RESEARCH REVIEW JOURNALS
Volume-03
Issue-07
July-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Resource Handling in Cloud Computing Environment using Cross Tenant Access Control (CTAC) Model

[*1]D. Dhanya; [2]R. S. Akhila; [3]Aparna Jose & [4]R. P. Bincy Raj

[*1]*Assistant Professor, School of Computer Science & Engineering, Mar Ephraem College of Engineering & Technology, Malankara Hills, Elavuvilai, KanyaKumari (India)*

[2,3,4]*BE Student, School of Computer Science & Engineering, Mar Ephraem College of Engineering & Technology, Malankara Hills, Elavuvilai, KanyaKumari (India)*

ARTICLE DETAILS

Article History
Published Online: 05 July 2018

Keywords
Cloud computing, resource handling, Tenant Management ,CRMS, TAC

[*]**Corresponding Author**
Email: dhanvis[at]gmail.com

ABSTRACT

As cloud computing becomes more flexible and effective in terms of economy, data owners are motivated to outsource their complex data system from local size to commercial public cloud. Sharing of resources on the cloud can be achieved on large scale since it is cost effective and location independent. In this paper, we propose a cloud resources mediation service offered by cloud service providers, which place 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 proposed cloud resource meditation service. The permission activation and delegation mechanism among different tenants are demonstrated using four modules tenant management, CRMS (Cloud Resource Mediation Service), TAC (Tenant Access Control) and resource handling.

1. Introduction

Over the past 60 years, computing technology has undergone a series of platform changes and has gone through five generations of development, each lasting from 10 to 20 years. But the concept of delivering computing resources through a global network is rooted in the sixties.

One of the first milestones for cloud computing was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The services are delivered as a service to the user through the internet. The next development was amazon web services in 2002, which provides cloud based services such as storage, computation etc. Then in 2006, amazon launched its Elastic Compute cloud (EC2) as a commercial web service where individuals and companies can rent computers to build their own applications

Cloud storage is one of the possible services that can be provided to individuals and organizations through the cloud computing model. Cloud storage is a form of networked online storage that differs from traditional storage methods in several ways. Traditionally, portable media such as optical discs and flash drives allow end users to access data directly, while personal computers and other devices contain their own storage devices. Alternatively, data stored on the cloud is accessed exclusively through network resources. Corporations traditionally own their own computer resources that their users access over their private network. With cloud storage, an individual or an organization does not own or specify the hardware used or the physical location of the data. As the user relinquishes the control over their data to the cloud service provider, problems concerning data integrity and data availability arises.

The objective of this work is to achieve access control and efficient revocation in cross-tenant cloud storage. In this paper, two different access models are proposed, CRMS model and CSP. The CSP is responsible for verifying the user's identity and making access control decisions. The correctness of permission activation and delegation mechanism among different tenants uses a distinct algorithm.

This paper specifies the resource sharing between two different tenants. The cloud resource meditation services are offered by the cloud service providers which in turn are provided by CTAC. The permission activation and delegation mechanism among different tenants implemented using four distinct modules tenant management, CRMS (Cloud Resource Mediation Service), TAC (Tenant Access Control), resource handling.

A tenant provider can define access control for each tenant. Access control gives or set privileges over cloud storage server. But in this scenario, after giving set of privileges to the tenant ,if the tenant is not willing to use the services, then the tenant provider must revoke, and after revoking the tenant the storage must be re allocate to other tenant or to the new tenant. A multi tenancy a storage server is partitioned into blocks, after each block allocate to tenant for security reason every block signed with tenant secret key.

The proposed CRMS act as a trusted-third party in this cross-tenant environment. For example, users who belong to an intra-tenant cloud can allow other cross-tenant users to activate permission in their tenant via the CRMS and presented a formal model CTAC with four modules designed to handle the requests for permission activation. Then modeled the algorithms using the HLPN, formally analyzed these algorithms in Z language. The obtained results allow secure execution of permission activation on the cloud via the CRMS.

2. Literature Survey

This section includes the existing literatures related to the proposed work.

Akhunzada A et.al [1] proposed the secure and dependable software-defined networking empowers network operators with more flexibility to program their networks. With sdn, network management moves from codifying functionality in terms of low-level device configurations to building software that facilitates network management and debugging. By separating the complexity of state distribution from network specification, sdn provides new ways to solve long-standing problems in networking routing, for instance while simultaneously allowing the use of security and dependability techniques, such as access control or multi-path.

Alam Q et.al [2] suggested the formal verification of the xDAuth protocol in which the Service-oriented architecture offers a flexible paradigm for information flow among collaborating organizations. As information moves out of an organization boundary, various security concerns may arise, such as confidentiality, integrity, and authenticity that need to be addressed. Moreover, verifying the correctness of the communication protocol is also an important factor. This work focuses on the formal verification of the xDAuth protocol, which is one of the prominent protocols for identity management in cross domain scenarios. And has modeled the information flow of xDAuth protocol using high-level Petri nets to understand the protocol information flow in a distributed environment and it analyze the rules of information flow using Z language, while Z3 SMT solver is used for the verification of the model. This formal analysis and verification results reveal the fact that the protocol fulfills its intended purpose and provides the security for the defined protocol specific properties.

