RESEARCH ARTICLE OPEN ACCESS

# Access Control and Revocation for Digital Assets on Cloud with Consideration for Sharing

Prof.Sabera Begum[1], Mohd.Ghouse[2]
[1] *Professor, Department of Computer Science & Engineering, KCT Engineering College, Kalaburagi-585104* ,
[2] *U.G. Student, Department of Computer Science & Engineering, KCT Engineering College, Kalaburagi-585104 Karnataka, India*

**Abstract**
In cloud computing applications, users' data and applications are hosted by cloud providers. With internet and cloud availability increasing numbers of people are storing their content on cloud. Also with presence of social networking, contents stored on cloud are also shared. This requires more security for the contents on cloud. Traditional security solution address only encryption, decryption of data on cloud and its access control , but with this new trend of sharing, the scope of security becomes even higher. In this paper we propose a solution of integrated access control for contents shared on cloud and its efficient revocation.

.

## I. INTRODUCTION

Cloud computing has attracted extensive attentions from both academic and IT industry. It can provide low-cost, high-quality, flexible and scalable services to users. In particular, cloud computing realizes the pay-on-demand environment in which various resources are made available to users as they pay for what they need. Cloud storage is one of the most fundamental services, which enables the data owners to host their data in the cloud and through cloud servers to provide the data access to the data consumers (users). However, it is the semi-trusted cloud service providers (CSPs) that maintain and operate the outsourced data in this storage pattern. Therefore, the privacy and security of users' data are the primary obstacles that impede the cloud storage systems from wide adoption. To prevent the unauthorized entities from accessing the sensitive data, an intuitional solution is to encrypt data and then upload the encrypted data into the cloud. Cryptography algorithms are available for encryption and decryption. But this scheme is fine if the user is only person who stores and retrieves from cloud. In case of multi users, flexibility is needed to provide access control on the data and the operation other user can do on that data like modifying it or sharing. Methods like ABE are available for access control but they cannot control the user's action on content once they got the access right for the content.

In this paper, we provide a solution for multiple users to collaborate in cloud and create content, access control on the content and sharing on content and revoking the control.

## II. RELATED WORK

In this section we survey the current solutions for access control for users in cloud computing and their drawbacks. Goval et al. [1] formulated two complimentary forms of ABE: key policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, user's secret key is associated with an access policy and each cipher text is labeled with a set of attributes; while in CP-ABE, each cipher text is associated with an access policy and user's secret key is labeled with a set of attributes. Compared with KP-ABE, CP-ABE is more suitable for the cloud-based data access control since it enables the data owner to enforce the access policy on outsourced data.

Hur and Noh [1] proposed an immediate attribute-level revocation mechanism in CP-ABE by utilizing a binary key-encrypted-key tree for attribute group key distribution. Different from the attribute-level revocation, user-level revocation makes the revoked users lose all the access privileges in the system.

Yu et al. [4] proposed a CP-ABE scheme with indirect attribute-level revocation by the semi-trusted proxy deployed in the data server.The key re-randomization is adopted in Yang et al.'s CP-ABE scheme [3].

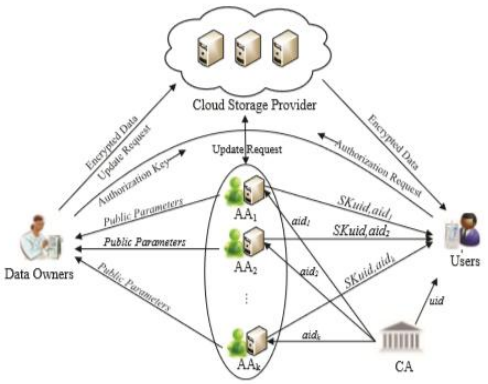
Bethencourt et al. explicitly formalized the notion of CP-ABE and proposed a CP-ABE scheme in [5], but its security proof was given in the generic group model.

Cheung and Newport [6] proposed another CP-ABE scheme that supports AND∗ +,− access policy, and proved its security under decision bilinear Diffie Hellman assumption ABE (MA-ABE) scheme was proposed by Chase in [17], where there are several AAs and one central authority (CA) in the system. Each AA issues a set of attribute secret keys

to each user, while the CA distributes a global unique identifier together with a final secret key to each user.
Emura et al. [18] put forth a CP-ABE scheme with constant size cipher text. And yet, their scheme only supports the (n,n)threshold access policy on multi-valued attributes. Another CP-ABE scheme with constant-size ciphertext was proposed in [19], and works for the (t,n)-threshold case. Cheng et al. [20] proposed two new CP-ABE schemes, which have both constant-size ciphertext and small computation cost for AND∗ +,− access policy. The revocation issue is an important and cumbersome problem in attribute-based systems

## III. PROPOSED SOLUTION

The architecture of the proposed solution




The CA sets up the system and responses the registration requests from all the AAs and users. However, the CA is not involved into any attribute-related management.

