Abstract

Security of applications has been identified as one of the major concerns in today's multi-domain collaborative environments such as multi-cloud systems. Each domain in this context consists of a group of users and resources (objects) owned by an organization. The applications that span across multiple domains are often found to be vulnerable to security threats which are caused by unauthorized accesses of resources by the users across the collaborating domains. Developing a highly effective access control mechanism for multi-domain environments, which meets security requirements such as confidentiality, integrity, availability, and accountability, is a challenging task. Since multi-domain applications are bounded by numerous constraints of the disparate domains they are deployed in, traditional access control mechanisms such DAC, MAC, and RBAC are inappropriate for such systems. The constraints can be either semantic or contextual in nature. The semantic constraints such as separation of duty are associated with the subjects and objects of the system, whereas the contextual (environment) constraints are independent of both.

A fine-grained access control mechanism such as Attribute-based Access Control (ABAC) is considered to be an appropriate choice for authorization management in multi-domain systems. In ABAC, constraints can be expressed in terms of the properties of the subjects, objects, and environments and are often called attributes. ABAC uses subject attributes, object attributes, and environment attributes for making access control decisions. Furthermore, integration of accesses control policies expressed using traditional access control models in domains can be done easily by migrating them into ABAC policy.

A first step towards successfully deploying ABAC is to define an appropriate set of access control rules that establish the desired inter-domain accesses. An ABAC access control rule comprises an antecedent and a consequent. A set of attribute-value pairs of subjects, objects, and environment constitutes the antecedent of a rule. The consequent consists of grant or denial of access privileges over objects. Depending upon the truth value resulting from the evaluation of the antecedent, access privileges on objects are either granted or denied to subjects. If certain accesses are granted in accordance with a rule, such a rule is called a positive authorization rule (*permit* rule). On the other hand, if certain accesses are denied by a rule, it is called a negative authorization rule (*deny* rule).

We propose two approaches for inter-domain rule formation in ABAC. In the first

approach, we consider cross domain rule mining as the problem of forming a minimal set of positive authorizations only. The second approach shows the advantage of developing deny rules along with positive authorizations in reducing the total number of rules and hence, the response time for evaluating access requests. The problem of forming a minimal set of cross domain rules is proved to be NP-Hard. Heuristic solutions are proposed and evaluated on benchmark datasets showing encouraging results.

The process of forming a correct set of access control rules becomes more challenging when the access requirements vary with time or the users and objects are updated quite frequently. We also study the problem of formulation of an optimal set of ABAC rules for granting inter-domain accesses in a dynamic environment. The problem being NP-Hard, we propose heuristic solutions.

Finally, we study the problem of data leakage as a major security concern in a multi-domain collaborative environment, which is caused by illegitimate actions of malicious users often acting in collusion. The possibility of data leakage in such environments is characterized by the number of interoperations as well as the trustworthiness of users on the collaborating clouds. We address the problem of data leakage free multi-domain collaboration from an ABAC policy management perspective. In particular, we define a problem that aims to formulate ABAC policy rules for establishing a high degree of inter-domain accesses while eliminating potential paths for data leakage. A data leakage free ABAC policy generation algorithm is proposed that first determines the likelihood of data leakage and then attempts to maximize inter-domain collaborations. We also pose several variants of the problem by imposing additional meaningful constraints on the nature of accesses. Experimental results on several large data sets show the efficacy of the proposed approach.

Keywords: Distributed security, Multi-domain authorization, Dynamic collaboration, Data leakage, Trustworthiness, Attribute-based access control, ABAC policy mining.