Ali M et.al [3] presented the data security for cloud environment with semitrusted third party in which off-site data storage is an application of cloud that relieves the customers from focusing on data storage system. 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. Wholesale of data by cloud service provider is yet another problem that is faced in the cloud environment. Consequently, high-level of security measures is required and the data security has been proposed for cloud environment with semi-trusted third party Data Security for Cloud Environment (DaSCE), a data security system that provides (a) key management (b) access control, and (c) file assured deletion. The performance is evaluated based on the time consumed during various operations, access control formally model and analyze the working of DaSCE using High Level Petri Nets (HLPN), and file assured deletion 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.

Bofill M et.al [4] proposed the system description of the Barcelogic SMT solver, which implements all techniques that group, has been developing over the last four years as well as state-of-the-art features developed by other project groups and also pay special attention to the theory solvers and to functionalities that are not common in SMT solvers.

Bruttomesso R et.al [5] presented the MATHSAT 4 SMT Solver, a state-ofthe-art SMT solver. MATHSAT 4 handles several useful theories: equality and uninterrupted functions, difference logic, linear arithmetic, and the theory of bitvectors. It was explicitly designed for being used in formal verification, and thus provides functionalities which extend the applicability of SMT in this setting. In particular: model generation (for counterexample reconstruction), model enumeration (for predicate abstraction), an incremental interface (for BMC), and computation of unsatisfiable cores and craig interpellants (for abstraction refinement)

Choo K K et.al [6] considered the refuting security proofs for tripartite key exchange with model checker in planning problem setting. This work includes encoding of a simplified version of the Canetti and Krawczyk (2001) formalism using Asynchronous Product Automata (APA) and then uses a model checker tool, Simple Homomorphism Verification Tool (SHVT), to perform state-space analysis on our automata in the setting of planning problem. As a case study, two tripartite key exchange protocols of Hitchcock, Boyd, and Gonzalez Nieto (2004) are considered in which it carry claimed security proofs in the Canetti and Krawczyk (2001) model and refute their proofs of security by pointing out previously unpublished flaws in the protocols using SHVT and it points out corresponding flaws in the refuted proofs.

Choo K K et.al [7] presented the cloud cryptography: theory, practice and future research directions in which cloud computing is a convenient way of accessing services, resources and applications over the Internet, shifts the focus of industries and organizations away from the deployment and day-to-day running of their IT facilities by providing an on-demand, self-service, and pay-as-you-go business model. It is, therefore, unsurprising that cloud computing has continued to increase in popularity in recent times. While cloud computing provides various benefits to users, there are underlying security and privacy risks.

Dutertre B & De Moura [8] suggested the YICES SMT solver in which SMT stands for Satisfiability Modulo Theories (SMT). An SMT solver decides the satisfiability of propositionally complex formulas in theories such as arithmetic and uninterpreted functions with equality. SMT solving has numerous applications in automated theorem proving, in hardware and software verification, and in scheduling and planning problems. This paper describes YICES, an efficient SMT solver developed at SRI International. YICES supports a rich combination of firstorder theories that occur frequently in software and hardware modeling: arithmetic, uninterpreted functions, bit vectors, arrays, recursive data types, and more. YICES is the main decision procedure used by the SAL model checking environment, and it is being integrated to the PVS theorem proved.

Lin Y et.al [11] considered the designing and modeling of convert channels in operating system. Covert channels are widely considered as a major risk of information leakage in various operating systems, such as desktop, cloud, and mobile systems. The existing works of modeling covert channels have mainly focused on using Finite State Machines (FSMs) and their transforms to describe the process of covert channel transmission. However, a FSM is rather an abstract model, where information about the shared resource, synchronization, and encoding/decoding cannot be presented in the model, making it difficult for researchers to realize and analyze the covert channels. In this paper, High-Level Petri Nets (HLPN) is used to model the structural and behavioral properties of covert channels and it issued to model the classic covert channel protocol. Moreover, the results from the analysis of the HLPN model are used to highlight the major shortcomings and interferences in the protocol. Furthermore, this work proposes two new covert channel models, namely: (a) Two Channel Transmission Protocol (TCTP) model and (b) Self-Adaptive Protocol (SAP) model.

Liu J K et.al [12] projected the new fine-grained Two-Factor Authentication (2FA) access control system for web-based cloud computing services. Specifically, in this 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, this work also carries out a simulation to demonstrate the practicability of our proposed 2FA system.

3. Proposed model

In the proposed method, model checking is used to exhaustively explore the system and verify the finite state concurrent systems. The three algorithms and DFD (Data Flow Diagram) are used for the modeling and analysis of the model for collaboration, and the CRMS to facilitate resource sharing among the various tenants and their users.The algorithms in this model are tenant management, CRMS (Cloud Resource Mediation Service), TAC (Tenant Access Control) and resource handling.

The fact that the cloud server may leak data or information to unauthorized entities or even be hacked. It follows network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In cross-tenant scenario a tenant provider can allow multiple tenants to outsource their data to the cloud storage server, due to security issues the data must be encrypted before uploading to the cloud storage server, in multi-tenancy one tenant can't access another tenant data.

