A SURVEY OVER VARIOUS ACCESS CONTROL AND AUTHENTICATION TECHNIQUES IN CLOUD COMPUTING

Priya Gour, Bhupchandra kumhar, Akshay Varkale
IES College of Technology, RGPV University Bhopal.

Abstract: In cloud computing data resides in cloud server, that data contains private and confidential data of the user. Thus security of that is the major task in cloud computing. There are various techniques are presented by different researchers to provide a secure access for that data. A review over the various techniques which used to provide security for that data is presented. Role based Access control technique is generally used, but that technique required some enhancementto provide a secure and enhanced framework to access data in cloud server.

Keywords: - Cloud Computing, Role Based Access Control (RBAC), Cloud server.

Introduction

Cloud computing is framework which provide on-demand resource and application for the user. Cloud computing offers on demand services to the user such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS). Thus it gains huge popularity for cloud computing. But security for that data is major issue in cloud computing, securityframework which provides an on-demand security architecture for cloud computing is required. For a RBAC (Role Based Access Control) mechanism is presented in [1]. That defines role for the members in the cloud, only administrator can access all the data.

There are various techniques which used to provide a secure access for the user's data and preserve the integrity of the data. There are techniques like Role Based Access Control (RBAC) are used to provide access for the user's data. In that a role for the user is defined to provide access for the data. In that different authentication mechanism are used to define the roles of the user. A RBAC technique is presented in the Figure 1.1. Attribute Based Access Control (ABAC) mechanism also used for the technique. In that properties of the user are used to provide an access control mechanism in that a subject and object's attribute are used to define different access levels for the user on the basis of that an access control mechanism is provided to the user. A description for the ABAC is presented in the Figure 1.2.

In Figure 1.1, a Role based access control mechanism is presented which shows that there is different roles are assigned to the members in the cloud.

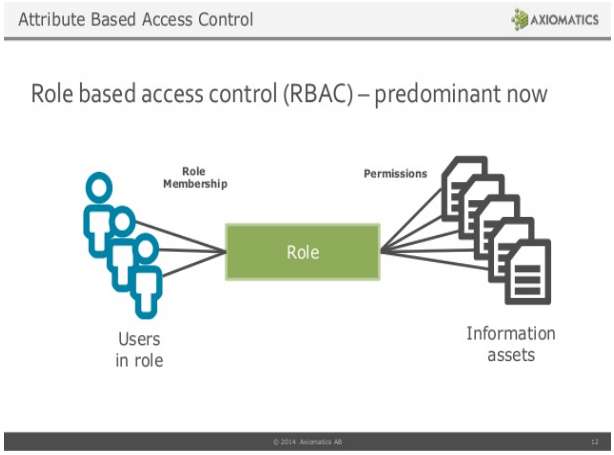

Figure 1.1:- Role Based Access Control.

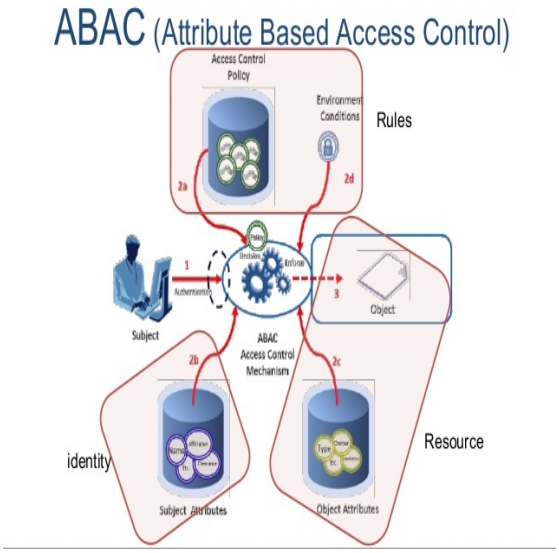

Figure 1.2:- Attribute Based access Control

Generally there are three types of models [13] are used called 1) Discretionary Model, 2) Mandatory Model, 3) Role Based Model. In discretionary model owner of the data object decides the access permission for the other users. In that owner of the object decides that what access permission the other user have. Mandatory Model, in that model access permission decided by the administrator not by the owner of the objects. That provides enhanced functionality for enhanced control in distributed computing scenario. In role based technique different role for the users are assign to provide access to the data.

In [2] a hybrid technique is presented which uses attribute based encryption with probability re-encryption and lazy re-encryption to provide an enhanced framework to encrypt data and store it in the cloud also resolve the issues in attribute based encryption like performance degradation in user re-invocation and some others. In figure an Attribute based access control mechanism is presented.

