International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 16
June 2018

Secure and Efficient Across Different Tenants For Sharing Of Resources in Cloud Computing

Md Imran & MdAteeq Ur Rahman
[1]*Research Scholar, Dept. of Computer Science & Engineering,*
SCET, Hyderabad, India
shadan.16081d7807@gmail.com
[2]*Professor and Head, Dept. of Computer Science & Engineering,*
SCET, Hyderabad, India
shadan.authors1@gmail.com

Abstract - *We demonstrate the utility of the scheme in a cloud deployment, which achieves fine-grained data sharing. This application implements cloud server-enabled user revocation, offering an alternative yet more efficient solution to the user revocation problem in the context of fine-grained encryption of cloud data. High user-side efficiency is another prominent feature of the application, which makes it possible for users to use resource constrained devices, e.g., mobile phones, to access cloud data. Our evaluations show promising results on the performance of the proposed scheme. Sharing of resources on the cloud may be achieved on an oversized scale since it's price effective and site freelance. Despite the promotional material close cloud computing, organizations area unit still reluctant to deploy their businesses within the cloud computing atmosphere thanks to issues in secure resource sharing. during this paper, we tend to propose a cloud resource mediation service offered by cloud service suppliers, that plays the role of trusty third party among its totally different tenants. This paper formally specifies the resource*
sharing mechanism between 2 totally different tenants within the presence of our projected cloud resource mediation service. The correctness of permission activation and delegation mechanism among totally different tenants mistreatment four distinct algorithms (Activation, Delegation,Forward Revocation and Backward Revocation) is additionally incontestable mistreatment formal verification. The performance analysis counsel that sharing of resources may be performed firmly and with efficiency across totally different tenants of the cloud. High user-side efficiency is another prominent feature of the application, which makes it possible for users to use resource constrained devices, e.g., mobile phones, to access cloud data. Our evaluations show promising results on the performance of the proposed scheme.

Index Terms— Cross Tenant Access Control(CTAC), Formal Specification and Verification, Cloud Computing, Revocation

I. INTRODUCTION

The application implements cloud server-enabled user revocation, offering an alternative yet more efficient solution to the user revocation problem in the context of fine-grained encryption of cloud data. While there square measure variety of advantages afforded by the employment of cloud computing to facilitate collaboration between users and organizations, security and privacy of cloud services and therefore

the user knowledge could deter some users and organizations from victimisation cloud services (on a bigger scale) and stay topics of interest to researchers . Typically, a cloud service supplier (CSP) provides an online interface wherever a cloud user will manage resources and settings (e.g. permitting a specific service and/or knowledge to chose users). A CSP then implements these access management options on shopper knowledge and alternative connected resources.

However, ancient access management models, like role based mostly access management , square measure usually unable to adequately take care of cross-tenant resource access requests. specifically, cross-tenant access requests create 3 key challenges. Firstly, every tenant should have some previous understanding and information regarding the external users WHO can access the resources. Thus, associate administrator of every tenant should have a listing of users to whom the access are going to be allowed.

This method is static in nature. In alternative words, tenants cannot leave and be a part of cloud as they want, that could be a typical setting for a realworld readying. Secondly, every tenant should be allowed to outline cross-tenant access for alternative tenants as and once required. Finally, as every tenant has its own administration, trust management issue among tenants will be difficult to handle, notably for a whole lot or thousands of tenants. to supply a secure cross-tenant resource access service, a fine-grained cross-tenant access management model is needed .

Thus, during this paper, we have a tendency to propose a cloud resource mediation service (CRMS) to be offered by a CSP, since the CSP plays a polar role managing totally different tenants and a cloud user entrusts the info to the CSP. we have a tendency to posit that a CRMS will offer the CSP competitive advantage, since the CSP will offer users with secure access management services in a very crosstenant access atmosphere (hereafter, we have a tendency to said as cross tenant access management - CTAC). From a privacy perspective, the CTAC model has 2 blessings. The privacy of a tenant, say T2, is protected against another tenant, say T1, and therefore the CRMS, since T2's attributes don't seem to be provided to T1. T2's attributes attributes square measure evaluated solely by the CRMS. what is more, a user doesn't offer authentication credentials to the CRMS. Therefore, the privacy of T2 is additionally protected because the CRMS has no information of the permissions that T2 is requesting from T1. The security policies outlined by T1 use pseudonyms of the permissions while not revealing the particular info to the CRMS throughout publication of the policies. To demonstrate the correctness and security of the projected approach, we have a tendency to use model checking to thoroughly explore the system and verify the finite state synchronic systems. Specifically, we have a tendency to 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, that facilitates the analysis of its reactions to a given input .