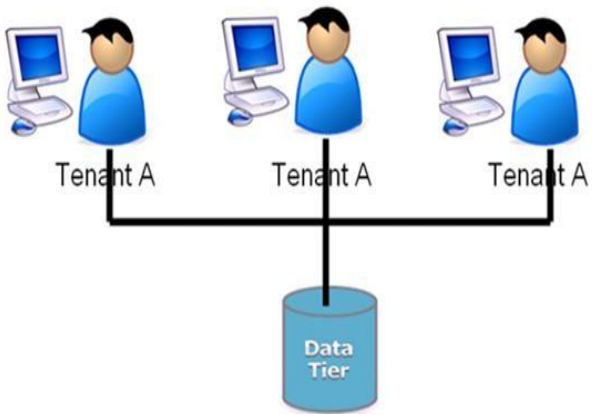


Fig . 1.1 Fine-grained cross tenant approach

Each user gets his own portion of database on the primary key.A tenant provider can define access control for each tenant, access control means giving set privileges over cloud storage server, but in this scenario after giving set of privileges to tenant if they not willing to use services then the tenant provider must revoke, and after revoking the tenant the storage must be re allocate to other tenant or new tenant. In multi tenancy a storage server is partitioned into blocks, after each block allocate to tenant for security reason every block signed with tenant secrete key. The modules are

1. Tenant management
2. CRMS (Cloud resource Mediation Service)
3. TAC (Tenant access control)
4. Resource handling

1.Tenant management

In the first module, the data owner module (tenant) is developed. Owner will sign up and wait for the approval key of admin. After getting key owner can login using the key, and upload any records related to users medical Information on the cloud and the data owner will check the progress status of the file upload by him/her. It needed to store a large amount of data and shared in cloud system. In this algorithm, the entity is in charge of access data and executing encrypt operation. And it uploads the encrypted text to CSP. After the completion, the owner logout the session

2. CRMS (Cloud Resource Mediation Service)

It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. It would like to find out as much sensitive contents as possible. In this project, it provides cipher text storage and transmission services. This module also includes the development of admin module process. Admin will login on the admin's page. Owner will check the pending requests of any of the above person. After accepting the request from the above person owner will generate master key for encrypt and Secret key for decrypt.