Further this paper organizes as follows:-

II Literature Review, a review over the various techniques which used for access control mechanism in cloud computing is presented in this section, III. Conclusion .

Literature Review

Lan Zhou, VijayVaradharajan[1] presents a cryptographic role based access control (RBAC) to provide secure access to the data and allow only authorized user to access that data. In that a RBAC scheme is used to provide access control for the data in an unstructured environment, in that scheme only authorized users are allowed to access that data. In RBAC owner user and role based model is used, in that model owner is the entity which owns the data and store that

data in the cloud server, user is the entity who want to access that data and role is the entity which provide association between user and the owner. In that way a trusted cryptographic mechanism is provided to store data.

V.Sathya Preiya, R.Pavithra, Dr. Joshi [2] presented a hybrid technique which uses the properties of the three cryptographic techniques called KP-ABE (Key Policy Attribute-Based Encryption), PRE (Proxy Re-encryption), Lazy Re-encryption. In that technique, each data file associated with the attribute and an access structure is provided to the user which is based on these attributes. KP-ABE encryption technique is used to provide key to form that access structure that enables a fine grained access structure. But this technique alone generates system overhead and not able to provide an efficient mechanism. To resolve such issues PRE (proxy re-encryption) technique is used to allow user re- encrypt data while user invocation. In that way a fine grained access policy mechanism is provided.

Mali Varsha, Pramod Patil[3] presents a cryptographic role- based access control (RBAC) technique, to ensure the privacy of the user over in the cloud storage. In RBAC a role based access control mechanism is used, in that administrator take care all the access control tasks and then for each member in the cloud a role is defined to access the server, such that each member has their own access levels. In that way a new flexible access control mechanism is provided.

Punya Peethambaran, Jayasudha J. S. [4] presents a fine grained access control mechanism which also provides a traitor tracing technique. In existing techniques an attribute based encryption techniques are used but these techniques generates computation overhead and lacking in the mechanism to trace traitors. To reduce these defects a new technique which provide a mechanism to key management and tracing traitor in the process is presented. In existing techniques equality based oblivious commitment based envelope (EQ-OCBE) is used which not efficient to manage multiple equality thus a Fast Access control vector broadcast group key management protocol is presented. in existing techniques a no efficient mechanism for tracing traitor is presented but in that technique audit logs is performed which restrict traitors to access users data.

Pooja R. Vyawhare, Namrata D. Ghuse [5] presents a new technique for the secure mechanism to secure storage in the cloud. In cloud computing user data resides in the cloud server, thus security of that data is the biggest concern in cloud computing. There are various techniques are proposed by the different researchers. In that paper a new technique is presented which provide resistance to the various type of the attacks like replay attack or some other attacks? This technique uses a decentralized mechanism to deal with such problems. In that technique four phases are there called setup, encryption, key generation and decryption. Thus that technique provides a secure way to share data.

Sowmiya Murthy [6] presents digital signature based scheme for the secure cloud storage to provide authentication for the user in a decentralize cloud scenario. Provide key management for the multiple key distribution centers. In that homomorphic encryption with a paillier encryption is used to provide encryption for the data for cloud storage. In that technique key distribution centers are used to provide a decentralized cloud structure, role based access control is used to provide access control mechanism, a digital signature based technique is used to provide anonymous authentication for the user. Then an enhanced access policies is provided to access the data.

Yu Jin, ChuanTian, Heng He, Fan Wang [7] a secure access control mechanism for the outsourced data in cloud is presented. In mobile cloud computing data resides at cloud server, thus that data is vulnerable to unauthorized access. CP-ABE based encryption scheme is presented which provides an enhanced mechanism to deal with such issues. It provides a cost effective and reduce computation overhead for encryption and decryption. A flexible data access policy to the user to provide an access for the data. SL-CP-ABE scheme is presented which reduce the encryption and decryption time of the process and a simple tree based structure is used to provide a flexible mechanism to the user that way that technique provides an efficient way to deal security related issues in cloud computing.

Mohammad Ahmadi, Mohammad Eslami [8] a survey over the various security and access control issues in cloud computing is presented. In that first a description over the services provided in the cloud computing and mechanism that used to store data in cloud server is presented, there are various issues presented in cloud, but security is the biggest concern in cloud computing. User's data resides in cloud server which is vulnerable to various types of threats thus a secure mechanism is required to provide security for that data. There is an access control mechanism is presented to provide access to the various user to access that data.

