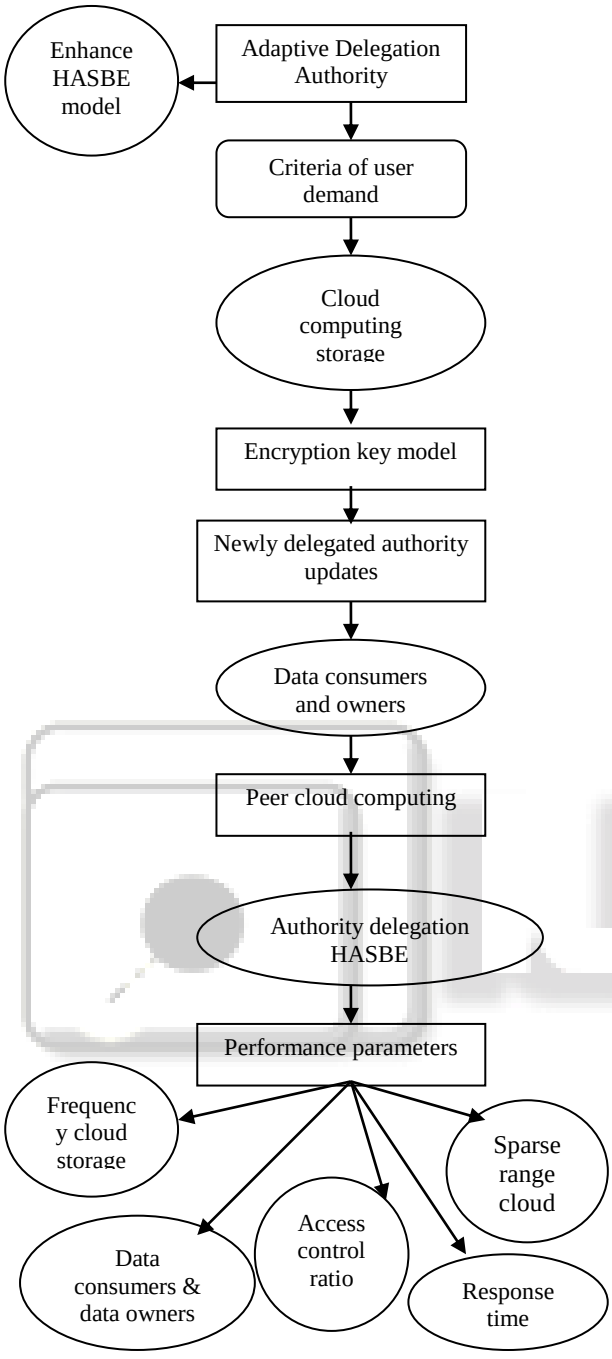

Fig. 1: Enhance HASBE model process

The hierarchical organization of the cloud system users is data owners, data consumers, domain authority, and trusted authority. Data owners and consumers are not always online. Cloud service provider, domain and trusted authority are always in the online. The cloud has abundant storage capacity and computation power and the data consumer's access data file only for reading.

B. Access Control

Trusted authority is responsible to generating and distributing system parameters and root master keys that authorizing the top-level domain authorities. The domain authority is responsible for delegating keys to subordinate domain authorities at next level or users in its domain. Each user in the system is assigned a key structure to specify attributes associated with the user's decryption key.

C. Hierarchical attributes set encryption

HASBE components are System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion. Trusted authority calls HASBE algorithm to create the system public parameters to made public to other parties for master key and kept secret. HASBE algorithm selects a bilinear group of prime order with generator and chooses random exponents. File Access user sends request for data files stored on the cloud, cloud sends corresponding cipher texts to the user and user decrypts them by invoking DECRYPT function to obtain decryption value to decrypt data files. User Revocation is done to make sure for revoked user cannot access associated data files. New File Creation is used to protect data stored on the cloud. The data owner first encrypts data files and it stores encrypted data files on the cloud for each file is encrypted with a symmetric data encryption key in turn encrypted with HASBE. Before uploading to cloud, data file is processed by the data owner as to pick a unique ID for the data file and that files are randomly choose a symmetric data encryption key. Encrypt the data file that define a tree access structure for the file and encrypt using HASBE algorithm which returns Ciphertext. Finally encrypted data file is stored on the cloud