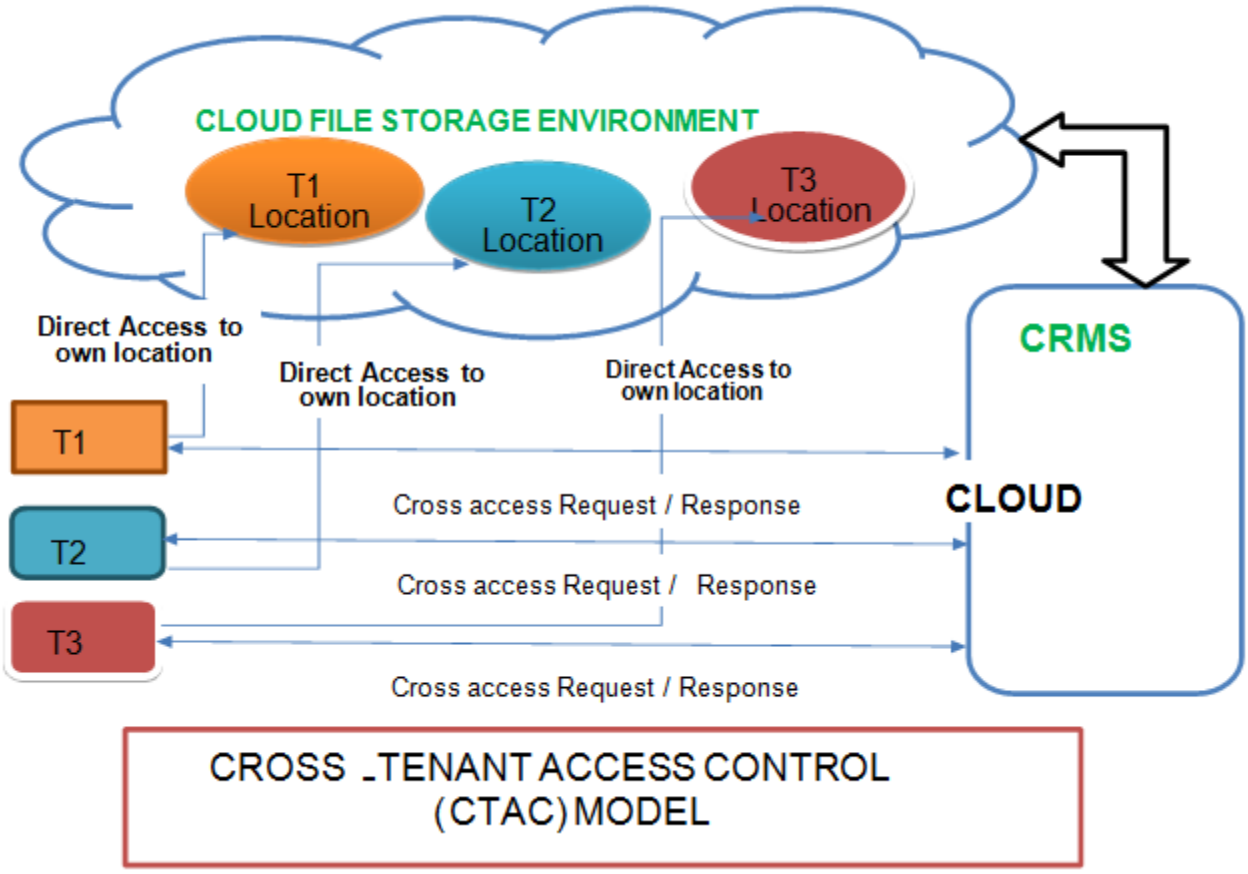
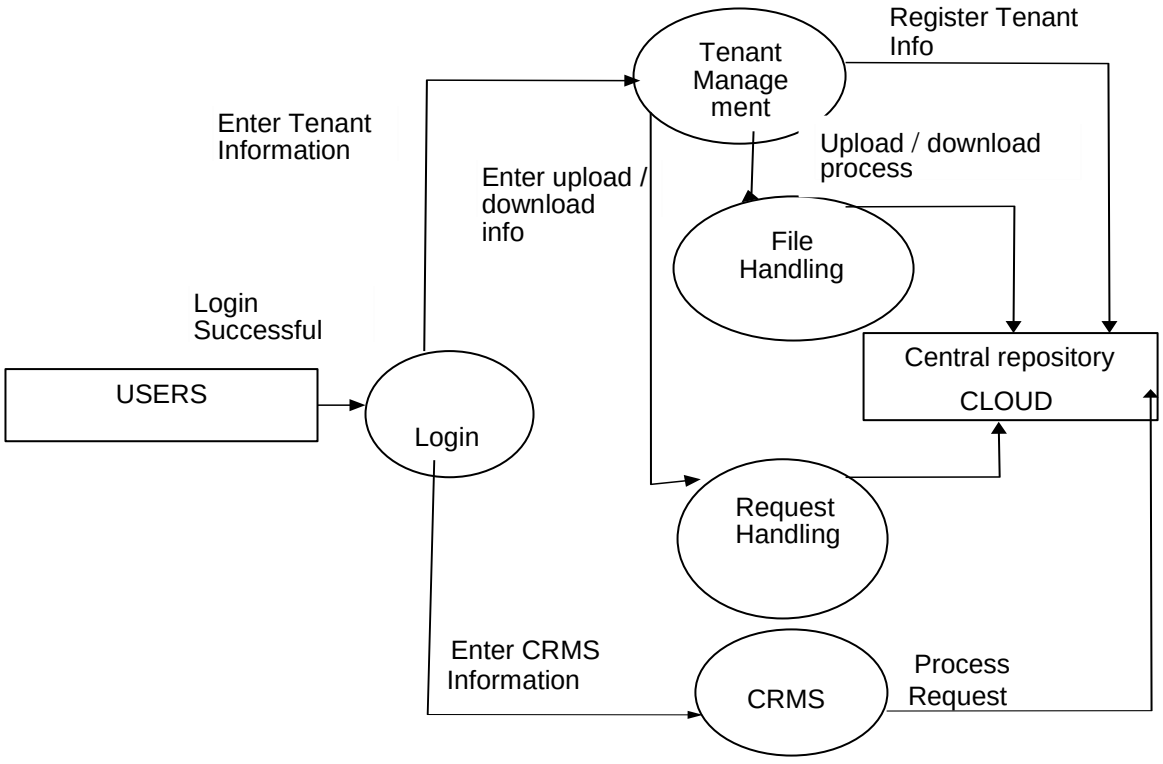
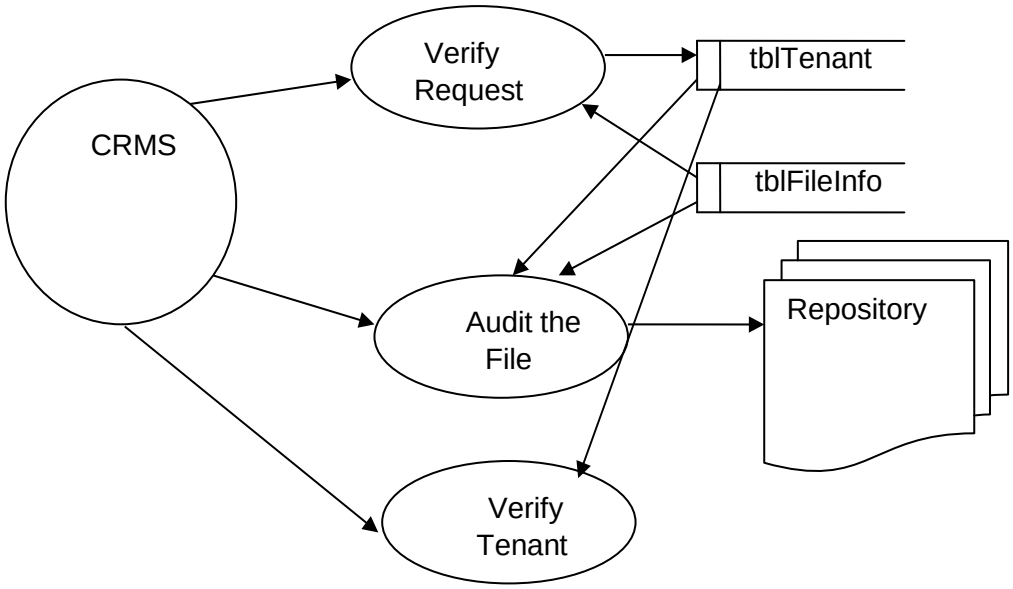


Fig 1.2 Cross tenant access control model





3. TAC (Tenant Access Control)

It is a completely trusted entity and accepts the user enrolment in cloud computing. It can also execute setup and key gen operations of the proposed scheme. User requests for decrypt key to the admin. After getting the key from admin, user can access to the resources without any secured details. After the process, is completed the user can logout of the session.