Punya Peethambaran1 and Dr. Jayasudha J. S [9] a key management, secret key sharing scheme and a traitor tracing scheme is presented. Generally attribute based encryption technique is used to provide a fine grained access control scheme to the user. In that technique, four entities called user, owner, cloud and identity provider are considered to design a mechanism to deal with various issues in cloud computing. An oblivious commitment based scheme (OCBE) and BGKM (Border Gateway Key Management) based technique is used to provide a flexible and easy mechanism to provide access control to the user.

Prachi Shah [10] a role based access control mechanism is presented. In that mechanism different user having different roles in the cloud. Like an administrator can have the access to all the data and can work as a controller to control the whole process of access mechanism. Owner of the data can access the file and restrict the unauthorized access for the data. A role based encryption technique is used to provide access to the data. I that way an access control

mechanism is provided to provide a secure success to the data.

Technique	Advantage	Disadvantage
ABAC (Attribute Based Access Control) [1]	It provide functionality to assign rum time access control for the user. It provide flexibility to set the rule for adding and removing attribute for the access control mechanism.	The auditing process provided by that technique is not efficient. It degrades in performance when performing auditing in large scale data.
TRBAC (Temporal-Role Based Access Control) [13]	In that technique role are assigned at runtime,that provide dynamic role assigning functionality.	But in some application Static roles are also required, thus that technique degrades performance in assigning roles.
GTRBAC (Generalized Temporal Role Based Access Control) [13]	Static and dynamic role assigning mechanism for the users. In that maximum duration allowed to the user and maximum no of roles in a certain time interval.	That technique does not provides any trust mechanism and context aware access control for the services thus techniques does not provide better solution for the cloud scenario.
RC-ABAC (Role centric Attribute based access control)	A enhanced functionality to assign roles for the various users is provide. It provides flexible, fine grained, and dynamic access control mechanism.	It has a Complex setup mechanism which degrades the performance of the whole technique.

Table 1- Comparison Analysis of different access control approach

The table 1, above demonstrate how the access control mechanism differentiate in themselves for operations.

Conclusion

In cloud computing user's data stored in cloud server, security of that data is the biggest concern in cloud computing. A secure access and authentication mechanism is required to preserve security of that data while accessing that data. a review over the

various techniques, used to provide access control and authentication in cloud computing is presented in this paper. For future work a new technique which resolves issues of authentication access control in cloud computing can be evolved to provide an enhanced security mechanism.

REFERENCES

[1] Lan Zhou,Vijay Varadharajan,and Michael Hitchens "Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage" IEEE, 2015.

[2] V.Sathya Preiya, R.Pavithra, Dr. Joshi "Secure Role based Data Access Control in Cloud Computing" IJCTT, 2011.

[3] Mali Varsha, Pramod Patil "A Survey on Authentication and AccessControl for Cloud Computing using RBDACMechanism" IJIRCCE, 2015.

[4] Punya Peethambaran, Jayasudha J. S. "Cloud Based Access Control Model For Selective Encryption Of Documents With Traitor Detection" IJNSA, 2014.

[5] Pooja R. Vyawhare, Prof.Namrata D. Ghuse "User Anonymous Authentication Scheme for Decentralized Access Control in Clouds" IJCSIT, 2015.

[6] Sowmiya Murthy "Cryptographic Secure Cloud Storage Model With Anonymous Authentication And Automatic File Recovery" ICTACT, 2014.

[7] Yu Jin, ChuanTian, Heng He, Fan Wang "A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing"IEEE, 2015.

[8] Mohammad Ahmadi, Mohammad Eslami, Mohammad JavadGolkar "Access Control in Cloud and User Authentication Computing Environment on Concernsents" IEEE, 2015.

[9] Punya Peethambaran1 and Dr. Jayasudha J. S. "CLOUD BASED ACCESS CONTROL MODEL FOR SELECTIVE ENCRYPTION OF DOCUMENTS WITH TRAITOR DETECTION" IJNSA, 2014.

[10] Prachi Shah " Data Security for Cloud Storage System Using Role Based Access Control"IJSR 2013.

[11] Zheng Yan, Xueyun Li, Mingjun Wang and Athanasios V. Vasilakos "Flexible Data Access Control based on Trust and Reputation in Cloud Computing" IEEE, 2015.

[12] Natarajan Meghanathan "Review Of Access Control Models For Cloud Computing" CS & IT-CSCP 2013.

[13] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data," Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89-98, 2006.