ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

An Attribute based Access Control and it's Application on Cloud based Information Systems – a Survey

Krupali Patel[1], Vishal Shah[2]

M.E. Student, Dept. of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India[1]

Assistant Professor, Dept. of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India[2]

ABSTRACT: An Attribute-based access control (ABAC), a relatively new authorization approach has gained an immense attention of researchers. The benefits offered by ABAC can be used to control un-authorized access to the data stored in a dynamic environment while supporting the essential features of the current storage platforms such as scalability, flexibility, diverse type of users and heterogeneity. In this paper, we have analyzed the current systems using ABAC as an authorization approach, the benefits offered by ABAC over a distributed, heterogeneous, cross-platform environment and usefulness of ABAC Cloud storage.

KEYWORDS: ABAC, Access Control, Authorization, Cloud computing.

I. INTRODUCTION

There are many authorization systems which, primarily based only on the identity of the user requesting for the execution of an operation. Examples include DAC, RBAC and IBAC in which access to an object has been granted to a particular identity or role of user. These Authorization systems do not support flexibility, maintainability and expressiveness of access control requirements for current dynamic storage applications.

Cloud IAAS provides data outsourcing capability to the users but security and privacy is a key concern due to vulnerability of Cloud platforms. ABAC is an authorization model which uses attributes of involved entities such as subjects (users), objects (resources) and environmental/contextual variables relevant to request for granting privileges to subject. In ABAC, Access control policies are used for expressing authorization requirements which contains access rules, based on attributes of involved entities. Use of attributes enables more precise and expressive representation of access control requirements and administrator can define numerous policies using these attributes. This flexibility allows creation of access rules without specifying individual relationship between each subject and object [1]. In ABAC, access decision can be changed between access requests simply by altering attribute values defining the underlying rule sets; this provides more dynamic access control and limits long-term maintanance requirements [1].

This paper is organized as follows: section II explains survey of various extensions of ABAC, section III presents a comparison of work done in all the papers which have been analysed. Finally, section V concludes the paper.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

II. RELATED WORK

There are many access control systems based on an ABAC in dynamic, distributed and heterogeneous, we will take a closer look at those systems.

Marc Huffmeyer et al [2] propose an access control language for RESTful services. The popular standard called XACML [8] is used to implement access control system. The basic architecture used by their system is inspired by the the XACML architecture and is modified according to the operations of REST which is as shown in figure 1.

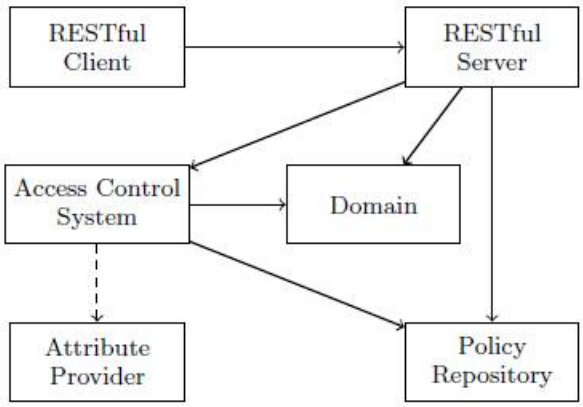

Figure 1: RESTAcl access control architecture [2].

A standardized RESTful client (browser) sends a resource request to a RESTful server; this request is then forwarded to the access control system. The access control system determines the access decision depending upon the attributes of user, resource structure (domain) representation and policies. The Access control system identifies the policies that needs to be evaluated and loads them from policy repository and might request additional attributes from attribute provider. The access decision is returned to RESTful server and it is responsible for enforcing this decision to the access request. The Resource-Policy-mapping is maintained at RESTful server and at any time if a user wants to change or add policies, only mapping needs to be changed. In this way separation of duty and flexibility is enabled in a system.

Algorithms Used:

Mapping algorithm: An algorithm is needed to identify the policies associated with a resource of the RESTful application; for this, hashing is used for mapping between resource and policies.

