A Multi-Tenant Access Control Scheme for Sharing Resources in Cloud Computing Environments

Rajeswari P.V.N[1], [2]T. Sahithi*
[1]Assoc Professor, Dept. of CSE, Visvodaya Engineering College, AP, India.
[2]M.Tech, Dept. of CSE, Visvodaya Engineering College, AP, India.

***Abstract*:**

Objective: This paper is aimed to study sharing of resources on the cloud can be achieved on a large scale since it is cost effective and location independent.

Methods/Statistical analysis: Despite of the advantages of 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.

Findings: To evaluate the our proposed method in terms of security, effectiveness, and efficiency each algorithm was modeled, analyzed, and verified using HLPN, and the Z formal language was used to define transition rules. Finally, the properties of the algorithm were verified using the Z3 solver. The outcomes acquired in the wake of executing the solver exhibited that the asserted algorithm explicit access control properties were fulfilled and permits secure execution of privilege activation on the cloud through the CRMS.

Applications/Improvements: we 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.

Keywords: Access Control, Revocation, Cloud Computing.

1. Introduction

While there are various advantages managed by the utilization of cloud computing to encourage coordinated effort among clients and associations, security and protection of cloud services and the client information may discourage a few clients and associations from utilizing cloud and remain points important to analysts[1-4]. Regularly, a cloud service provider (CSP) gives a web interface where a cloud client can oversee assets and settings.

In any case, traditional access control models, for example, role based access control[5], are commonly unfit to enough manage cross-tenant resource get to demands. Specifically, cross-tenant access request present three key difficulties. First, each occupant must have some earlier understanding and learning about the

outside clients who will access the assets. Along these lines, an administrator of each occupant must have a list of clients to whom the access will be permitted. This procedure is static in nature. Secondly, each occupant must be permitted to define cross-occupant access for different occupants as and when required. At long last, as each occupant has its very own control, trust the management issue among occupants can be trying to address, especially for hundreds or thousands of occupants.

To give a protected cross-tenant resource right to use service, a fine-grained cross-tenant access control[6-8] demonstrate is required. Along these lines, in this paper, we propose a cloud resource mediation service (CRMS) to be offered by a CSP, since the CSP assumes a urgent job overseeing diverse occupants and a cloud client endows the information to the CSP. We set that a CRMS can give the CSP upper hand, since the CSP can give clients with secure access control benefits in a cross- tenant access control (CTAC).

To show the accuracy and protection of the proposed methodology, we utilize model checking to exhaustively investigate the framework and verify the limited state simultaneous frameworks. In particular, we utilize High Level Petri Nets (HLPN) and Z dialect for the demonstrating and examination of the CTAC model.

2. Research Method

In this segment, we illustrate our proposed CRMS designed to encourage the CSPs in overseeing cross-tenant resource access requests for cloud clients. To give details of the service, we utilize a example including two tenants, T_1 and T_2, where T_1 is the Service Provider (SP) and T_2 is the Service Requester (SR). T_1 must claim some consent pi for which client of T_2can produce a cross-tenant request. The service request for from a client of T_2 must be submitted to T_1, which then handovers the demand to the CRMS for verification and approval decisions. The CRMS executes the request dependent on the security polices given by T_1. The steps are signified in Figure 1 and described.

Insert Figure 1 Here

2.1 Steps for permission activation request in the cloud

There are three principle substances, to be specific: the SP (T_1), the SR (T_2), and the CRMS. The roles of these substances are explained as follows:

a) Tenant T_1 responsibilities: T_1 is in charge of distributing cross tenant approaches on the CRMS. T_1 receives access request from T_2 and transmits the request to the CRMS for further handling.

b) Tenant T_2 responsibilities: The CRMS diverts access requests to T_2 for validation. When the diverted access request is received, the duty of T_2 is to validate the identity of specific client. Accordingly, T_2 sends the client validation response and tenant validation reaction to the CRMS.

c) CRMS responsibilities: The CRMS gets the authorization activation request transmitted from T_1. When an access request for received, the CRMS evaluates the request on the pre-distributed approaches and reacts to T_1.

The steps for initiating a permission-activation request are as follows:

1. Permission activation request: A client wishing to access a resource at T_1. The client will be introduced an directory where a list of shared services alongside their depictions are available.

2. Request redirection to the CRMS: Upon choice of a mutual service the client wishes to access, the client is diverted to the CRMS site. On the site, the client will be requested the parent tenant. The client chooses the parent tenant and the CRMS diverts the client's demand to the chosen tenant.

3. Tenant T_2 authentication: The client needs to validate at her parent tenant, T_2. Upon effective verification, the client will be diverted again to CRMS with the attributes requested by the CRMS for cross tenant approach execution.