4. Resource handling

The resources in the cloud are handled in an efficient and secure way between tenants. The encrypted data that is uploaded by the user and tenants are stored in the database. With cloud storage, an individual or an organization does not own or specify the hardware used or the physical location of the data. As the user relinquishes the control over their data to the cloud service provider, problems concerning data integrity and data availability arises. In multi tenancy a storage server is partitioned into blocks. Each block is allocated to tenant. For security reason every block is been signed with the tenant secret key.

4. Results and Discussions

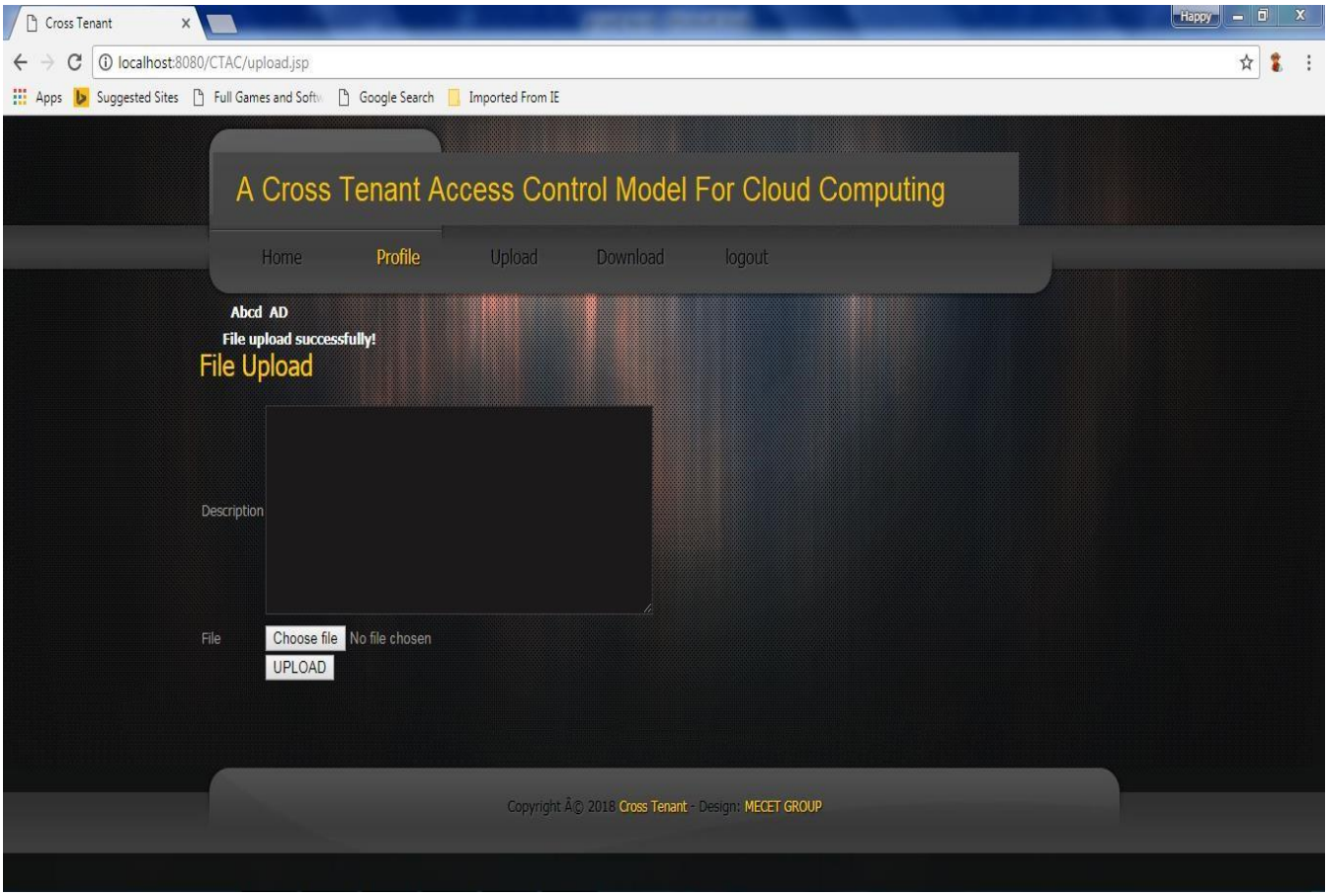


Fig 1.3 Tenant file uploading page

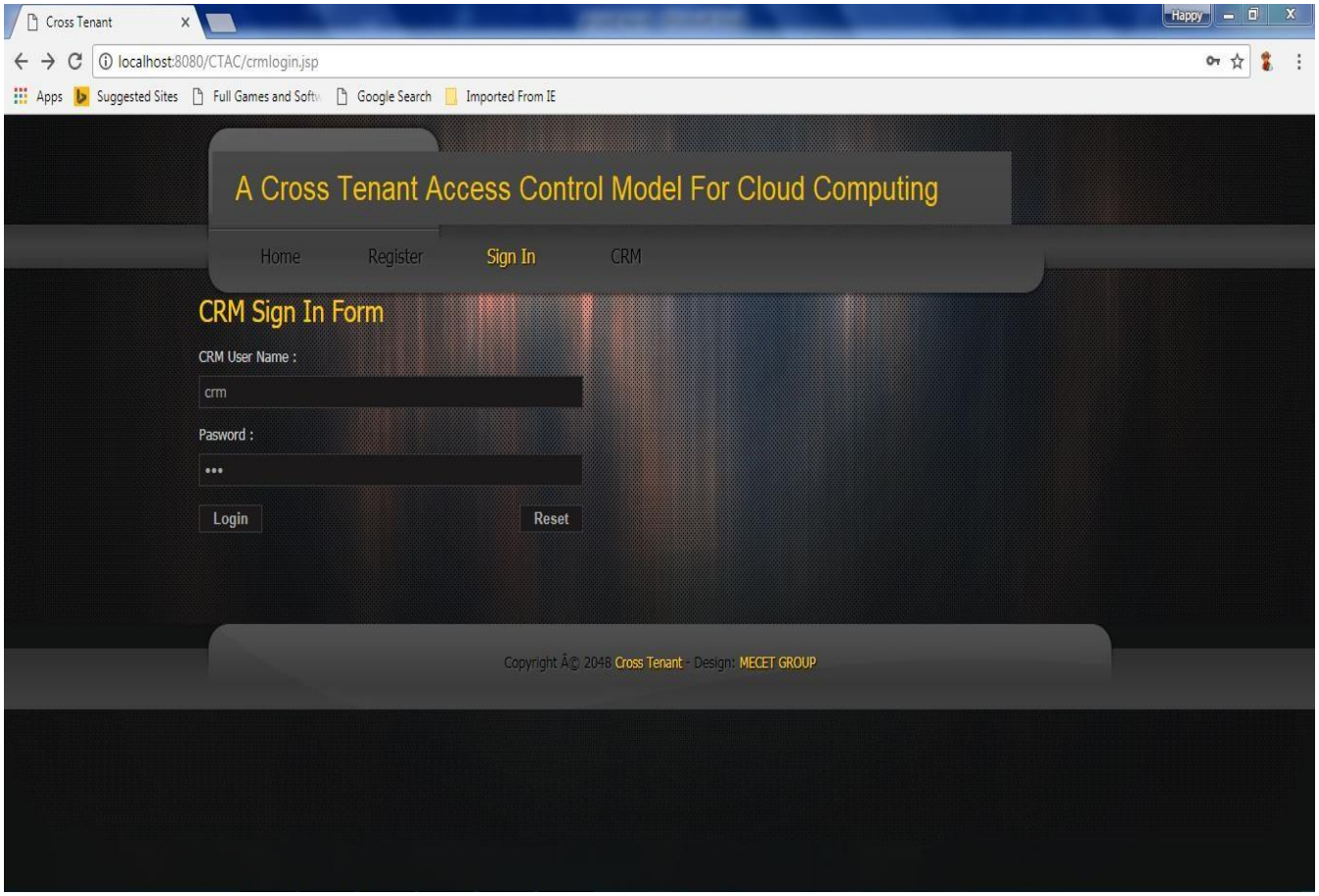


Fig 1.4 Login page of CRM

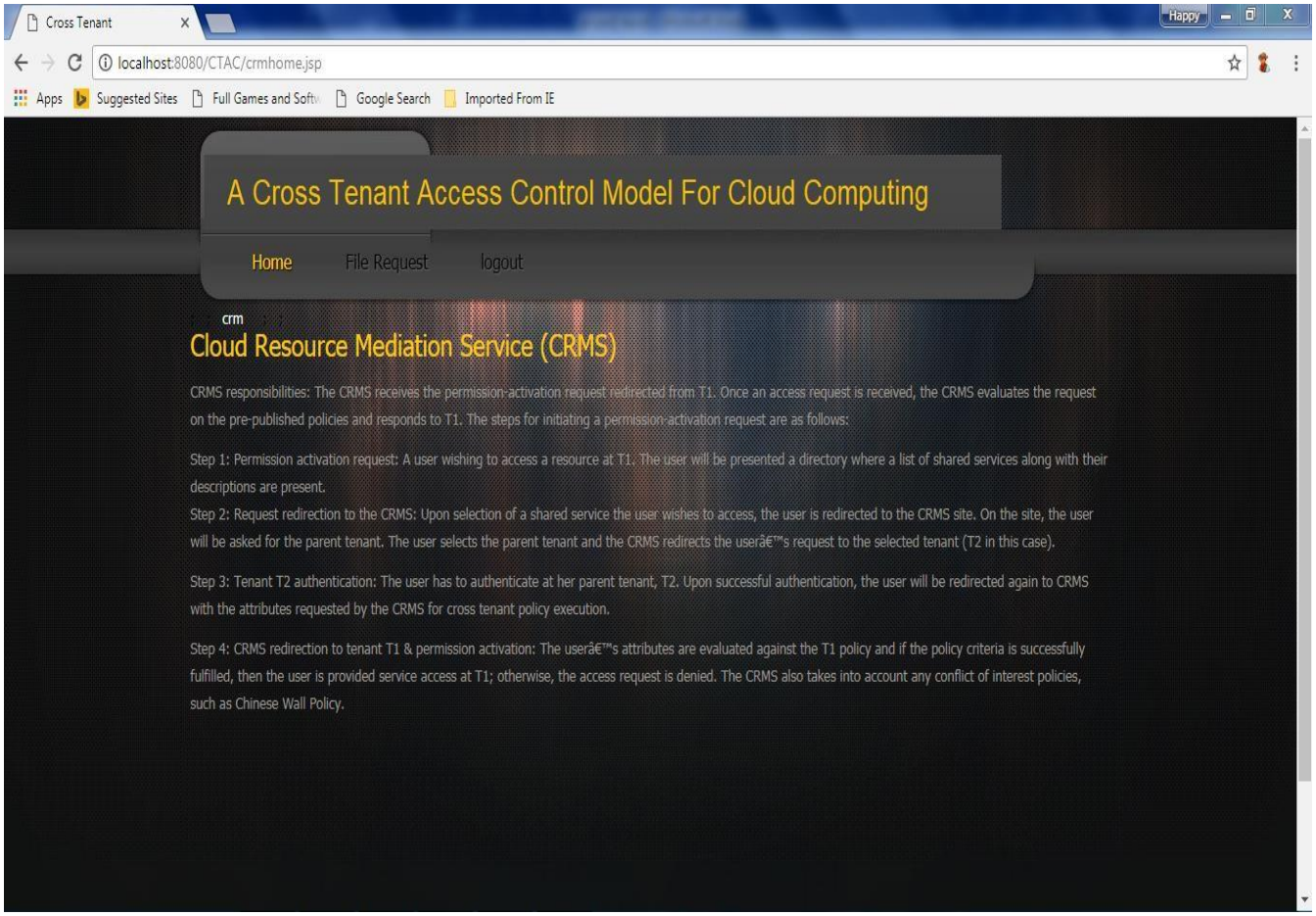


Fig 1.5 Login page of CRM

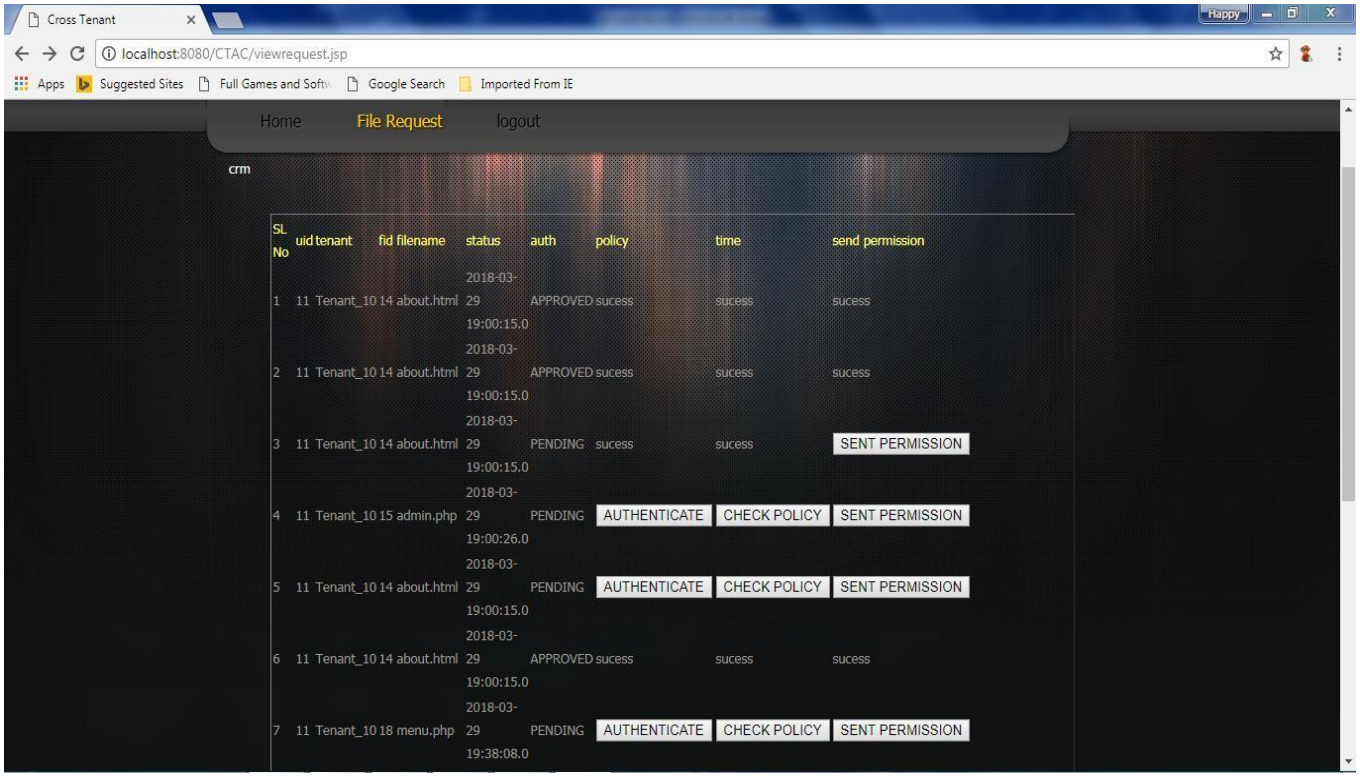


Fig 1.6 CRM Respond to tenant request

5. Conclusion

In this work, a cross-tenant cloud resource mediation service (CRMS) has been proposed, which can act as a trusted-third party for fine-grained access control in a cross-tenant environment. For example, users who belong to an intra-tenant cloud can allow other cross-tenant users to activate a permission in their tenant