D. Authority delegation

Data consumers demand of various files needs that cause file access permission a constraint in turn, influence the data owner to delegate authorization. Data owner provide temporarily, delegates to the authorization of file access permission (for data consumers) to intermediary party or other trusted party in the lower hierarchy. The delegation authority allocates access permission to data consumers as is assigned by the higher authority rule delegation for file attributes in dynamic cloud data access environment. The attribute encryption authorization is delegated to new domain authority or trusted authority.

E. Dynamic access control policy

Dynamic nature of trusted authority is enforcing the attribute encryption key model to be changed as and when highly demanded. The data consumers get access permission from new trusted authority that having delegation powers to allow file access permissions. The access control automatically changes without any delay and that file access permission is granted quickly to data consumers. Delegated authority modifies the access policies of data consumers based on access control key of data files. Distributed cloud computing models delegates authority of access control management on user demand and location.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

Experiment is conducted on Access Control for evaluating the performance of Adaptive Delegation Authority Enhancement to HASBE for Efficient Access Control in Distributed Cloud Computing. Proposed Adaptive Delegation Authority Enhancement to HASBE for Efficient Access Control in Distributed Cloud Computing evaluated with different performance metrics and compare it with

Existing HASBE for access control in cloud computing.
By comparing Existing HASBE for access control, the experimental results show that Proposed Adaptive Delegation Authority Enhancement to HASBE.
The performance of Privacy Proposed Adaptive Delegation Authority Enhancement to HASBE is evaluated by the following metrics

1. Delegation to Access Control Ratio
2. Response Time for Access Control Policy Alerts
3. Sparse Range of Cloud Data

Number of Cloud Storage Providers	Existing HASBE for Access Control	Proposed Adaptive Delegation Authority model
10	5.4	8.9
20	4.8	7.5
30	3.6	6.2
40	2.7	5.3
50	1.5	4.4

Table 1: Delegation to Access Control Ratio

Fig 2 describes the delegation to access control ratio. X axis represent the number of cloud storage providers. Whereas Y axis denotes the delegation to access control ratio using both the existing HASBE for Access Control and our proposed Adaptive Delegation Authority Model.
When the number of cloud storage providers increased the delegation to access control ratio will get decreased. The Adaptive Delegation Authority Model achieves 20% to 35% more delegation to access control ratio when compared with the existing scheme.
Figure 3 demonstrates the response time for access control policy alerts. X axis represents number of data consumer and data owners whereas Y axis denotes the response time for access control policy alerts using both the HASBE for Access Control and our proposed Adaptive Delegation Authority Model.

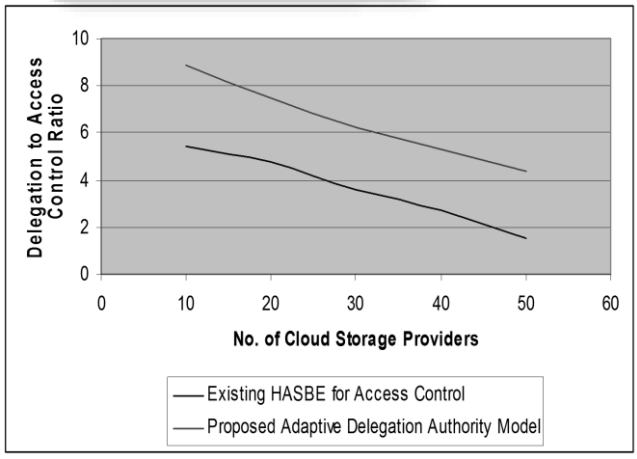

Fig. 3: Delegation to Access Control Ratio

When the number of data consumer and data owners increased response time for access control policy alerts also gets increased.
Figure 3 shows the effectiveness of response time for access control policy alerts over different number of data consumer and data owners than existing HASBE for Access Control and our proposed Adaptive Delegation Authority Model. Adaptive Delegation Authority Model achieves 25% to 45% less access control policy alerts on response time,
When compared with existing schemes.

