International Journal of Science Engineering and Advance Technology

# Dynamic Access Control In Cloud Computing Using Encryption/Decryption

**Ravindra R #1, S Krishna Chaitanya R #2**
#1Student of M.Tech (CSE) and Department of Computer Science Engineering,
#2 Asst.Prof, Department of Computer Science and Engineering, Sir C R Reddy College of Engineering, Eluru, W.G.DIST

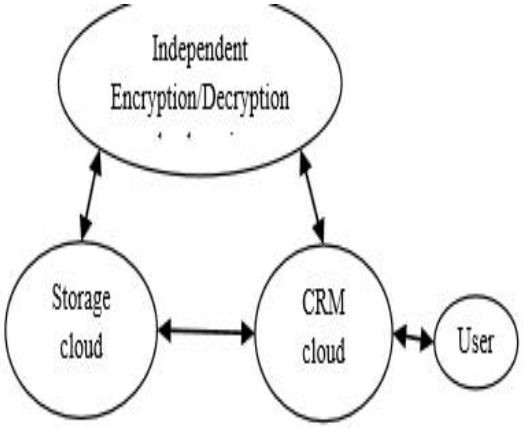
ABSTRACT: Cloud computing has emerged as one of the most important paradigms in the IT industry for last few years. In general data owners and service providers are not in the same trusted domain in cloud computing. Service providers should not be a trusted one anyhow they are all third party. The system focuses on a novel technique to Hierarchical Attribute Set Based Encryption (HASBE); it is driven by the Cipher Policy attribute based encryption (CPABE) with a hierarchic al structure of cloud users. Cloud computing is known as "Utility". Cloud Computing enabling users to remotely store their data in a server and provide services on demand. Since this new computing technology requires user to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. We can increase security on access of the data in the cloud. Morever we can provide encryption on the data so third party can not use the data. In this paper we will be reviewing various encryption based access control model for enhancing cloud security along with their limitations. We will be concluding with a proposed access control model to enhance cloud security. The proposed work focuses CRM (Customer Relationship Management) for business model that is driven by the category of Software as a Service (Saas) method in cloud. Using this scheme it achieves the flexible, scalable and fine grained access control of data. It also achieves high secure and effective user revocation in cloud environment.

Key Words :Cloud Computing, Access Control , Security Encryption, Encryption Techniques.

**I.Introduction:**

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, service oriented architecture, and utility computing. The advantages of cloud computing comprise decreased costs and capital expenses, scalability, increased operational, immediate time to promote,
flexibility, and so on. Different service oriented cloud computing models have been designed, Platform as a Service (PaaS), including Infrastructure as a Service (IaaS), and Software as a Service (SaaS). Frequent commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2, Amazon's S3, and IBM's Blue Cloud are IaaS systems, while Google App Engine and Yahoo Pig are representative PaaS systems, and Google's Apps and Sales force's Customer Relation Management (CRM) System be owned by SaaS systems. The cloud service supplier directs a cloud to offer data storage s
ervice. Data owners encrypt their statistics files and store them in the cloud for sharing with data customers. To contact the shared data files, data customers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is managed by a domain influence. A domain authority is directed by its parent domain authority or the believed authority. Data owners, domain authorities, data consumers, and the conditioned authority are prearranged in a hierarchical way . The confidences authority is the root authority and responsible for organization top-level domain authorities. Data owners/consumers may communicate to employees in an organization. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain. In our system, neither data owners nor data customers will be forever online. They arrive online only when essential, whereas the cloud service provider, the confidences authority, and domain authorities are always online. The cloud is unspecified to have plentiful storage capacity and computation power. Additionally, we suppose that data customers can right of entry data files for reading only.This paper deals with a novel business model for cloud computing supported on a separate encryption and decryption service in Fig.1. In this business model, Encryption/Decryption as a Service and Storage as a Service (SaaS) are not provided by a single operator. In Addition , the SaaS provider may not
store unencrypted. user data. Once the provider of Encryption /Decryption as a Service has completed, encrypting user data supplied it off to an application (e.g. a CRM system). The encryption/decryption system must delete all encrypted and decrypted user data. The observation of separating authority is often applied in business management. For example, responsibility for a company's finances is divided between the accountant and cashier. In business processes, the

accountant is responsible for keeping accounts, while the cashieris in charge for making payments. By keeping these two functions divide, the company can prevent the accountant from misrepresenting accounts and embezzling corporate finances. Authorized documents frequently need to be stamped with two seals (i.e., the corporate seal and the legal representative's seal), thus avoiding a staff member from abusing his position to issue fake documents, and these seals are normally delegated to two dissimilar people. These examples of the division of authority are designed to avoid a concentration of power which could raise operational risks.In a cloud computing environment, the user usually uses cloud services with exact purposes, e.g., Salesforce.com's CRM service, SAP's ERP services, etc. Data generated while using these ervices is then stored on storage facilities on the cloud service. This work highlights the addition of an independent encryption/decryption cloud service. This type of business model, with the result that two service providers split responsibility for data storage and data encryption/decrypt ion. Fig 1illustrates the concept of our proposed business model. It presents an example in which the user utilizes separate cloud services for CRM, storage and encryption/decryption. According to the user's needs, CRM Cloud Services could be transferred for other function specific application services (e.g., ERP Cloud Services, Account Software Cloud Services, Investment Portfolio Selection and Financial Operations Cloud Services).




