A Cross tenant Secure Data Sharing Scheme Using Cloud Resource Mediation Service

M.Rajeswari & E.Ravi

[1]PG Scholar, Dept of CSE, Khader Memorial College of Engineering & Technology, Nalgonda, TS, India.

[2]Associate Professor, Khader Memorial College of Engineering & Technology, Nalgonda, TS, India

Abstract-*Most cloud services are built with multi-tenancy which enables data and configuration segregation upon shared infrastructure. Each tenant essentially operates in an individual silo without interacting with other tenants. However, outsourcing data to a third-party administrative control entails serious security concerns. Data leakage may occur due to attacks by other users and machines in the cloud. Consequently, high-level of security measures is required. Resource sharing on the cloud can be achieved on a large scale as this is location independent and cost effective. In this paper, we propose a cloud resource mediation service (CRMS) which is offered by the cloud service providers (CSP), which acts as the role of trusted third party among their various tenant members. This specific model determines the asset sharing information between two different tenants within the sight of our proposed cloud resource mediation service. The correctness of activation and delegation mechanism is done by four distinct algorithm (Activation, Delegation, Forward Revocation and Backward Revocation) is also illustrated using formal verification.*

KEYWORDS: Cross Tenant Access Control, Authentication, Verification, Cloud Computing, Security

INTRODCUTION

Cloud computing has developed rapidly and become a force transforming the IT industry. Its service models have been increasingly accepted by consumers and enterprises. A cloud consumer outsources part of its computing resources to a cloud service provider (CSP). The CSP is responsible for providing a web interface where a cloud user can manage resources and settings. A CSP then implements these access control features on consumer data and other related resources. Multi tenancy is a basic feature of cloud computing. It seeks to isolate activities of tenants from each other to protect data security and privacy. Currently many CSPs simply block cross tenant accesses in the cloud. This solution raises many problems, such as data lock-in [8], which restrict the development of cloud computing. In order to break the barrier between tenants in a controllable way, a suitable cross tenant access control model is essential. Traditional access control models, such as role based access control [7], are generally unable to adequately deal with cross tenant resource access requests. A fine grained access control model is required [21] to provide secure cross tenant access service. Thus in this paper, we propose a cloud resource mediation service (CRMS) to be offered by a cloud service provider (CSP). We posit that a CRMS can provide the CSP competitive advantage, since the CSP can provide users with secure access control services in a cross tenant access environment. A CSP plays a pivotal role managing different tenants and the cloud user entrusts the data to the CSP. The CTAC model has two advantages. The privacy of a tenant, say T2, is protected from another tenant, say T1, and the CRMS, since T2's attributes are not provided to T1. T2's attributes are evaluated only by the CRMS. Furthermore, a user does not provide authentication credentials to the CRMS. Therefore, the privacy of T2 is also protected as the CRMS has no knowledge of the permissions that T2 is requesting from T1. The security policies defined by T1 use pseudonyms of the permissions without revealing the actual information to theWe use High Level Petri Nets (HLPN) and Z language for the modeling and analysis of the CTAC model. HLPN provides graphical and mathematical representations of the system, which facilitates the analysis of its reactions to a given input [14], [20]. 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 Z3 solver [17], [13].

2. RELATED WORK

In [1] the author explains Cross Tenant Trust Models supported and enforced by the cloud service provider. Considering the On-demand Self-Service feature intrinsic to cloud computing. Author propose a formal cross tenant trust model (CTTM) and its role-based extension (RB-CTTM) integrating various types of trust relations into cross-tenant access control models which can be enforced by the multi-tenant authorization as a service (MTAaaS) platform in the cloud.

In [2] the author discusses Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption which presents a semi-anonymous privilege control scheme AnonyControl to address not only the data privacy but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi-anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, author presents the AnonyControl which fully prevents the identity leakage and achieve the full anonymity. Security analysis shows that both AnonyControl and AnonyControl-F are secure under the DBDH assumption, and performance evaluation exhibits the feasibility of schemes.