4. CRMS redirection to tenant T_1 & permission activation: The client's attributes are validated against the T_1 strategy and if the policy criteria is effectively satisfied, then the client is provided service access at T_1; otherwise, the access request is denied. The CRMS likewise considers any irreconcilable circumstance approaches, for example, Chinese Wall Policy.

2.2 Cross-Tenant Access Control (CTAC) Model

To manage cross- tenant resource requests within the sight of CRMS, we depict the components of the CTAC display whose key components are as per the following:

- U_i explores set of intra-tenant client. A client from this set can likewise go about as the delegator of the privilege.
- U_j and U_k represent to the set of cross-occupant clients. A client from both of the sets can likewise go about as delegator or delegate.
- Y Pi represents a set of privileges.
- $U\ P\ A_i \subseteq (U_i \times P_i)$. A binary association between the intratenant clients and the set of authorizations relegated to them in the i^{th} tenant.
- $U\ P\ A_a \subseteq (U_i \times P_i)$. A binary association between the intra-tenant clients and the set of privileges turn on by them in the i^{th} tenant.
- $L\ E\ U_a \subseteq (U_i \times U_j \times P_i)$. A triple association between the intra-tenant clients, cross-tenant clients and the set of privileges turn on by them in the i^{th} tenant.

- $E\ E\ U_a \subseteq (U_j \times U_k \times P_i)$. A triple association between the cross-tenant clients and the set of privileges turn on by them in the i^{th} tenant.
- $L\ E\ D_a \subseteq (U_i \times t \times P_i)$. A triple association between the intra-tenant clients, the tenant and the set of privileges turn on by the clients of that tenant in the i^{th} tenant.
- $E\ E\ D_a \subseteq (U_k \times t \times P_i)$. A triple association between the cross-tenant clients, the tenant and the set of privileges turn on by the clientss of that tenant in the i^{th} tenant.
- $LEU\ D_{POL} \subseteq (U_i \times U_j \times P_i \times C)$. A fourfold associations among the intra-tenant clients, the cross-tenant clients, the set of privileges, and the set of delegation imperatives distributed on the CRMS for the evaluation of the requested resource.
- $EEUD\_POL \subseteq (U_j \times U_k \times P_i \times C)$. A fourfold associations among the cross-tenant clients, the set of authorizations, and the set of delegation requirements distributed on the CRMS for the evaluation of the requested resource.
- $LEDD\_POL \subseteq (U_i \times t \times P_i \times C)$. A fourfold connection among the intra-tenant clients, the tenant, the set of authorizations, and the set of delegation constraints distributed on the CRMS for the evaluation of the requested resource.
- $EEDD\_POL \subseteq (U_k \times t \times P_i \times C)$. A fourfold connection among the cross-tenant clients, the tenant, the setof authorizations, and the set of delegation requirements distributed on the CRMS for the evaluation of the requested resource.

3. Results and Analysis

a) The System verification: The accuracy of a framework is exhibited by the verification procedure. To prove the accuracy of the framework under thought, the framework is checked on the framework particulars, and the framework properties.

b) The CTAC model verification using the Z3 constraint solver: We verified the CTAC model by demonstrating the rightness of activation algorithm, delegation algorithm, forward revocation algorithm, and backward revocation algorithm. Every algorithm was displayed, dissected, and checked. In particular, the algorithm was demonstrated utilizing HLPN, and the Z formal language was utilized to define change rules. The array hypothesis of SMT-Lib was then utlized to change such principles. At long last, the properties of the algorithm were checked utilizing the Z3 solver. The properties of algorithm were additionally checked for satisfiability of sensible formulae over the algorithm determination. The Z3 solver played out the calculations and produced result as satisfiable sat or unsatisfiable unsat. On the off chance that the produced yield is sat, this shows there is an infringement of the stated property and the solver will create a counter precedent. On the other hand, if the produced outcome is unsat, then this demonstrates the property holds and suggests the accuracy of the algorithm.

c) Security Properties for Activation Algorithm: The activation algorithm exact properties are as follows:

- **(Activation.a) Intra-tenant client to authorization allotment property** holds when the intra-tenant client and the privilege both exist in the intra-tenant privilege allotment set.
- **(Activation.b) Intra-tenant client to cross-tenant client enactment property** holds when the intra-tenant client, cross-tenant client and the authorization match the intracross-tenant client privilege set.
- **(Activation.c) Cross-tenant client to cross-tenant client activation** property holds when the two cross-tenant clients and the privilege coordinate the cross-cross-tenant client authorization set.
- **(Activation.d) Intra-tenant client to cross-tenant enactment property** holds when the intra-tenant client, cross tenant and the authorization coordinate the intra-client cross tenant privilege set.
- **(Activation.e) Cross-tenant client to cross-tenant activation property** holds when the cross-tenant client, crosstenant and the authorization coordinate the cross-client crosstenant-privilege set.

d) Correctness of Activation Algorithm: In the activation algorithm, at the season of enactment, an intra-tenant client or a cross-tenant client activates a privilege in the wake of satisfying a few conditions. To demonstrate the rightness of the activation algorithm, the activation algorithm must satisfy one of the accompanying legitimate equations.