**Related Work:**

From the internet through web based tools and applications, a model by which information technology services being delivered and resources are retrieved, rather than direct connection to a server where the Data and software packages are amassed in servers. To achieve flexible scalable and fine grained access control, a number of schemes to be used. In [1] survey on several schemes such as Ciphertext Policy Attribute Based Encryption, Key Policy Attribute Based Encryption, Ciphertext Policy Attribute Set Based Encryption, Hierarchical Identity Based Encryption, Fuzzy Identity Based Encryption, Hierarchical Attribute Based Encryption and Hierarchical Attribute Set Based Encryption for access control of out sourced data are conversed. In [2] presented a survey on various encryption methods that gives ecurity, scalable and flexible fine grained access control. As the data is divided over the network, it is required to be encrypted.

Distribution of data signifies the data should be protected and proper access control should be maintained. There are many encryption systems that offer security and access control in clouds that ensure that authorized users access the data and the system.

**II. Proposed System**

The proposed scheme HASBE on security features in implementing access control for cloud computing.[13]

**A. Scalability:**

We extend ASBE with a hierarchical structure to effectively delegate the trusted authority's private attribute key generation operation to lower level domain authorities. By doing so, the workload of the trusted root authority is shifted to lower level domain authorities, which can rovide attribute key generations for end users. Thus, this hierarchical tructure achieves great scalability. Only has one authority to deal with key generation, which is not scalable for large scale cloud computing applications.

**B. Flexibility:**

HASBE organizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. So HASBE can support compound attributes and multiple numerical assignments for a given attribute conveniently.

C. Fine grained access control:

Based on HASBE, our scheme can easily achieve fine grained access control. A data owner can define and enforce expressive and flexible access policy for data files as the scheme.

D. Efficient User Revocation:

To deal with user revocation in cloud computing, we add an attribute to each user's key and employ multiple value assignments for this at tribute. So we can update user's key by simply adding a new expiration value to the existing key.

**Conclusion**

The existing system provides the cloud service provider to facilitate

both encryption and decryption service and storage service as a single unit. In order to enhance the encryption and decryption standards and storage services, it's required to separate encryption and decryption standard and storage services as separate unit. To address this, a business model for cloud computing need to the introduced so as to

increase the service performance of both the units. The proposed system handles this business model and the performance of separate encryption and decryption service and storage service is enhanced. In future HASBE scheme can be extended to sustain any depth of the key structure also system can be improved during new algorithms and techniques.

**References**

[1]K.Priyadarsini, C.Thirumalai selvan,"A Survey on Encryption Schemes for Data Sharing in Cloud Computing", (IJCSITS), ISSN: 2249-9555,Vol. 2, No.5, October 2012.

[2]Neena Antony, A. Alfred Raja Melvin,"ASurvey on Encryption Schemes in the Clouds for Access Control",International Journal of Computer Science and ManagementResearch Vol 1 Issue 5 December 2012
.
[3]Abdul Raouf Khan,"Access Control in Cloud Computing Environment", ARPN Journal of Engineering and Applied Sciences, Vol. 7, No. 5, May 2012 Issn 1819-6608.

[4]Yan Zhu, Hongxin Huy, GailJoon Ahny, Dijiang Huangy, and Shanbiao Wang," TowardsTemporal Access Control in Cloud Computing",INFOCOM 2012
.
[5]Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou," AchievingSecure, Scalable, and Fine -grained Data Access Control in Cloud Computing",INFOCOM10.

[6]Guojun Wang, Qin Liu, Jie Wub, Minyi Guo,"Hierarchical attributebased encryption and scalable user revocation for sharing data in cloud servers",Jul 1, 2011.

[7]Miss. Rehana Begum, Mr. R.Naveen Kumar, Mr. Vorem Kishore,"Data Confidentiality Scalability and Accountability (DCSA) in Cloud Computing ", Volume 2, Issue 11, November 2012.

[8]Chittaranjan Hota, Sunil Sanka,"Capabilitybased Cryptographic Data Access Control in Cloud Computing",Int. J. Advanced Networking and Applications, Volume: 03; Issue: 03; Pages: 11521161 (2011)
.
[9]V.Suma,K.Vijay Kuma,"An Efficient Scheme For Cloud Services Based On Access Policies",International Journal of Engineering Research & Technology (IJERT),Vol. 1 Issue 8, October –2012,ISSN: 2278-0181
.
[10]R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[11]R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.

[12]R.Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.

[13]L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

[14]Salesforce.com, Inc., "Force.com platform," Retrieved Dec. 2009, from http://www.salesforce.com/tw/
.
[15]SAP AG., "SAP services: maximize your success," Retrieved Jan. 2010, from http://www.sap.com/services/index.epx.
.
[16]D. Benslimane, S. Dustdar, and A. Sheth, "Services mashups: the new generation of web applications". IEEE Internet Computing, vol. 12, no. 5, pp. 13–15, 2008.