*International Journal For Technological Research In Engineering*
*Volume 3, Issue 8, April-2016* *ISSN (Online): 2347 - 4718*

# SURVEY ON SECURE DATA ACCESS CONTROL SCHEMES IN CLOUD COMPUTING

S. Rohith[1], Sr. Asst. Prof. Mylara Reddy C[2]
[1]M.Tech, [2]Faculty, Department of Computer Science Engineering, REVA ITM, Bangalore, India.

***Abstract: Today the presence of cloud computing technology has become essential for many organizations, businesses enterprises and personal usage for sharing resources, flexible data storage, reduced maintenance cost, anytime anywhere access and availability of applications and many more. Managing and maintaining data has become a tedious operation for the data owners. Hence data owners prefer to outsource their data to cloud. Despite of having many benefits, issues related to data security, data privacy and data control are haunting the data owners. Access control mechanism provides the data owner to control and regulate access of data users which achieves the goal of safeguarding data or sensitive information. Access control method is the ultimate way to ensure access to authorized data users only and have complete control over the data. This paper reviews different secure data access control methodologies and study the functionality of the schemes that helps to build a secure, scalable, flexible, efficient and dynamic data access control standard in cloud computing.***

***Keywords: Cloud computing, Access Control;***

## I. INTRODUCTION

Cloud computing is popularly known as on-demand computing that functions on the idea of distributed computing. The cloud technology utilizes service oriented architecture and virtualization concept. The large scale computing allows processing of shared resources and data to multiple systems connected through internet on demand basis. Cloud computing represents a platform that generates ubiquitous, reliable, on-demand network access to a shared pool of configurable, flexible and large scale computing resources. In today's scenario, Cloud computing has reformed into a paradigm which delivers computing services through internet. Few attractive features of cloud computing are availability of shared resources, flexible data storage, low maintenance cost, disaster recovery management, pay as you use, etc. The agenda of cloud computing technology is to deliver CPU, storage, network bandwidth and virtually unlimited scalability at low cost. Access control is a mechanism designed and developed to function as a gateway for controlling and regulating user entry into the system. Access control performs operations of permission, rejection and restriction of user access. It decides authority for user access to systems, information, resources and applications. It also monitors and records each and every entry from authorized users and trusted members to their respective dedicated resources leading to securing sensitive and confidential information. By this means, Access control models allow the data owner or administrator to delineate user access rights. To achieve fine-grained secure access control of data, security techniques, protocols and algorithms are utilized. By using Encryption techniques, the encrypted data can be kept confidential regardless the storage server is un-trusty. The first access control model proposed was Lampson's access matrix in 1960. Later on various prominent successful access control models were introduced namely Discretionary Access Control [DAC], Mandatory Access Control [MAC], Role Based Access Control [RBAC] and Attribute Based Access Control [ABAC]. The DAC scheme allows access to users based on identity and specified authorization. This means data created by users are authorized to permit or deny access to other users. However, as the size of network and number of users increase depending on the distribution of data across numerous servers, DAC fails to achieve the requirement. In MAC, each user is assigned individual security level. Access is granted based on matching of predefined relationship criteria in the security level. However, MAC fails to achieve practical requirements in commercial enterprises. The RBAC model functions on the principles of user roles and access permission is encapsulated in role which is assigned to users. Access is permitted according to the roles and activities performed by the user. A role may vary for each individual user. However, RBAC is not feasible in large user groups because of similar type of access. The ABAC model includes user attributes like location, time, department, qualification, etc. It is more flexible, secure, fine grained, scalable and hierarchical compared to DAC, MAC and RBAC. ABAC overcomes the problems encountered by RBAC. The former access control models fails to provide dynamic complex security policies as they face the challenge of network size and number of users increase. To overcome these drawbacks, Attribute based encryption [ABE] was introduced [3]. ABE is a public key cryptographic technique that operates in one to-many communications. It also referred as Fuzzy encryption. ABE resolves the problem of public key encryption by reduction of communication overhead of internet. ABE utilizes set of attributes to encrypt and decrypt data. The ciphertexts are embedded with set of attributes and their respective private keys are designed based on a predefined access structure. The ciphertext is decrypted only if set of user key attributes and ciphertext attributes match. Hence fine grained sharing of encrypted data is achieved. ABE scheme is further classified into Key Policy-Attribute Based Encryption and Ciphertext Policy-Attribute Based Encryption.