In [3] the author proposes Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, author also carry out a simulation to demonstrate the practicability of proposed 2FA system.

In [4] the author discusses the Jobber: Automating inter-tenant trust in the cloud that present Jobber: a highly autonomous multi-tenant network security framework designed to handle both the dynamic nature of cloud datacenters and the desire for optimized inter-tenant communication. Jobber prototype leverages principals from Software Defined Networking and Introduction Based Routing to build an inter-tenant network policy solution capable of automatically allowing optimized communication between trusted tenants while also blocking or rerouting traffic from untrusted tenants. Jobber is capable of automatically responding to the frequent changes in virtualized data center topologies and, unlike traditional security solutions, requires minimal manual configuration, cutting down on configuration errors.

In [5] author proposes Toward Fine-grained Data-level Access Control Model for Multi-tenant Applications, where role based and data based access control are both supported. Lightweight expressions are proposed to present complicated policy rules in solution. Moreover author also discusses the architecture and authorization procedure which implements these two models. Some technical implementation details together with the performance result from the prototype are provided.

In [6] the author proposes Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE) that explains the data security system that provides (a) key management (b) access control, and (c) file assured deletion. The DaSCE utilizes Shamir's (k, n) threshold scheme to manage the keys, where k out of n shares are required to generate the key. The author use multiple key managers, each hosting one share of key. Multiple key managers avoid single point of failure for the cryptographic keys. (a) implement a working prototype of DaSCE and evaluate its performance based on the time consumed during various operations, (b) formally model and analyze the working of DaSCE using High Level Petri nets (HLPN), and (c) verify the working of DaSCE using Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The results reveal that DaSCE can be effectively used for security of outsourced data by employing key management, access control, and file assured deletion.