Therefore, we have a tendency to square measure ready to perceive the links between totally different system entities and the way info is processed. we have a tendency to then verify the model by translating the HLPN victimisation finite model checking. For this purpose, we have a tendency to use Satisfiability Modulo Theories Library (SMT-Lib) and Z3 problem solver [19], [9]. we have a tendency to remark that such formal verification has antecedently been

accustomed judge security protocols like in. we have a tendency to regard the key contributions of this paper to be as follows: we have a tendency to gift a CTAC model for collaboration, and therefore the CRMS to facilitate resource sharing amongst varied tenants and their users. Y we have a tendency to additionally gift four totally different algorithms within the CTAC model, namely: activation, delegation, forward revocation and backward revocation. Y we have a tendency to then offer a close presentation of modeling, analysis and automatic verification of the CTAC model victimisation the finite Model Checking technique with SMTLIB and Z3 problem solver, so as to demonstrate the correctness and security of the CTAC model.

II. Related Works

The revolutionary idea of package outlined Networks (SDNs) doubtless provides versatile and well-managed next-generation networks. All the promotional material encompassing the SDNs is preponderantly owing to its centralized management practicality, the separation of the management plane from the info forwarding plane, and sanctioning innovation through network programmability. Despite the promising design of SDNs, security wasn't thought-about as a part of the initial style. Moreover, security considerations square measure doubtless increased considering the logical centralization of network intelligence. moreover, the protection associate degreed responsibility of the SDN has for the most part been a neglected topic and remains an open issue. The paper presents a broad summary of the protection implications of every SDN layer/interface. This paper contributes additional by fashioning a up to date layered/interface taxonomy of the rumored security vulnerabilities, attacks, and challenges of SDN. we tend to additionally highlight and analyze the potential threats on every layer/interface of SDN to assist style secure SDNs. Moreover, the following paper contributes by presenting the progressive SDNs security solutions. The categorization of solutions is followed by a critical appraisal and discussion to plot a comprehensive thematic taxonomy. we tend to advocate the assembly of secure and dependable SDNs by presenting potential necessities and key enablers. Finally, in a trial to anticipate secure and dependable SDNs, we tend to gift the continuing open security problems, challenges and future analysis directions.

The design of advanced system networks is of preponderant importance as a result of their increasing role within the implementation of Cyber– Physical Systems (CPS) and package outlined Networking (SDN) involving integrated ICT and physical parts and devices. However, the planning of such networks effectively encounters difficulties which require to be resolved. These difficulties stem from the extremely distributed and heterogeneous nature of SDN and therefore the extent of intelligence, responsibility and security that they have to demonstrate throughout their operation. the planning and verification ways for developing secure and dependable system networks is important and will be thought-about at the planning level to ensure security and mitigate safety threats, on remote monitored and managed networks. Especially, with the quick growth of SDN and therefore the integration with 5G network architectures [1], the planning of networks enters during a new era and makes necessary a careful investigation of the new security and responsibility risks, that haven't been relevant in inheritance systems. one in all the challenges of future

