ENHANCED SECURE DATA SHARING IN DYNAMIC GROUPS

Suresh Kumar RG[1], D.Revathi[2], V.Subha[2]

[1,2,3]Asst. Professor, CSE Department
Rajiv Gandhi College of Engineering and Technology, Puducherry (India)

ABSTRACT

Storing data on remote cloud storage makes the maintenance affordable by data owners. The trustworthiness and reliability of these remote storage locations is the main concern for data owners and cloud service contributor. When multiple data owners are drawn in, the aspects of membership and data sharing need to be addressed. In this paper we proposed efficient multi owner data sharing technique over cloud storage space.The planned scheme provides isolation and complication while handling the data distribution over the cloud. The proposed system works with improved hierarchical attribute-set-based encryption scheme for access control in cloud computing. In this technique, data can be uploaded into the server after the encryption of the content by the secret group key. New contracted users can openly decrypt data files uploaded without contacting with data owners.

***Keywords:* Data Sharing, Access Control, User Revocation.**

I. INTRODUCTION

The cloud computing model allows access to information and computer resources from anywhere through network. Cloud computing is defined as "A collection of abstract, highly scalable, and managed compute infrastructure capable of hosting end - customer applications and billed by consumption." Computing cloud provides computation, software, data access, and storage resources without requiring cloud users to know the location and other details of the computing. End users access cloud based applications through a web browser or a light weight desktop or mobile app while the business software and data are stored on servers at a remote location. Cloud application providers strive to give the same or better service and performance as if the software programs were installed locally on end-user computers [1].

At the foundation of cloud computing is the broader concept of infrastructure convergence (or Converged Infrastructure) and services. This type of data center environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance, and enables IT to more rapidly adjust IT resources (such as servers, storage, and networking) to meet fluctuating and unpredictable business demand.

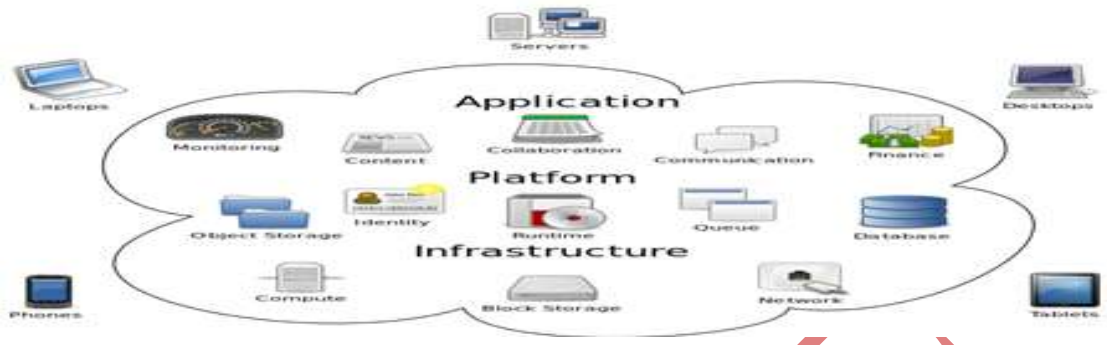


Fig 1.1: Cloud Computing

1.1 Cloud Service Models

Cloud computing providers offer their services according to several fundamental models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower taxonomy model published in 2009, such as Strategy-as-a-Service, Collaboration-as-a-Service, models.

Other key components in anything as a service (XaaS) are described in a comprehensive Business Process-as-a-Service, Database-as-a-Service, etc. In 2012, network as a service (NaaS) and communication as a service (CaaS) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models, recognized service categories of a telecommunication-centric cloud eco system [2].

a) Software as a Service (SaaS)

In this model, a complete application is offered to the user, as a service on demand. A single instance of the service runs on the cloud & services multiple end users. On the customer's side, there is no need for upfront investment in servers or licenses, while for the provider, the costs reduced, since only a single application needs to be hosted & maintained.

b) Platform as a Service (Paas)

Here, a layer of software or development environment is encapsulated & offers a service, upon which other higher levels of service can be built. The customer has the freedom to build their own applications that run on the provider's infrastructure.