3.PROPOSED WORK

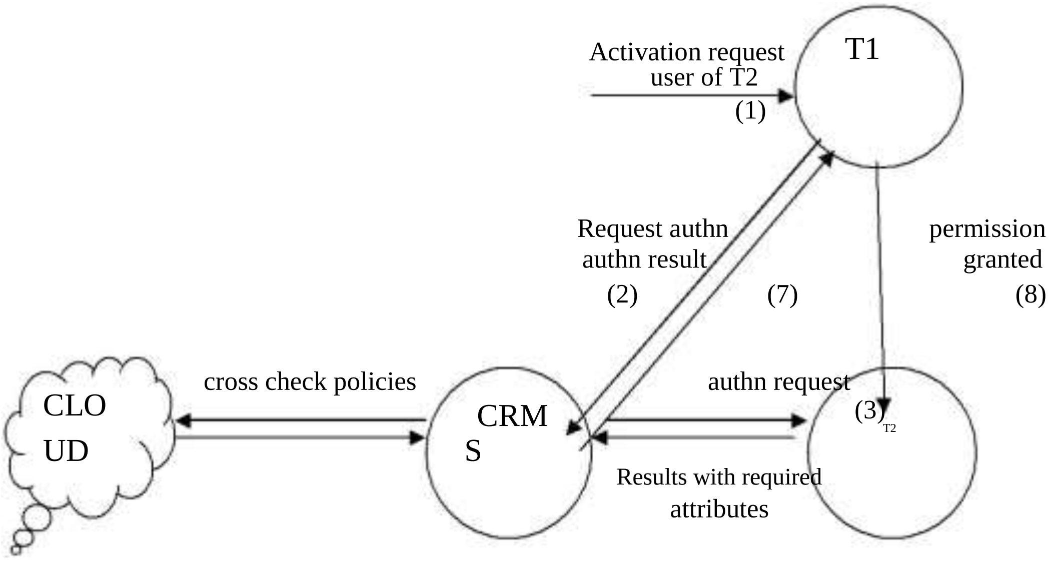

Fig1: System Architecture

In the Fig1 we describe our proposed cloud resource mediation service (CRMS) to be offered by CSP, designed to facilitate in managing cross-tenant resource access requests for cloud users. To explain the service, we use an example of two tenants, T1 and T2, where T1 is the Service Provider (SP) and T2 is the Service Requester (SR) (i.e. user). T1 must own some permission pi for which user of T2 can generate a cross-tenant request. The resource request from a user of T2 must be submitted to T1, which then handovers the request to the CRMS for authentication and authorization decisions. The CRMS evaluates the request based on the security polices provided by T1. We use model checking to thoroughly explore the system and confirm the finite state concurrent system. We show a CTAC demonstrate for collaboration and the CRMS to encourage resource sharing among different tenants and their clients. for the modeling and analysis of the CTAC model we use High Level Petri Nets (HLPN) and Z language. We additionally introduce four distinct algorithms in the CTAC model, (activation, delegation, forward revocation and backward revocation). We at that point give an detailed introduction of modeling, examination and robotized confirmation of the CTAC show utilizing the Bounded Model Checking procedure with SMTLIB and Z3 solver, keeping in mind the end goal to exhibit the accuracy and security of the CTAC model.

4.LIMITATIONS

- Using single tenant resource utilization is less when compared to multi-tenant.
- Using single tenant more expensive.
- Difficult to define access control over multi-tenant
- Revocation of particular tenant is difficult process

5.OBJECTIVE

The objective of this research work is achieving access control and efficient revocation in multi-tenancy cloud storage. For this proposing two different access models one is R-RBAC model and RW-Access control.TSP using R-RBAC (Revocable-Role based access control) model can allocate roles to different tenants and when ever required he can revoke also.Tenant can enable security for his data using RW (Read Write)-Access control.

6. SCOPE

Multi tenant is a shared storage server paradigm where multiple tenants are sharing single storage server in order to avoid cost and it avoid local storage maintenance, in multi tenancy achieving high scalability and effective access control is defined. In this implementation Tenant service provider (TSP), Tenant and Cloud service provider (CSP) are involved. From CSP storage server can accessed by TSP after TSP will share resource among multiple tenants.

7. RESEARCH METHODOLOGY

In cloud environment multi-tenant storage server is accessed by multiple users called tenants, so multi-tendency improve resource sharing and it reduces cost. But providing security between multi-tenants is major challenge so in this work in order to overcome challenges in multi-tendency proposing two levels of security.First level security for TSP, using R-RBAC the TSP can give set of privileges to set of tenants over storage server. Whenever tenant requesting for storage based on tenant signature the TSP will allocate particular block, and he can also revoke particular tenant and reassign storage to another tenant.

Second level security for Tenant, using RW-Access control, a tenant can define set polices over his storage like who can have read access control and write access control.

8. CONCLUSION

In this paper studied about multi tenant access control and efficient revocation by utilizing with two levels of security one is R-RBAC and RRW-Access control, the first level security for allocating set of resource to tenant and it can revoke when ever required. Second level security tenant can set policies by utilizing RW-Access control.

REFERENCES

[1] Frederic F. Leymarie; Benjamin B. Kimia, 2007, The Medial Scaffold of 3D Unorganized Point Clouds, ISSN: 0162-8828, volume 29, issue 2, pp: 313 – 330.

[2] Christopher Moretti; KarstenSteinhaeuser; Douglas Thain; Nitesh V. Chawla, 2008, “Scaling up Classifiers to Cloud Computers”, Data Mining, 2008. ICDM '08. Eighth IEEE International Conference on, 1550-4786.

[3] Dancheng Li; Cheng Liu; Qiang Wei; Zhiliang Liu; Binsheng Liu, 2010, 2010 2nd International Conference on Information Engineering and Computer Science, Pages: 1 - 4

[4] QuratulainAlam; Saif U. R. Malik; Adnan Akhunzada, 2017, “A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification”, ISSN: 1556-6013 volume 12, issue 6, pp: 1259 – 1268.