networks is to develop SDN capabilities tailored to cycles/second and drive the reconfiguration of those capabilities through network configuration specifications embedded in essential infrastructures. SDN permits network programmability and management to be decoupled from the forwarding plane and therefore the forwarding plane to be directly programmable by the management plane. during this paper, we tend to gift a model driven approach to {the style|the planning|the look} and verification of secure and dependable SDN networks that's supported S&D network design patterns (referred to as S&D patterns within the remainder of this paper). These patterns will be wont to style and/or verify SDN network infrastructures and establish appropriate ways and nodes which will guarantee S&D properties. S&D patterns will be wont to style SDN infrastructures, and verify additionally the kind, location and property of finish nodes with forwarding devices. At the management layer, S&D patterns will guarantee secure property between the controllers and therefore the programmable switches. during this paper, we tend to provides a elaborate description of the theme for specifying S&D patterns and their use for the planning of S&D protective SDN networks. the most contribution of the approach is that our approach encodes styles of network topologies, that square measure tested to satisfy S&D properties, as style patterns. additionally, S&D patterns will be used for the definition of best ways that square measure ready to guarantee S&D properties in deployed networks. a primary definition of our pattern-based approach for planning reliable cyber-physical systems was given in [2]. This paper extends the initial approach by developing a pattern framework during which we will measure and emulate S&D feasible patterns on SDN-based network styles. It additionally presents associate degree application framework during which S&D patterns will insert and modify flow rules through the controller to the programmable switches of SDN infrastructures. the rest of this paper is organized as follows. In Section a pair of an outline of connected work is given. In Section three, we tend to gift the schema of the pattern execution kind. In Section four, we tend to introduce abstract specification instances of patterns with relation to confidentiality and convenience encoded additionally to a rulebased reasoning language. In Section five, we tend to propose associate degree implementation framework during which S&D network patterns will be applied so as to style and verify SDN network architectures. In Section half-dozen, we tend to emulate our projected network patterns for {the style|the planning|the look} of wireless SDN-based network architectures ready to offer security against physical layer attacks and failures at design or at runtime in hostile environments.

2.1 Existing System

Traditional access management models, like role based mostly access management, ar typically unable to adequately manage cross-tenant resource access requests.

However, takes the decidability downside as 1st order logic formula and decides its satisfiability supported the decidable background theory. There ar variety of theories supported by the SMT solvers, like equality and uninterpreted functions, linear arithmetic over rationals, linear arithmetic over integers, non-linear arithmetic over reals, over arrays, bit vectors, and mixtures.

The SMT-Lib provides a typical input platform for variety of solvers employed in the verification of systems. activity specifications of a system may be

diagrammatic exploitation abstract models. The SMT solvers ar then accustomed perform delimited model checking to explore a delimited symbolic execution of the model.

III. PROPOSED SYSTEM

We gift a CTAC model for collaboration, and therefore the CRMS to facilitate resource sharing amongst numerous tenants and their users. We additionally gift four totally different algorithms within the CTAC model, namely: activation, delegation, forward revocation and backward revocation. We then offer a close presentation of modeling, analysis and automatic verification of the CTAC model victimisation the finite Model Checking technique with SMTLIB and Z3 problem solver, so as to demonstrate the correctness and security of the CTAC model.

Role primarily based access management (RBAC) permits fine-grained access management (and usually in a very single domain). totally different extensions of RBAC are planned within the literature to support multi-domain access management. These approaches consider one body to blame for maintaining cross-domain policies.

IV. System Architecture

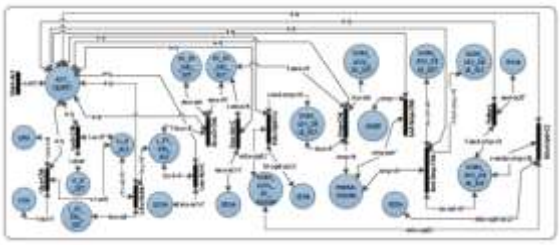

Figure 1: A HLPN Model for the process of activating a permission p_i in a cross-tenant environment.

Service-oriented design offers a versatile paradigm for info flow among collaborating organizations. As info moves out of a corporation boundary, varied security considerations could arise, like confidentiality, integrity, and genuineness that must be addressed . Moreover, confirmative the correctness of the communication protocol is additionally a very important issue.

This paper focuses on the formal verification of the xDAuth protocol, that is one in all the distinguished protocols for identity management in cross domain situations. we've got shapely {the info|the knowledge|the data} flow of xDAuth protocol victimization high-level Petri nets to grasp the protocol information flow during a distributed setting. we have a tendency to analyze the foundations of knowledge flow victimization Z language, whereas Z3 SMT convergent thinker is employed for the verification of the model. Our formal analysis and verification results reveal the very fact that the protocol fulfills its meant purpose and provides the safety for the outlined protocol specific properties, e.g., secure secret key authentication, and wall security policy and secrecy specific properties, e.g., confidentiality, integrity, and genuineness.

