ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

# Resource Sharing Between Tenants in the Cloud Using Cross Tenant Access Control (CTAC) Model: Formal Specification and Verification

Nihar Nikhat Sultana[1], Dr. Rekha Patil[2]

PG Student, Department of CSE, PDA College of Engineering, Kalaburagi, Karnataka, India[1]

Professor, Department of CSE, PDA College of Engineering, Kalaburagi, Karnataka, India[2]

**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

## I. INTRODUCTON

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 the CRMS during publication of the policies.

DOI: 10.15680/IJIRCCE.2018.0606025

We 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].

## II. 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 discuss 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.

DOI: 10.15680/IJIRCCE.2018.0606025

## III. PROPOSED WORK

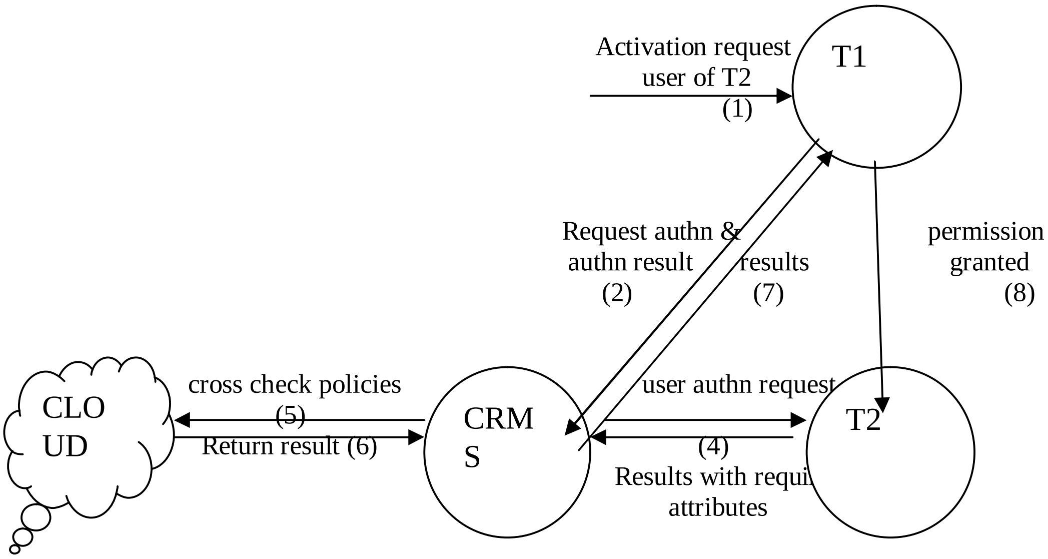


**Fig1: System Architecture**

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.

## IV. IMPLIMENTATION AND RESULTS

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 the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve change over 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.

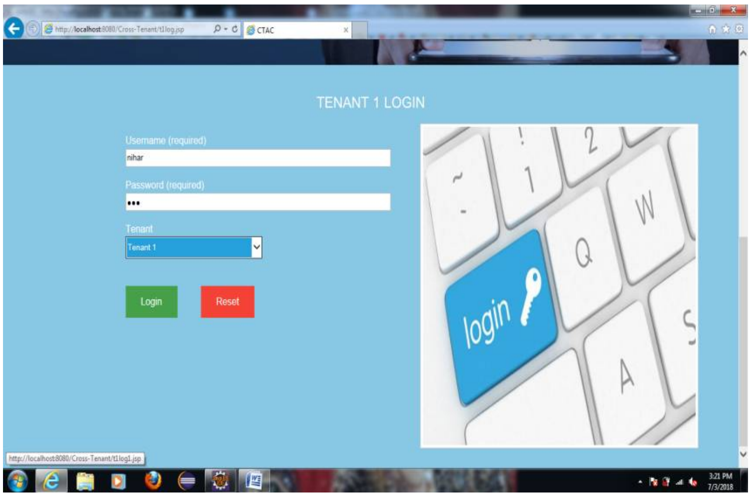
**CRMS responsibilities:** The CRMS receives the permission-activation request redirected from T1. Once an access request is received, the CRMS evaluates the request on the pre-published policies and responds to T1.