Each AA administers a distinct attribute domain and generates a pair of public/secret key for each attribute in this attribute domain. Without any doubt, each attribute is only managed by a single AA. Once receiving the request of attribute registration from a user, the AA generates the corresponding attribute secret keys for this user. Additionally, each AA is responsible to execute the attribute revocation of users. Before uploading a shared data to the cloud storage servers, the data owner defines an access policy and encrypts the data under this access policy. After that, the data owner sends the cipher text and its corresponding access policy to the CSP. Meanwhile, the data owner is responsible for issuing and revoking the user's authorization. Each user is labeled with a set of attributes, besides a global unique identifier. In order to obtain the shared data, each user needs to request the attribute secret keys and authorization from AAs and data owner, respectively. Any user can download the cipher text from the CSP.Only the authorized user who has the specific attributes can successfully recover the outsourced data. It becomes obvious that the CSP provides data storage service and enforces the process of ciphertext update. The ciphertext update occurs in the following two cases: (1) any of AAs revokes users' one or more attributes; (2) the data owner revokes one or more authorized users.

The proposed scheme uses a fine-grained attribute based access control approach. In fine-grained attribute-based access control, a set of access control rules specifies the conditions under which access to a digital asset is granted. The rules are defined in terms of the attributes that a user might possess, e.g., radar designer, etc.

Cloud providers store their users' digital assets. Each asset has an access control list containing rules that allow users to access the asset based on the attributes possessed by the users. An access control list specifies three access modes: read, write, and share. Each mode has a set of access control rules. A user may access an asset in a given mode if the user satisfies the access control rule for that access mode. The owner of an asset delegates the access permission of the asset to other users by setting the access control rule for each of the access modes of the asset.

A user that satisfies the access control rule of an asset is called a delegate. For each access mode, the owner also specifies whether a delegate can further delegate her access permission to other users. If further delegation is allowed, the delegates can delegate their permissions to other users by specifying their own access control rules. Thus, a chain of delegation can be formed for each access mode of the asset. The users high up in the chain can revoke the delegations to the users lower down in the chain.

**Advantages of Proposed Solution**

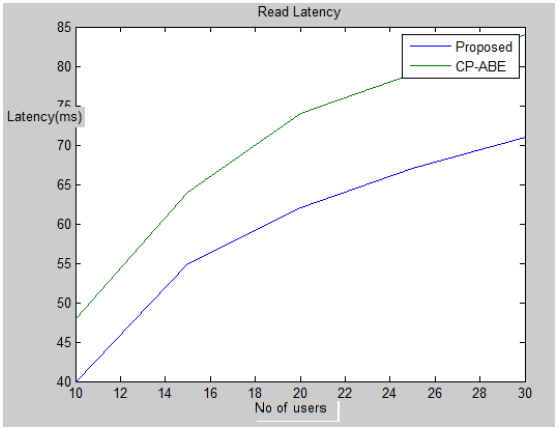
1. Joint Ownership is present
2. Delegation to any number of levels
3. Since the access control list is encrypted, third party cannot infer information about access mode of digital asset

## IV. RESULTS

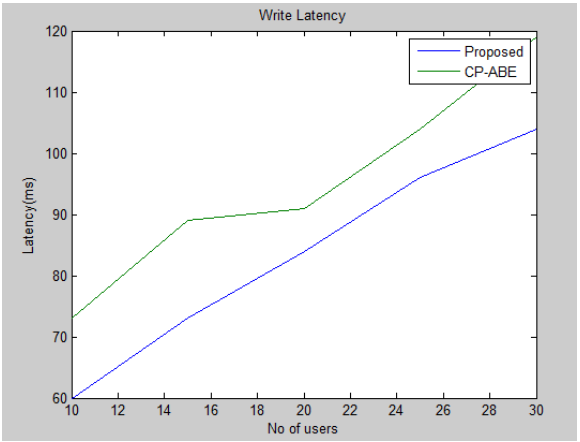
The proposed solution was implemented in real cloud in Microsoft Azure. All the data were stored on a single bucket in the cloud.
We measured following parameters

1. Read Latency
2. Write Latency
3. Share Latency
4. Revocation Latency

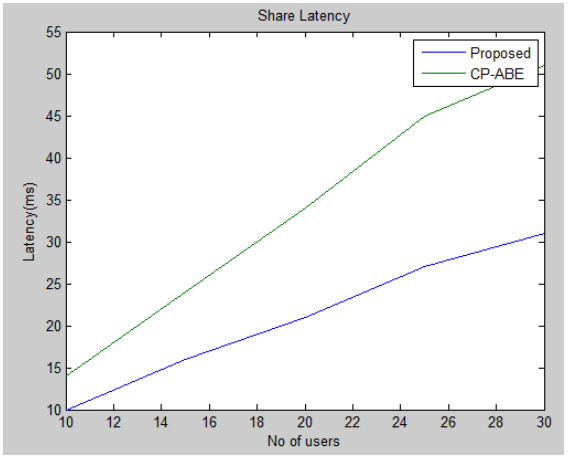
For conducting the performance analysis, uses continuously send requests in different intervals of time and for varies number of users , the performance parameters is a measured and plotted in graph. The performance is compared with CP-ABE.