via the CRMS and also presented a formal model CTAC with four modules designed to handle the requests for permission activation. Then modeled the algorithms using flow chart, formally analyzed these algorithms in DFD. The results obtained after executing the solver demonstrated that the asserted algorithm specific access control properties were satisfied and allows secure execution of permission activation on the cloud via the CRMS. Future work 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. For example, one could implement the protocols in a closed or small scale environment, such as a department within a university. This would allow the researchers to evaluate the performance, and potentially in security, of the various approaches under different real-world settings.

References

1. Akhunzada, A., Gani, A. A, Anuar, N. B., Abdelaziz, A., Khan, M. K. Hayat, A., & Khan, S. U. (2016). “Secure and dependable software defined Networks”. Journal of Networks and Computer Applications, Vol . 61,pp. 199-221.
2. Alam, Q., Tabbasum, S., Malik, S., Alam, M., Tanveer, T., Akhunzad. A., Khan,S., Vasilakos, A. and Buyya, R., (2016). “Formal Verifications of the x D Auth Protocol”, IEEE Transactions on Information Forensics and Security, Vol.11 (9), pp. 1956-1969.
3. Ali. K, M.R, Malik, S. and Khan, S., Alam, Da SCE: “Data Security for Cloud Environment with Semi-Trusted Third Party”.
4. Bofill, M., Nieuwenhuis, R., Oliveras, A., Rodrguez - Carbonells, E. S., Rubio, A., (2008, July), “The barcelogic SMT solver”. International Conference on Computer Aided Verification,pp. 294-298. Springer, Berlin Heidelberg.
5. 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. SpringerBerlin Heidelberg.
6. 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
7. Choo, K. -K. R., Domingo - Ferrer, J. and Zhang. L., (2016). “Cloud a Cryptography Theory, Practice and Future Research Directions”. Future Generation Computer Systems, Vol. 62, pp. 51-53.
8. Dutertre, B., and De Moura, L., 2006. “The yices smt solver”, Tool paper at http://yices. csl. sri. Com/tool-paper.pdf, Vol. 2 (2).
9. De Moura, L.and Bjørner, N., (2011). “Satisfiability and modulo theories: Introduction and applications”, Communications of the ACM, Vol.54 (9), pp.69-77.
10. Heiser, R. J., (2009). “ What you need to know about cloud computing security and compliance”, Gartner, Research, ID, (G00168345).
11. 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, Vol. 65 (6), pp.1706-1719.

12. 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, Vol. 11 (3), pp.484- 497.
13. 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 Informations Forensics and Security, Vol. 11(11), pp. 2401-2414.