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

An intra tenant user, after the activation of the permission, has delegated the request permission to a tenant (i.e., an approved delegation must exist for a particular tenant). There are two types of delegation that exists on the system, namely: user level delegation and tenant level delegation. Failure of one of these two cases will result in checking of the other case. If no one 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 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 is 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.



http://localhost:8080/Cross-Tenant/t1log.jsp

CTAC

TENANT 1 LOGIN

Username (required): nihar

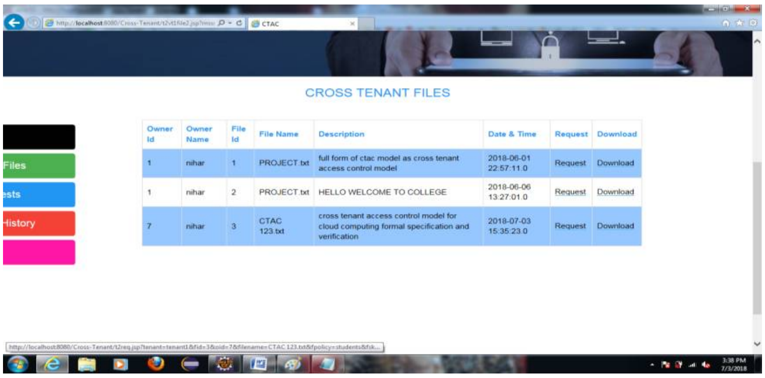
Password (required): •••

Tenant: Tenant 1

**Fig2: Login Page**

The above figure2 shows the Login page where the user have to enter his username and password. Then select the Login option.

DOI: 10.15680/IJIRCCE.2018.0606025



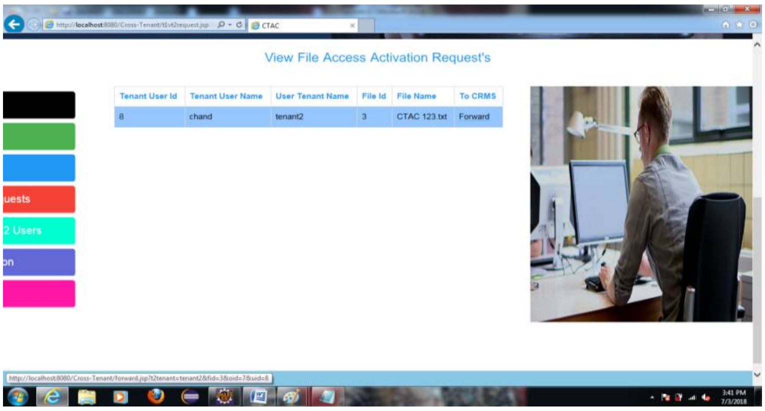
CROSS TENANT FILES

| Owner Id | Owner Name | File Id | File Name | Description | Date & Time | Request | Download |
|---|---|---|---|---|---|---|---|
| 1 | nihar | 1 | PROJECT.txt | full form of ctac model as cross tenant access control model | 2018-06-01 22:57:11.0 | Request | Download |
| 1 | nihar | 2 | PROJECT.txt | HELLO WELCOME TO COLLEGE | 2018-06-06 13:27:01.0 | Request | Download |
| 7 | nihar | 3 | CTAC 123.txt | cross tenant access control model for cloud computing formal specification and verification | 2018-07-03 15:35:23.0 | Request | Download |

http://localhost:8080/Cross-Tenant/t2req.jsp?tenant=tenant1&fid=3&oid=7&filename=CTAC 123.txt&fpolicy=students&fsk...
3:38 PM
7/3/2018

**Fig3: Request Process**

In the figure 3 the T2 (user) sends request to T1 (admin) for accessing the resource which the T1 was uploaded.


http://localhost:8080/Cross-Tenant/t1vt2request.jsp
CTAC
uests
2 Users
on

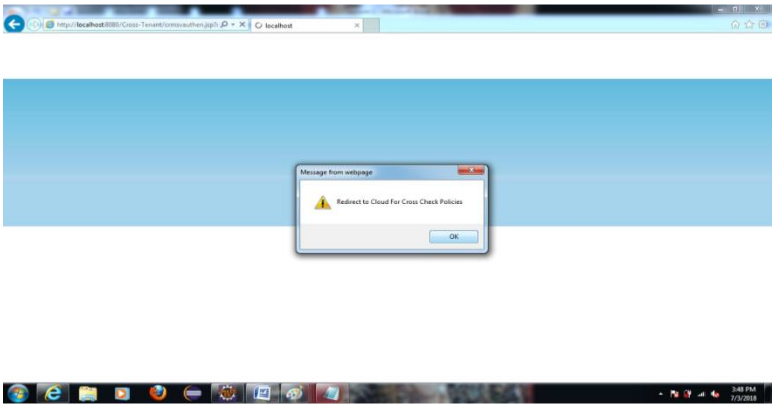
View File Access Activation Request's

| Tenant User Id | Tenant User Name | User Tenant Name | File Id | File Name | To CRMS |
|---|---|---|---|---|---|
| 8 | chand | tenant2 | 3 | CTAC 123.txt | Forward |

http://localhost:8080/Cross-Tenant/forward.jsp?t2tenant=tenant2&fid=3&oid=7&uid=8
3:41 PM
7/3/2018

**Fig4: Authentication**

After receiving the access request from tenant T2, the tenant T1 forwards the request to the proposed CRMS for authentication of the user as shown in figure4.