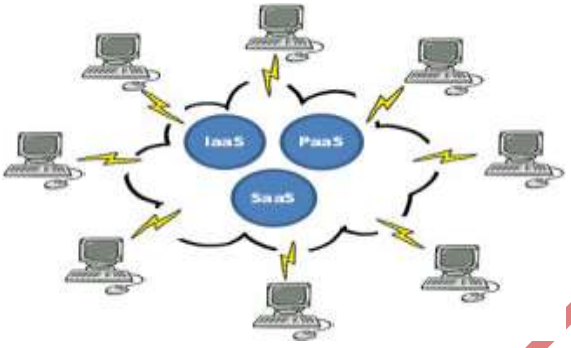
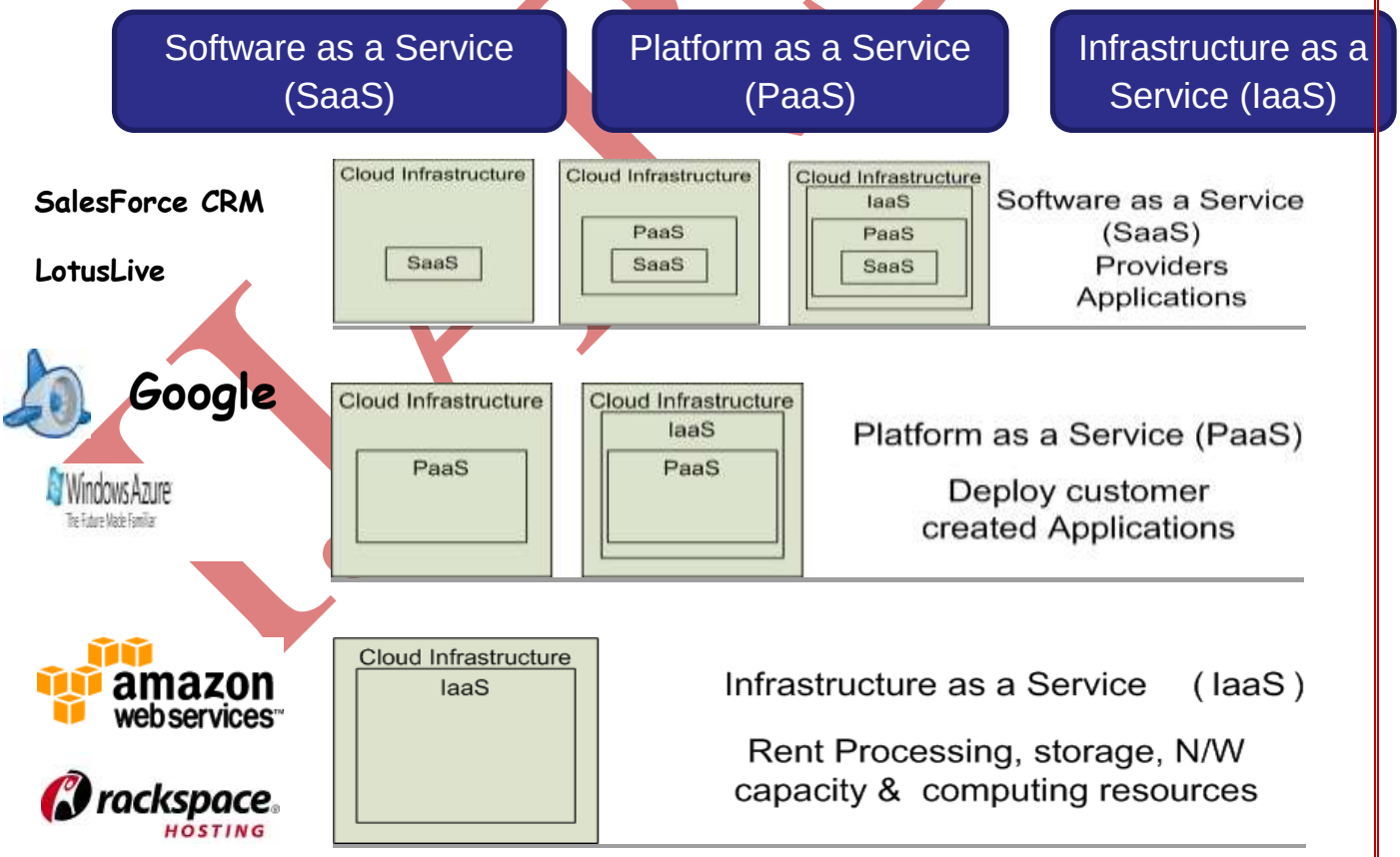