- (Activation.a) OR (Activation.b) OR (Activation.d) (For an intra-tenant user)
- (Activation.c) OR (Activation.e) (For a cross-tenant user)

Additionally, we characterized the algorithm explicit properties for the delegation, forward revocation and the backward revocation algorithms. In spite of the fact that these properties are not exhibited here, they were considered in the verification procedure.

e) Results: We changed every algorithm with their properties to the SMT solver, so we could check them. Z3 solver considers both the model and its attributes and checks the properties of the model satisfy the required dimension of fulfillment. In the execution of the CTAC display with the expressed qualities in the Z3 solver, the model of CTAC performed well and created the outcomes obviously. F QF AUFLIA rationale utilized for closed quantifier-free linear equations over the hypothesis of whole number exhibits stretched out with free sort and function symbols, was additionally utilized in execution under SMT-LIB.

Since our point is to verify the rightness of the proposed algorithms under the CTAC show, by executing the formal models of the algorithms with the affirmed properties in the Z3 solver, we acquired the required outcomes.

The outcomes exhibit that the CTAC display can achieve the tasks in a limited time. In addition, for this situation, the execution time demonstrates that the explicit time taken by the Z3 solver so as to measure the satisfiability of the properties. This exhibited both exactness and accuracy. The execution time devoured by Z3 solver on the individual security property of the algorithms is depicted in Figure 2.

Insert Figure 2 Here

4. 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 condition. For instance, clients who have a place with an intra-tenant cloud can enable different cross-tenant clients to make active an authorization in their tenant by means of the CRMS. We likewise exhibited a formal model CTAC with four algorithms intended to deal with the solicitations for authorization initiation. We at that point displayed the algorithms utilizing HLPN, formally examined these algorithms in Z language, and confirmed them utilizing Z3 Theorem Proving Solver. The outcomes got in the wake of executing the solver showed that the declared algorithm explicit access control properties were fulfilled and permits secure execution of privilege activation on the cloud through CRMS.

References

1. Heiser, J., 2009. What you need to know about cloud computing security and compliance. Gartner, Research, ID, (G00168345).

2. Choo, K.-K. R., Domingo-Ferrer, J. and Zhang, L., 2016. Cloud Cryptography: Theory, Practice and Future Research Directions. Future Generation Computer Systems, 62, pp. 51-53.

3. Jung, T., Li, X. Y., Wan, Z. and Wan, M., 2015. Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption. IEEE Transactions on Information Forensics and Security, 10(1), (pp. 190-199).

4. Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J., 2016. Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services. IEEE Transactions on Information Forensics and Security, 11(3), (pp. 484-497).

5. Liu, X., Deng, R. H., Choo, K.-K. R. and Weng, J., 2016. An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys. IEEE Transactions on Information Forensics and Security, 11(11), pp. 2401-2414.

6. Yang, Y., Zhu, H., Lu, H., Weng, J., Zhang, Y. and Choo, K.-K. R., 2016. Cloud based data sharing with fine-grained proxy re-encryption. Pervasive and Mobile Computing, 28, pp. 122-134.

7. Tang, B. and Sandhu, R., 2013, August. Cross-tenant trust models in cloud computing. In Information Reuse and Integration (IRI), 2013 IEEE 14th International Conference on (pp. 129-136). IEEE.

8. Ma, K., Zhang, W. and Tang, Z., 2014. Toward Fine-grained Data-level Access Control Model for Multi-tenant Applications. International Journal of Grid and Distributed Computing, 7(2), pp.79-88.