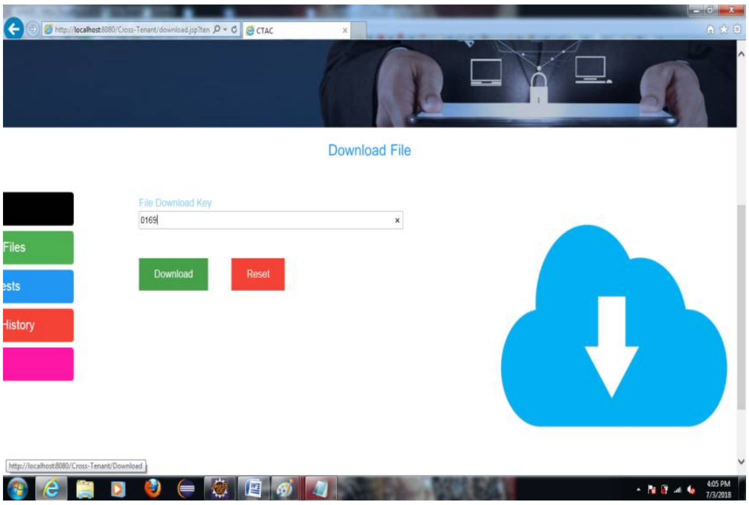
Message from webpage

Redirect to Cloud For Cross Check Policies

**Fig5: Cross Check Policies**

DOI: 10.15680/IJIRCCE.2018.0606025

CRMS receives the request from tenant T1 for authentication, then it redirects the access request to the Cloud for cross check policies. As shown in the figure, the cloud verifies and redirects cross check policies to CRMS.


http://localhost:8080/Cross-Tenant/download.jsp?ten
CTAC
Download File
Files
ests
History
Download
Reset
http://localhost:8080/Cross-Tenant/Download
4:05 PM
7/3/2018

File Download Key: 0169

**Fig6: Download File**

After receiving the permission activation for access the resource, a private key is sent to user's mail. As shown in the figure, to download the file user needs to enter the private key then select the download button.

## V. CONCLUSION

We proposed across tenant cloud resource mediation service (CRMS), which can act as a trusted-third party among different tenants for a fine grained access control in a cross tenant environment. Hence we concluded that a formal model CTAC with four algorithms intended to deal with the requests for permission activation. The outcomes got consequent to executing the solver demonstrated that the stated algorithm specific access to control properties were satisfied and secure execution of permission activation on the cloud in the presence of the CRMS.

In future it can be extended of the proposed CTAC model with other state of the art cross domain access control conventions utilizing real assessments. For example, one could execute the conventions in a closed or small scale condition, for example, a section inside a college. This would enable the specialists to assess the execution, what's more, possibly (in) security, of the different methodologies under distinctive real settings.

## REFERENCES

[1] 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.

[2] 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).

[3] 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).

[4] Sayler, A., Keller, E. and Grunwald, D., 2013. Jobber: Automating inter-tenant trust in the cloud. In Presented as part of the 5th USENIX Workshop on Hot Topics in Cloud Computing.

[5] 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.

[6] Ali, M., Malik, S. and Khan, S., DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party.

[7] 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.

[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. knowinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical report, EECS Department, University of California, Berkeley, Feb 2009.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] De Moura, L. and Bjørner, N., 2011. Satisfiability modulo theories: introduction and applications. Communications of the ACM, 54(9), pp.69-77.
[14] Murata, T., 1989. Petri nets: Properties, analysis and applications. Proceedings of the IEEE, 77(4), pp.541-580.
[15] 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.
[16] 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.
[17] SMT-Lib. http://smtlib.cs.uiowa.edu/, 2015.
[18] Zhang, Y., Patwa, F., Sandhu, R. and Tang, B., 2015, August. Hierarchical secure information and resource sharing in open stack community cloud. In Information Reuse and Integration (IRI), 2015 IEEE International Conference on (pp. 419-426). IEEE.
[19] Zhao, G., Ba, Z., Wang, X., Zhang, Y., Huang, C. and Tang Y., 2016. Constructing Authentication Web in Cloud Computing. Security and Communication Networks, 9(15), pp. 2843-2860.
[20] Lin, Y., Malik, S.U., Bilal, K., Yang, Q., Wang, Y. and Khan, S.U., 2016. Designing and Modeling of Covert Channels in Operating Systems. IEEE Transactions on Computers, 65(6), pp.1706-1719.
[21] 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.