Cryptographic protocols kind the backbone of our digital society. sadly, the safety of various essential elements has been neglected. As a consequence, attacks

have resulted in loss, violations of private privacy, and threats to democracy. This thesis aids the secure style of cryptographical protocols and facilitates the analysis of existing schemes. Developing a secure cryptographical protocol is game-like in nature, and a decent designer can take into account attacks against key elements. not like games, however, AN resister isn't ruled by the foundations and will deviate from expected behaviours. Secure cryptographical protocols ar thus notoriously troublesome to outline. consequently, cryptographical protocols should be scrutinised by consultants victimization procedures which will appraise security properties. This thesis advances verification techniques for cryptographical protocols victimization formal strategies with a stress on automation.

4.1 Module Description:

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.

V. Conclusion

In this paper, we tend to planned a cross-tenant cloud resource mediation service (CRMS), which might act as a trusted-third party for fine-grained access management in a very cross-tenant setting. for instance, users United Nations agency belong to Associate in Nursing intra-tenant cloud will permit alternative cross-tenant users to activate a permission in their tenant via the CRMS. we tend to conjointly given a proper model CTAC with four algorithms designed to handle the requests for permission activation. we tend to then shapely the algorithms victimisation HLPN, formally analyzed these algorithms in Z language, and verified them victimisation Z3 Theorem Proving thinker. The results obtained once capital punishment the thinker incontestible that the declared formula specific access management properties were happy and permits secure execution of permission activation on the cloud via the CRMS.This embody a comparative analysis of the planned CTAC model with alternative progressive cross domain access management protocols victimisation real-world evaluations. for instance, one may implement the protocols in a very closed or tiny scale setting, like a department among a university. this could permit the researchers to guage the performance, and doubtless (in)security, of the varied approaches below totally different real-world settings.

References

[1] Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., & Khan, S. U. (2016). Secure and dependable software defined networks. Journal of Network and Computer Applications, 61, 199-221.
[2] Alam, Q., Tabbasum, S., Malik, S., Alam, M., Tanveer, T., Akhunzada, A., Khan, S., Vasilakos, A. and Buyya, R., (2016). Formal Verification of the xDAuth Protocol. IEEE Transactions on Information Forensics and Security, 11(9), pp. 1956-1969.
[3] Ali, M., Malik, S. and Khan, S., DaSCE: Data Security for Cloud

Environment with Semi-Trusted Third Party.
[4] Barrett, C., Conway, C.L., Deters, M., Hadarean, L., Jovanovi, D., King, T., Reynolds, A. and Tinelli, C., 2011, July. Cvc4. In International Conference on Computer Aided Verification (pp. 171-177). Springer Berlin Heidelberg.
[5] Bofill, M., Nieuwenhuis, R., Oliveras, A., Rodrguez-Carbonell, E. and Rubio, A., 2008, July. The barcelogic SMT solver. In International Conference on Computer Aided Verification (pp. 294-298). Springer Berlin Heidelberg.
[6] Bruttomesso, R., Cimatti, A., Franzn, A., Griggio, A. and Sebastiani, R., 2008, July. The mathsat 4 smt solver. In International Conference on Computer Aided Verification (pp. 299-303). Springer Berlin Heidelberg.
[7] Choo, K.K., 2006. Refuting security proofs for tripartite key exchange with model checker in planning problem setting. In 19th IEEE Computer Security Foundations Workshop (CSFW'06) (pp. 12-pp). IEEE.
[8] 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.
[9] De Moura, L. and Bjørner, N., 2011. Satisfiability modulo theories: introduction and applications. Communications of the ACM, 54(9), pp.69-77.
[10] Dutertre, B. and De Moura, L., 2006. The yices smt solver. Tool paper at http://yices. csl. sri. com/tool-paper. pdf, 2(2).
[11] 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.