**A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification**

**Abstract**

Sharing of resources on the cloud can be achieved on a large scale since it is cost effective and location independent. Despite the hype surrounding cloud computing, organizations are still reluctant to deploy their businesses in the cloud computing environment due to concerns in secure resource sharing. In this paper, we propose a cloud resource mediation service offered by cloud service providers, which plays the role of trusted third party among its different tenants. This paper formally specifies the resource sharing mechanism between two different tenants in the presence of our proposed cloud resource mediation service. The correctness of permission activation and delegation mechanism among different tenants using four distinct algorithms (Activation, Delegation,Forward Revocation and Backward Revocation) is also demonstrated using formal verification. The performance analysis suggest that sharing of resources can be performed securely and efficiently across different tenants of the cloud.

**Existing System**

Traditional access control models, such as role based access control, are generally unable to adequately deal with cross-tenant resource access requests.

However, takes the decidability problem as first order logic formula and decides its satisfiability based on the decidable background theory. There are a number of theories supported by the SMT solvers, such as equality and uninterpreted functions, linear arithmetic over rationals, linear arithmetic over integers, non-linear arithmetic over reals, over arrays, bit vectors, and combinations.

The SMT-Lib provides a common input platform for a number of solvers used in the verification of systems. Behavioral specifications of a system can also be represented using abstract models. The SMT solvers are then used to perform bounded model checking to explore a bounded symbolic execution of the model.

**Proposed System**

We present a CTAC model for collaboration, and the CRMS to facilitate resource sharing amongst various tenants and their users.

We also present four different algorithms in the CTAC model, namely: activation, delegation, forward revocation and backward revocation.

We then provide a detailed presentation of modeling, analysis and automated verification of the CTAC model using the Bounded Model Checking technique with SMTLIB and Z3 solver, in order to demonstrate the correctness and security of the CTAC model.

Role based access control (RBAC) enables fine-grained access control (and generally in a single domain). Different extensions of RBAC have been proposed in the literature to support multi-domain access control. These approaches rely on a single body responsible for maintaining cross-domain policies.

### IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

 The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules

1.Cloud resource mediation service (CRMS)

2. Cross-tenant access control (CTAC) model

3.Verification of the CTAC Model

**Cloud resource mediation service (CRMS)**

Tenant T1 responsibilities: T1 is responsible for publishing cross tenant policies on the CRMS. T1 receives access requests from T2 and redirects the request to the CRMS for further processing.

Tenant T2 responsibilities: The CRMS redirects access requests to T2 for authentication. Once the redirected access request is received, the responsibility of T2 is to authenticate the identity of particular user. In response, T2 sends the user authentication response (valid or invalid) and tenant authentication response to the CRMS.

CRMS responsibilities: The CRMS receives the permission-activation request redirected from T1. Once an access request is received, the CRMS evaluates the request on the pre-published policies and responds to T1.

**Cross Tenant Access Control (CTAC) Model**

An intra-tenant user, after the activation of a permission, has delegated the requested permission to the cross-tenant user. In other words, an approved delegation must exist for the cross-tenant user.

An intra-tenant/cross-tenant user has delegated the requested permission to a tenant (i.e. an approved delegation must exist for a particular tenant).

There are two types of delegation that exist in the system, namely: user-level delegation and tenant-level delegation. Failure of one of these two cases will result in the checking of the other case. If none of the cases are satisfied, then the algorithm terminates and the permission delegation for the corresponding cross-tenant user/ cross-tenant fails.

**Verification of the CTAC Model**

The correctness of a system is demonstrated by the verification process. To prove the correctness of the system under consideration, the system is verified on the system specifications, and the system properties.

The CTAC model verification using the Z3 constraint solver: We verified the CTAC model by proving the correctness of activation algorithm, delegation algorithm, forward revocation algorithm, and backward revocation algorithm. Each algorithm was modeled, analyzed, and verified. Specifically, the algorithm was modeled using HLPN, and the Z formal language was used to define transition rules. The array theory of SMT-Lib was then used to transform such rules. Finally, the properties of the algorithm were verified using the Z3 solver.

# System Configuration

# H/W System Configuration:

#  Processor - Pentium –III

Speed - 1.1 Ghz

RAM - 256 MB(min)

Hard Disk - 20 GB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

# S/W System Configuration:

* Operating System :Windows XP /7
* Application Server : Tomcat/6.X
* Front End : HTML, Java, Jsp, .Net
* Scripts : JavaScript.
* Server side Script : Java Server Pages.
* Database : Mysql
* Database Connectivity : JDBC.

**Conclusion**

In this paper, we proposed a cross-tenant cloud resource mediation service (CRMS), which can act as a trusted-third party for fine-grained access control in a cross-tenant environment. For example, users who belong to an intra-tenant cloud can allow other cross-tenant users to activate a permission in their tenant via the CRMS. We also presented a formal model CTAC with four algorithms designed to handle the requests for permission activation. We then modeled the algorithms using HLPN, formally analyzed these algorithms in Z language, and verified them using Z3 Theorem Proving Solver. The results obtained after executing the solver demonstrated that the asserted algorithm specific access control properties were satisfied and allows secure execution of permission activation on the cloud via the CRMS.

**Future Work**

Future work will include a comparative analysis of the proposed CTAC model with other state-of-the-art cross domain access control protocols using real-world evaluations. For example, one could implement the protocols in a closed or small scale environment, such as a department within a university. This would allow the researchers to evaluate the performance, and potentially (in)security, of the various approaches under different real-world settings.