Fig 1.2: Cloud Service Model

c) Infrastructure as a Service (Iaas)

IaaS provides basic storage and computing capabilities as standardized services over the network. Storage systems, servers, networking equipment, data centre space are pooled and made available to handle workloads. The customer would typically deploy their own software on the infrastructure.



1.2 Deployment of Cloud Services

Cloud services are typically made available through a private cloud, community cloud and hybrid cloud. The services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider [2].

a) COMMUNITY CLOUD

The cloud infrastructure is shared among a number of organizations with similar interests and requirements, which limit the capital expenditure costs. The operation may be in-house or with a third party on the premises.

b) PUBLIC CLOUD

The cloud infrastructure is available to the public on a commercial basis by a cloud service provider, which enables a consumer to develop and deploy services in the cloud.

c) HYBRID CLOUD

The Hybrid Cloud is mixture of public and private cloud. Conversely, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

II.RELATED WORKS

Data access: The fine-grained data access control is achieved through KPABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption [6].

Privacy preserving: privacy-preserving public auditing system for data storage security in Cloud Computing is achieved by utilizing the homomorphic linear authenticator and random masking. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files.

Secure Provenance: A concrete secure provenance is provided by SP scheme based on the bilinear pairings, and the provable security technique to prove its security in the standard model. SP scheme provides trusted evidences for data forensics in cloud computing and thus pushes the cloud computing for wide acceptance to the public.

III. PROBLEM STATEMENT

3.1 Exitising System

To preserve data privacy, a basic solution is to encrypt data files, and upload the encrypted data into the cloud. The data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, the unauthorized users as well as storage servers cannot learn the content of the data files

because they have no knowledge of the decryption keys. Conversely, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. The major issues in existing system is only the group manager can store and modify data in the cloud The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.

3.2 Proposed System

We propose a secure multi-owner data sharing scheme, which implies that any user in the group can securely share data with others by the untrusted cloud. The scheme is able to support dynamic groups efficiently. Specially, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be achieved through a novel revocation list without updating the secret keys of the other users. The encryption size and computation overhead are constant and independent with the number of revoked users .We provide secured privacy-preserving access control to users, by guarantying any member in a group to anonymously utilize the cloud resource. Moreover, when disputes occur, the real identities of data owners can be revealed by the group manager.

IV. CONCLUSION

In this paper we achieve a secure data sharing and authenticated data for dynamic groups in an untrusted cloud. The scheme, a user is able to share data with others in the group without revealing identity privacy to the cloud. More specifically, efficient user revocation can be achieved through a public revocation list without updating the private keys, and the new users can directly decrypt files stored in the cloud before their participation. Moreover, the encryption computation and storage overhead cost are constant.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, “A View of Cloud Computing,” Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[3] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[4] D. Boneh, X. Boyen, and E. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” Proc. Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[5] D. Chaum and E. van Heyst, “Group Signatures,” Proc. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[6] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[7] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[9] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[11] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.