[5] NidhibenSolanki; Wei Zhu; I-Ling Yen; FarokhBastani; ElhamRezvani, 2016, ”Multi-tenant Access and Information Flow Control for SaaS”, 2016 IEEE International Conference on Web Services (ICWS), pp: 99 – 106.

[6] QiongZuo; MeiyiXie; Wei-Tek Tsai, 2015, “Autonomous Decentralized Tenant Access Control Model for Sub-tenancy Architecture in Software-as-a-Service (SaaS)”, 2015 IEEE Twelfth International Symposium on Autonomous Decentralized Systems, Pages: 211 – 216.

[7] EyadSaleh; Johannes Sianipar; Ibrahim Takouna; ChristophMeinel, 2014, “SecPlace: A Security-Aware Placement

Model for Multi-tenant SaaS Environments", 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing, Pages: 596 – 602.

[8] EyadSaleh; Ibrahim Takouna; ChristophMeinel, 2013, "SignedQuery: Protecting users data in multi-tenant SaaS environments", 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Pages: 213 – 218.

[9] UsmanAslam; Hamid Mukhtar, 2012, "Data Sharing in Data-Centric Multi-tenant Software as a Service", 2012 Second International Conference on Cloud and Green Computing, Pages: 113 – 117.

[10] GanguDharmaraju, J. DivyaLalitha Sri and P. SatyaSruthi, A Cloud Computing Resolution in Medical Care Institutions for Patient's Data Collection. International Journal of Computer Engineering and Technology, 7(6), 2016, pp. 83–90.

[11] Dr. V. Goutham and M. Tejaswini, A Denial of Service Strategy To Orchestrate Stealthy Attack Patterns In Cloud Computing, International Journal of Computer Engineering and Technology, 7(3), 2016, pp. 179–186.

[12] Kuldeep Mishra, Ravi RaiChaudhary and DhereshSoni, A Premeditated CDM Algorithm In Cloud Computing Environment For FPM, Volume 4, Issue 4, July-August (2013), pp. 213-223, International Journal of Computer Engineering and Technology (IJCET).

[13] SupriyaMandhare, Dr.A.K.Sen and RajkumarShende, A Proposal on Protecting Data Leakages In Cloud Computing, Volume 6, Issue 2, February (2015), pp. 45-53, International Journal of Computer Engineering and Technology (IJCET).

[14] HadiGoudarzi; MassoudPedram, 2016, "Hierarchical SLA-Driven Resource Management for Peak Power-Aware and Energy-Efficient Operation of a Cloud Datacenter", IEEE Transactions on Cloud Computing, Volume 4, Issue 2, Pages: 222 – 236.

Author's Profiles:

M.RAJESWARI received her B.Tech Degree in Computer Science & Engineering from Bhoj Reddy Engineering College for Women, Santosh Nagar, Hyderabad, Telangana State. Affiliated to JNTUH and Pursuing M.Tech degree in Computer Science & Engineering in Khader Memorial College of Engineering & Technology, Devarakonda, Nalgonda, Telangana State, affiliated to JNTUH, Hyderabad in 2019.

E.RAVI B.Tech (CSE) M.Tech (CSE),(PhD) is having 10+ years of relevant work experience in Academics, Teaching, and Controller of Examinations. At present, he is working as an Associate Professor, In-charge of M.Tech CSE Dept, Khader Memorial College of

Engineering & Technology, Devarakonda, Nalgonda,Telangana State and utilizing his teaching skills, knowledge, experience and talent to achieve the goals and objectives of the Engineering College in the fullest perspective. He has attended seminars and workshops. He has also guided five postgraduate students. His areas of interest Data Mining, Data Warehousing, Network security, Data Structures through C Language & Cloud Computing.