Evaluation algorithm: An efficient algorithm is required to calculate the decision that depends on the given attributes and applicable policies identified by the mapping algorithm. The algorithm iterates over a prioritized list of policies and checks whether the collection of attributes A is applicable. If the policy is applicable, the algorithm returns the effect of the policy (deny/permit) otherwise it proceeds with the next highest prioritized policy.

Cheng Man Ma et al [3] propose a system which uses ABAC for controlling access to the information shared over collaborative social networks. Large number of people share photos, status, events, activities etc. over the network, thus creating large amount of data which requires an efficient access control mechanism. Information shared over social networks have their own attributes associated with them such as data type, access list, data owner, creation time etc.; their system tries to make use of this kind of attributes in a social network for regulating access.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

They establish architecture based on XACML which allows the process of authorization to take place between social collaborative networks. Here, the concept of ABAC serves as a basis for allowing cross domain access control, as only attributes needs to be evaluated for determining access decision and as long as the other local social network can provide required attributes to the remote social network no further change to the underlying authorization system of remote social network would be needed.

Ni Dan et al [7] propose an ABAC based cross domain access control in service-oriented architecture. SOA allows management and use of distributed resources which are managed by different management domain. As architecture of SOA involves loosely coupled systems, their system provides common access control mechanism which can provide authorization across distributed, loosely coupled and integrated services. Due to open environment of SOA, ABAC can be used as an access control model that can provide more fine-grained access control than traditional access control models.

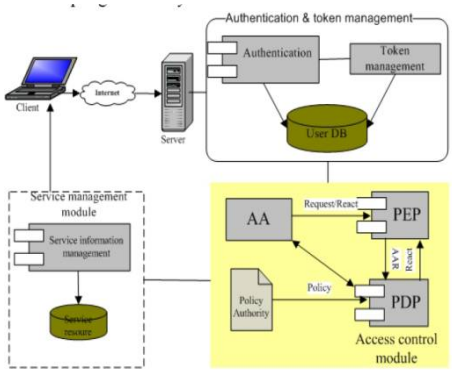

Figure 2:ABAC based cross domain access control in SOA [7].

The system contains three major functional modules as shown in figure 2:

1. The authentication and token management module: Authenticates the user and provides the identity token to user and also verifies user's identity token for authentication.
2. Access control module: Contains the policy enforcement point, policy decision point, policy authority, and attribute authorities.
3. Service management module: service registration and service querying functionality is provided by this module.

I. Indu et al [4] propose an integrated identity and attribute based authorization system for cloud web services. Identity as a service (IDaaS) refers to the management of identities of the users in the cloud by third party vendors. In their system a hybrid architecture, combining authentication and attribute based access control is used. The user's authentication is done thorough identity management system. After verifying user's credentials, a token is provided which will be used by web service for further verification. After successful authentication, the access control mechanism verifies the identity of that person, requested resources, time, location and policies of the organization [4].

Clouds have diverse groups of users with different sets of security requirements; to deal with this, Khaled Riad et al [5] propose an access control model called Attribute-Rule ABAC. This model aims to fulfil a set of cloud computing requirements such as flexible attribute management, least privileges and supporting multitenant aspect of cloud environment. An attribute rule defines what kind of and how many attributes should be taken into account for making access decisions. A specific role is assigned to each user based on the attributes of the user and each role has specific permitted tasks. Attribute rule assigns weight to each attribute and this reflects its power to be used, and if aggregated over a set of attributes, it reflects its assigned role (for user attributes) and sensitivity level (for object attributes)[5]. The capability of least privileges is supported by assigning role to each user; further role has specific allowed tasks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

which has different permissions associated with it. This is done automatically using set of attributes possessed by the user, policy, constraints and environment conditions.

In [6], Andy Chunliang Hsu et al proposes a location aware attribute based access control model for Online Social Networks (OSNs). The figure 3 shows the User attributes Credentials, Relations, Location, Group, and Application, with Credentials being the attributes, such as, login id and passwords which are used to determine access decision. Similarly, objects have attributes which describe their type, sensitivity level and owner. The relation permission has a single attribute called location. In order to get access to the object, the location for access must match with the location stored in the location attribute of the user.

