A Cross Tenant Access Control (CTAC) Model forCloud Computing: Formal Specification andVerification

ABSTRACT:

Sharing of resources on the cloud can be achievedon a large scale since it is cost effective and location independent.Despite the hype surrounding cloud computing, organizations arestill reluctant to deploy their businesses in the cloud computingenvironment due to concerns in secure resource sharing. In thispaper, we propose a cloud resource mediation service offered bycloud service providers, which plays the role of trusted thirdparty among its different tenants. This paper formally specifiesthe resource sharing mechanism between two different tenants inthe presence of our proposed cloud resource mediation service.The correctness of permission activation and delegation mechanismamong different tenants using four distinct algorithms(Activation, Delegation,Forward Revocation and Backward Revocation)is also demonstrated using formal verification. Theperformance analysis suggest that sharing of resources can beperformed securely and efficiently across different tenants of thecloud.

EXISTING SYSTEM:

- Zhao et al. propose a cross-domain single sign onauthentication protocol for cloud users, whose security was also proven mathematically. In the approach, the CSP is responsible for verifying the user's identity and making access control decisions.
- As computing resources are being shared between tenants and used in an on-demand manner, both known and zeroday system security vulnerabilities

could be exploited by the attackers (e.g. using side-channel and timing attacks).

- In existing, a fine grained data-level access control model (FDACM) designed to provide role-based and data-based access control for multi-tenant applications was presented. Relatively lightweight expressions were used to represent complex policy rules.

DISADVANTAGES OF EXISTING SYSTEM:

- Traditional access control models, such as role based access control, are generally unable to adequately deal with cross-tenant resource access requests.
- Specification level security is difficult to achieve at the user and provider ends.
- The security of the approach was not provided.

PROPOSED SYSTEM:

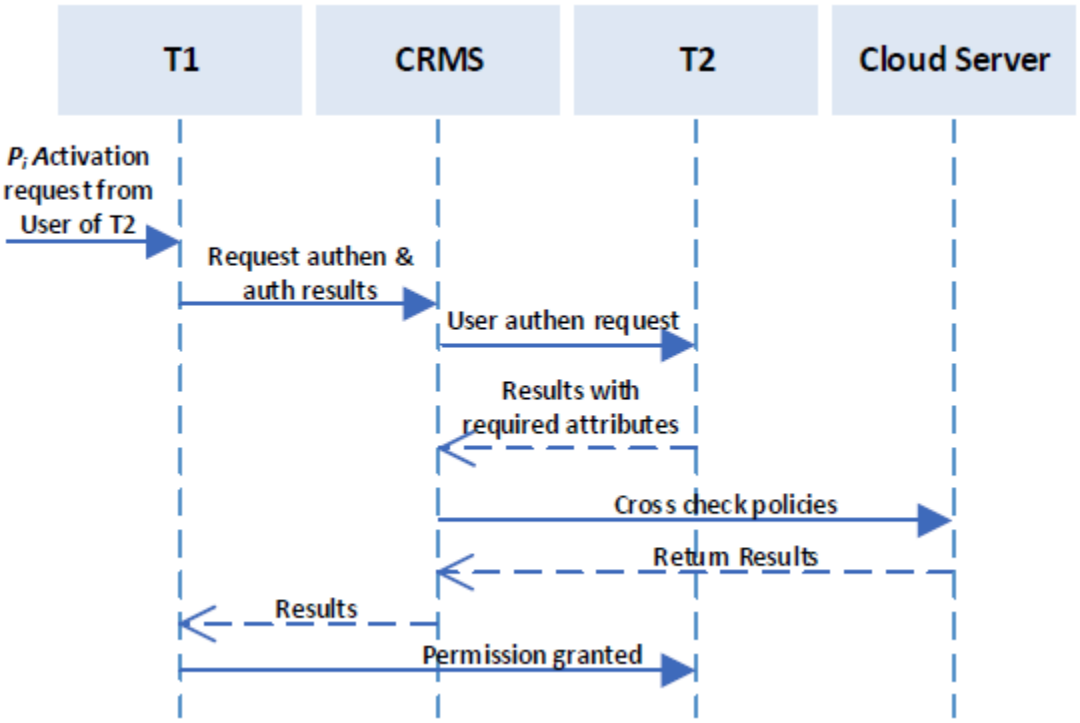
- We use model checking to exhaustively explore the system and verify the finite state concurrent systems. Specifically, we use High Level Petri Nets (HLPN) and Z language for the modeling and analysis of the CTAC model.
- We present a CTAC model for collaboration, and the CRMS to facilitate resource 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.

ADVANTAGES OF PROPOSED SYSTEM:

- HLPN provides graphical and mathematical representations of the system, which facilitates the analysis of its reactions to a given input. Therefore, we are able to understand the links between different system entities and how information is processed.
- We then verify the model by translating the HLPN using bounded model checking. For this purpose, we use Satisfiability Modulo Theories Library (SMT-Lib) and solver. We remark that such formal verification has previously been used to evaluate security protocols

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE

- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Quratulain Alam, Saif U. R. Malik, Member, IEEE; Adnan Akhunzada, Kim-Kwang Raymond Choo, SeniorMember, IEEE; Saher Tabbasum, and Masoom Alam, "A Cross Tenant Access Control (CTAC) Model forCloud Computing: Formal Specification andVerification", **IEEE Transactions on Information Forensics and Security, 2017.**