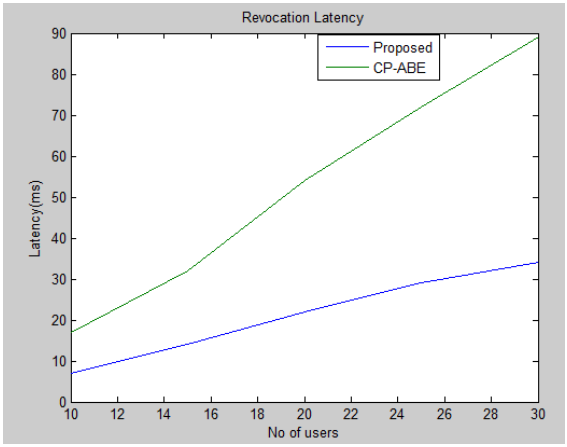

From the graph, we see that read latency is less in our proposed solution compared to CP-ABE.




From the results, we see that write latency in Proposed in less than that of CP-ABE




From the results, we see that share latency is less in the proposed when compared to CP-ABE.




From the results, we see that the revocation latency is less in the proposed solution compared to CP-ABE.

## V. CONCLUSION

The proposed collaborative access control policy allows user to create, modify and share contents. The access control implemented in our solution is integrated as it addresses access control on all operations like read, write, modification and revocation of rights. Through implementation on real cloud Microsoft Azure, we have measured the performance of solution in terms of latency time for gaining control to content and revocation and the result shows that our solution performs better than CP-ABE.

## REFERENCES

[1]. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'2006), pages 89–98. ACM, 30 October - 3 November 2006

[2]. J. Hur and D. K. Noh. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems, 22(7):1214–1221, 2011.

[3]. [12] J. Lai, R. H. Deng, C. Guan, and J. Weng. Attribute-based encryption withverifiableoutsourceddecryption. IEEETransactionsonInformation Forensics and Security, 8(8):1343–1354, 2013.

[4]. K. Yang, X. Jia, and K. Ren. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIACCS'2013), pages 523–528, New York, NY, USA, 2013. ACM.

[5]. S. Yu, C. Wang, K. Ren, and W. Lou.

Attribute based data sharing with attribute revocation. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS'2010), pages 261–270, New York, NY, USA, 2010. ACM.

[6]. J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attributebased encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy(S&P'2007), pages 321–334. IEEE, 20-23 May 2007.

[7]. L. Cheung and C. Newport. Provably secure ciphertext policy ABE. In Proceedings of the 14th ACM Conference on Computer and Communications Security(CCS'2007), pages 456–465. ACM, 28-31 October 2007.

[8]. F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan. CP-ABE with constant-size keys for lightweight devices. IEEE Transactions on Information Forensics and Security, 9(5):763–771, 2014.

[9]. J.Li, G.ZhaoandX.Chen, D.Xie, C.Rong, W.Li, L.Tang, andY.Tang. Fine-grained data access control systems with user accountability in cloud computing. In Proceedings of IEEE Second International Conference on Cloud Computing Technology and Science(CloudCom'2010), pages 89–96. IEEE, 2010.

[10]. R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'2007), pages 195–203, New York, NY, USA, 2007. ACM.

[11]. B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography (PKC'2011), volume 6571 of Lecture Notes in Computer Science, pages 321–334, Berlin, Heidelberg, 2011. Springer-Verlag.

[12]. A. Lewko and B. Waters. New proof methods for attribute-based encryption: Achievingfullsecuritythroughselectivetechniques. InAdvancesin Cryptology-CRYPTO'2012, volume 7417 of Lecture Notes in Computer Science, pages 180–198, Berlin, Heidelberg, 2012. Springer-Verlag..

[13]. M. Chase. Multi-authority attribute based encryption. In Proceedings of the 4th IACR Theory of Cryptography Conference (TCC'2007), volume 4392 of Lecture Notes in Computer Science, pages 515–534. SpringerVerlag, Berlin, 21-32 February 2007.

[14]. H. Lin, Z. Cao, X. Liang, and J. Shao. Secure threshold multi authority attribute based encryption without a central authority. In Proceedings of the 9th International Conference on Cryptology in India (INDOCRYPT'2008), volume 5365 of Lecture Notes in Computer Science, pages 426–436, Berlin, Heidelberg, 2008. Springer-Verlag..

[15]. A. Lewko and B. Waters. Decentralizing attribute-based encryption. In Advances in Cryptology-EUROCRYPT'2011, volume 6632 of Lecture Notes in Computer Science, pages 568–588. Springer Heidelberg, 2011.

[16]. J.Li, Q.Huang, X.Chen, S.S.M.Chow, D.S.Wong, andD.Xie. Multiauthority ciphertext-policy attribute-based encryption with accountability. In Proceedings of the 6th ACM Symposium on Information, Computer.