Number of Data Consumer and Data Owners	Existing HASBE for Access Control	Proposed Adaptive Delegation Authority model
20	30	10
40	38	18
60	46	25
80	52	30
100	69	45

Table 2: Response Time for Access Control Policy Alerts

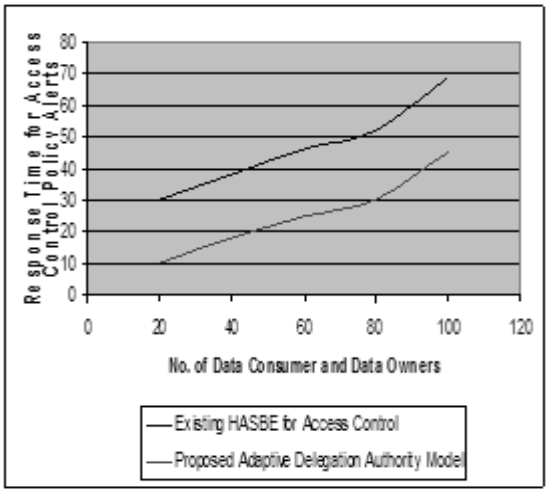

Fig. 4: Response Time for Access Control Policy Alerts

Number of Cloud Storage Providers	Existing HASBE for Access Control	Proposed Adaptive Delegation Authority model
10	250	500
20	200	400
30	150	300
40	100	200
50	50	100

Table 3: Sparse Range of Cloud Data

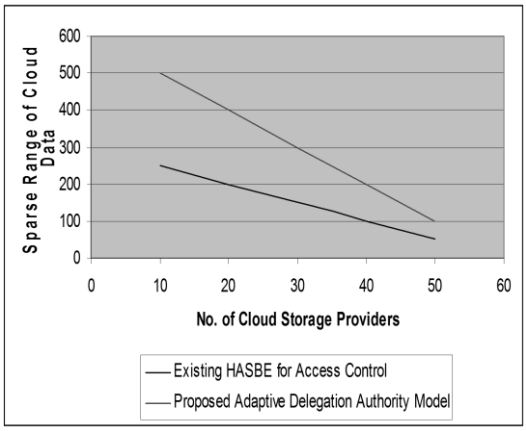

Fig. 5: Sparse Range of Cloud Data

Figure 4 demonstrates the sparse range of cloud data. X axis represents the number of cloud storage providers whereas Y axis denotes the sparse rage of cloud data using both HASBE for Access Control and our proposed Adaptive Delegation Authority Model. When the number of cloud storage providers decreased number of sparse range of cloud data also gets decreased. All the curves show a more of less

yet steady descendant when cloud storage providers increases. Figure 4 shows better data for sparse range of cloud of Adaptive Delegation Authority Model. Adaptive Delegation Authority Model achieves 40% to 60% more sparse range of cloud data result.

V. 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. Finally, we implemented the proposed scheme, and conducted comprehensive an Adaptive Delegation Authority model to enhance the HASBE model. The delegation authority is based on the criteria of user demand in changing cloud computing storage service providers. It is used to overcome attribute encryption authority is delegated to the new domain authority or trusted authority.

REFERENCES

[1] Shucheng Yu, Yao Zhen, Kui Ren, Wenjing Lou,"scalable and secure sharing of personal health record in cloud computing using Attribute based encryption",2012.
[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.
[3] G.Wang, Q. Liu, and J.Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.
[4] 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.
[5] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.
[6] R.Buyya, C. S. Yeo, and S. Venugopal. Market-Oriented Cloud Computing: Vision, Hype, and Reality forDelivering IT Services as Computing Utilities. In Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC 2008), Dalian, China, Sept. 2008.
[7] J.Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy, 2007.
[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM Conference on Computer and Communications Security, pages 89–98, 2006.
[9] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. 2005.
[10] C. Cocks. An identity based encryption scheme based on quadratic residues. In B. Honary, editor, IMA Int. Conf., volume 2260 of Lecture Notes in Computer Science, pages 360–363. Springer, 2001.