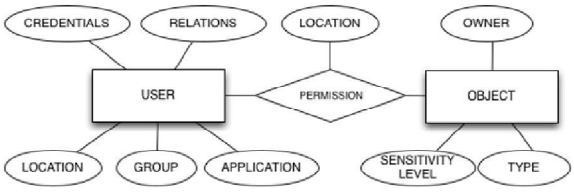

Figure 3: Location-Aware OSN model [6]

III. COMPARISON OF WORK DONE IN STUDIED PAPERS:

Lit. Ref.	Nature of the context	Problem discussed	Work done	Advantages
2.	Distributed Resources, accessed using HTTP methods GET, POST, PUT, DELETE.	Access control language for RESTful services supporting distributed nature of RESTful services.	An access control language RestACL, and supporting algorithms: Mapping (resources to policy) and Evaluation (evaluation of access decision).	Efficient processing of access requests, flexible addressing of sets of resources, separation of duty and ease of modification.
3.	Collaborative social networks.	Access control to the information shared over collaborative social networks.	A uniform access control architecture allowing secure access to the resources of members of other social network.	Does not require any data reprocessing the access request is directly handled by the location at which the resource resides.
7.	ABAC for SOA based Web services.	Security guarantee in integrated, loosely coupled and cross-domain access security.	Secure message passing using MD5, Authentication and token management, Access control using attribute, service management module.	Provides fine-grained access control, improves the scalability and flexibility of the system, and solves the problem of cross-domain access control.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

5.	Extending ABAC for cloud using Attribute-Rules.	Cloud security challenge.	Assignment of weight to attribute, sensitivity level to objects, role to users and using this assignment as a basis of access control	Attribute-rule feature of this system eliminates the larger decision making time.
6.	Location aware ABAC for OSN.	Providing more security to OSN using location attribute	Extension of Policy machine to accommodate location and time attributes.	Allows location based policy specification which can satisfy the needs of systems distributes over different locations.
4.	Identity and authorization management in the context of cloud	Authentication and authorization for cloud computing.	A token based authentication system, Attribute based authorization system	Fine grained, flexible and scalable access control

IV. CONCLUSION

In this study, different implementations of ABAC based authorization system were studied briefly; from the analysis of current ABAC implementations on distributed, heterogeneous and open environments, ABAC proves to be suitable for cloud storage services. Apart from the basic access control requirements, ABAC can prove as best authorization model for the dynamic cloud environment due to its inherent benefit offerings.

REFERENCES

1. Vincent C. Hu, D. Richard Kuhn, and David F. Ferraiolo, "Attribute based access control", Computer, Vol.48, Issue 2, pp 85-88, 2015.
2. Marc Hüffmeyer, Ulf Schreier, "RestACL - An Access Control Language for RESTful Services",ACM Conference on Data and Application Security and Privacy, pp. 58-67 , 2016.
3. Cheng Man Ma, Yan Zhuang, Simon Fong, "Information sharing over collaborative social networks using XACML", IEEE 8th International Conference on E-Business Engineering, pp.161-167, 2011.
4. I. Indu and P. M. Rubesh Anand, "Identity and Access Management for Cloud Web Services", IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp.406-410, 2015.
5. Khaled Riad, Zhu Yan, Hongxin Hu and Gail-Joon Ahn, "AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing", IEEE Conference on Collaboration and Internet Computing, pp.28-35, 2015.
6. Andy Chunliang Hsu and Indrakshi Ray , "Specification and Enforcement of Location-Aware Attribute-Based Access Control for Online Social Networks", ACM Conference on Data and Application Security and Privacy, pp.25-34, 2016.
7. Ni Dan, Shi Hua-ji, Chen Yuan and Guo Jia-hu, "Attribute Based Access Control (ABAC)-based cross-domain access control in service-oriented architecture (SOA)", International Conference on Computer Science and Service System, pp.1405-1408, 2012.
8. Extensible Access Control Markup Language (XACML) Version 3.0. , Organization for the Advancement of Structured Information Standards (OASIS), 2013.

BIOGRAPHY

Krupali Patel is a M.E. Student in the Computer Engineering Department, Sardar Vallbhbhai Patel Institute of Technology, Vasad. Her research interests are analysis of Access control systems and attribute based authorization.