14. 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, Vol. 7(2), pp.79-88.
15. Murata, T., (1989). "Petri nets: Properties, analysis and the applications ", Proceedings of the IEEE, Vol.77(4), pp.541-580.
16. Sayler, A., Keller, E. and Grunwald, D., (2013). "Jobber: Automating the Inter - tenant trust in the cloud ", In Presented as part of the 5th USENIX Workshop on Hot Topics in Cloud Computing.
17. Tang, B. and Sandhu, R., (2013), August. "Cross -tenant trust models in the cloud computing", In Information Reuse and Integration (IRI), IEEE 14th International Conference on pp. 129-136.
18. Yang, Y., Zhue, H., Lu, H.,T., Weng, J., Zhang, Y. and Choo, K. - K. R., (2016). "Cloud based data sharing with fine-grained proxy re-encryption", Pervasive and Mobile Computing, Vol. 28, pp. 122-134.
19. Zhang, Y., Patwa, F., Sandhu, R. and Tang, B., Zhao, G., H (August,2015), "Hierarchical secure information and the resource sharing in openstack community cloud", In The Information Reuse and The Integration (IRI), International Conference on pp. 419-426.
20. Zhao, G., Ba, Z., Wang, X., Zhang, Y., Tang, B. Huang, C. and Tang Y., (2016). "Constructing Authentication Web in Cloud Computing", Security and the Communication Networks, Vol. 9(15), pp..2843-2860.