  

## II. RELATED WORK

This section of paper describes different techniques and schemes proposed to achieve secure data access control in cloud computing. Butler W. Lampson [1] defined a protection state which is represented by access matrix. The access matrix contains set of subjects, set of objects, set of operations and a function. The function determines type of operation the subject performs on the object. A. Sahai et al [2] have constructed a fuzzy Identity Based Encryption scheme that enables data encryption combined with biometric measurements as identities and some amount of noise in each measurement. The distance metric used for measurement between identities is named as Hamming distance. There exists a challenge to generate strong cryptographic keys from biometric inputs due to rapid variation in every measurement of biometric values. Goyel et al [3] have proposed Key Policy-Attribute Based Encryption [KP-ABE] scheme that includes set of attributes describing encrypted data and generates access policy based on user's private key. The access control of encrypted data is completely dependent on private key. Decryption is possible only if access structure in user's private key matches the attributes of encrypted data. However, there is no option for encrypted data to choose who should decrypt and who should not. Bethencourt et al [4] have proposed Ciphertext Policy-Attribute Based Encryption [CT-ABE] scheme that is just inverse of KP-ABE scheme. This scheme implements encryption that specifies monotonic access structure. The encrypted data holds the threshold access structure from user selected predefined attributes during the encryption of data. The access structure is designed in a format that only those users whose attributes satisfy the access structure can be allowed to decrypt the encrypted data. This scheme also overcomes the possibility of KP-ABE scheme where the encrypted data chooses who can decrypt. However, the scheme has limitations like decryption key is valid for only logically organized user attributes and lacks in providing complete flexibility and efficiency in access control. G. Wang et al [5] have proposed Hierarchical Attribute-Based Encryption [HABE] scheme that is a combination of Hierarchical Identity-Based Encryption [HIBE] system and Ciphertext-Policy Attribute-Based Encryption [CP-ABE] system. The scheme provisions fine grained access control with full delegation, high performance and scalability. Aware of the problem, when users are not authorized to access the encrypted data, a scalable revocation scheme using Proxy Re-Encryption [PRE] and Lazy Re-Encryption [LRE] together with HABE scheme is applied in efficient revocation of access rights from users. However, HABE scheme defines its limitations in deficit support of compound attributes and multiple value assignments. Jin Li et al [6] have presented a secure fine-grained access control technique called outsourced attribute based access control which uses two entities, Key generation-cloud service provider [KG-CSP] and Decryption-cloud service provider [D-CSP]. The KG-CSP entity performs the delegated outsourced task of key issuing by attribute authority. The D-CSP performs the task of partial decryption on the ciphertext. This technique achieves efficient key-issuing and decryption without leakage of private information.

## III. CONCLUSION

In this paper, we have briefed introduction about cloud computing technology in current scenario. Later we review the functionality and drawbacks of different secure data access control schemes proposed by others. By reviewing the existing data access control methods, we study the real time requirements and challenges in construction of a secure, scalable, reliable, flexible, efficient and dynamic data access control scheme in cloud computing.

## REFERENCES

[1] Lampson, B. W., "Protection", in Proc. Fifth Princeton Symposium on Information Sciences and Systems, Princeton University, March 1971, pp. 437-443, reprinted in Operating Systems Review, 8,1, January 1974, pp. 18 - 24.

[2] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption In Advances in Cryptography", 2005.

[3] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", in Proc of CSS'06, 2006.

[4] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption", in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[5] G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, pp. 320-331, 2010.

[6] Jin Li, Xiaofeng Chen, Jingwei Li, Chungfu Jia, Jianfeng Ma, Wenjing Lou, " Fine-Grained Access Control System based on Outsourced Attribute-based Encryption", 2013.

  