Figures

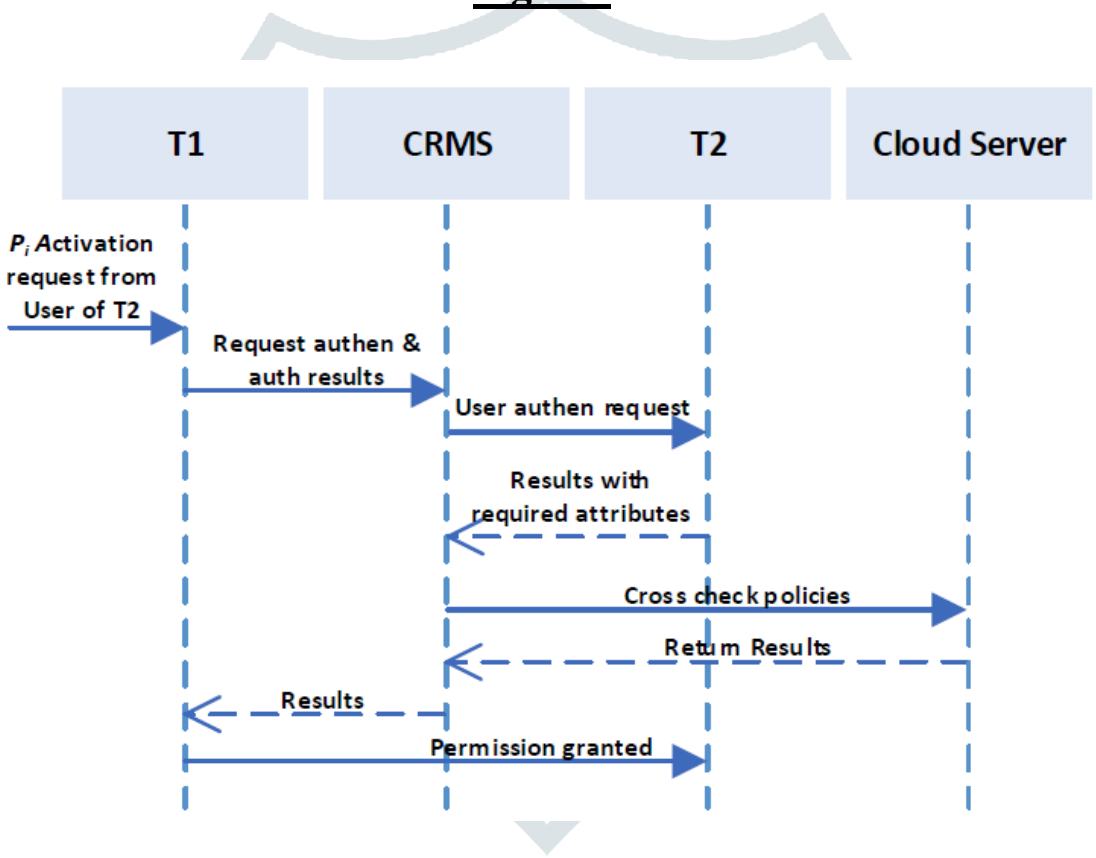

Figure 1: Sequence diagram for permission request in the cloud

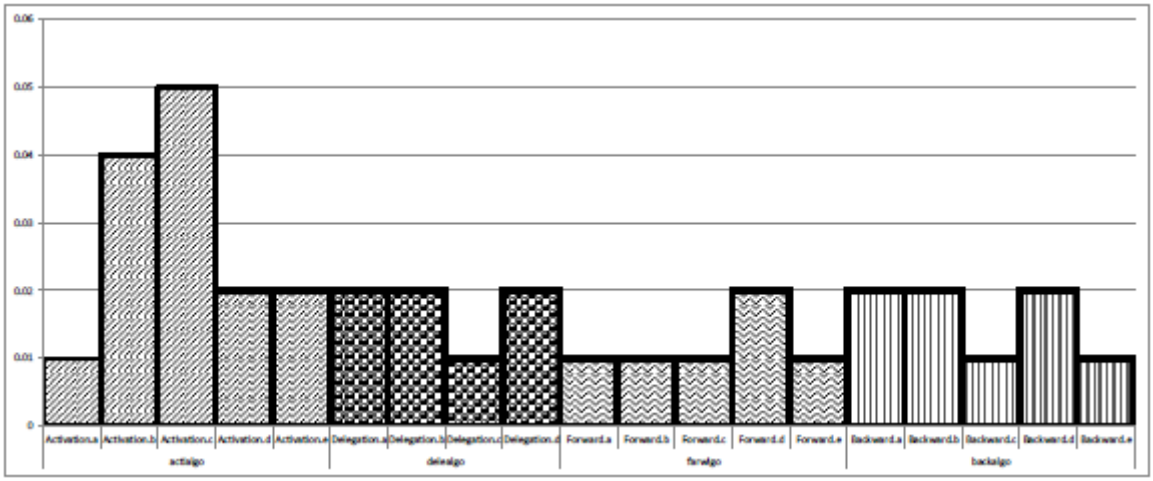

Figure 2: Verification results of the CTAC model