International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-4, Issue-3, March 2016

An Effective Trust Based Access Control Services for Adaptive Monitoring in Cloud Computing

L.V Sowmya Therese, Bastin C Rogers

***Abstract*— Cloud computing has now become a high demanded service due to its high computing power, cheap cost of services, high performance, scalability, accessibility and availability. This paper provides a trust based access control mechanism for adaptive monitoring in cloud computing. Firstly a basic cloud monitoring system is developed and then trust is introduced into this system. Different methodologies are used in order to calculate trust in inter domain and intra domain. Since the aspects to be considered in these domains to calculate trust are different. This system involves three major participants they are the cloud user, the cloud service provider (CSP) and the trusted third party (TTP). Where the CSP provides users the cloud resources, the cloud user are the customers who hire and use the resources and the TTP is the monitoring service which act as an intermediate between the CSP and the cloud user. Since it is an adaptive system the cloud user can specify what all resources has to be monitored by the cloud monitoring system.**

***Index Terms*— cloud monitoring; access control services; trust; multi-domain**

I. INTRODUCTION

Cloud computing has set a different way in usage of the hardware infrastructures. OpenStack, Apache CloudStack, Snooze, OpenNebula are all some of the commonly available open source cloud computing stacks. Cloud computing has some important challenges to be resolved. One of the main challenges in cloud monitoring system is the lack of trust between the cloud service provider and the cloud user [17][18].

To providing a new way of solving the security problems in cloud computing environment, based on trust management, trust mechanism will be introduced into access control area, which will be redefined and calculated [2]. Finally this developed access control model will be implanted in the credibility of cloud computing in distributed multi-domain environment, trust model will be built and trust computation and updating mechanisms will be included [5].

In this paper, cloud computing security issues will be analyzed and then trust management and RBAC [4] model will be discussed. In addition, the paper introduces trust degree into access control model and finally proposes trust-based access control model of multi-domain in cloud computing. Trust computation methods are given in local domain and multi-domain, respectively.

L.V Sowmya Therese, PG Student, Department of Computer Science, Stella Mary's College of Engineering, Anna University, Chennai, India.

Bastin C Rogers, Assistant Professor, Department of Computer Science, Stella Mary's College of Engineering, Anna University, Chennai, India

II. RELATED WORK

There are lot of inventions and research carried out in the cloud monitoring service. These works are mostly related based on the software used in the cloud monitoring service and not considering their additional features such as network traffic monitoring [7], security monitoring [15], QoS monitoring [4], SLA-monitoring services [9] based on physical sensor devices. Thus some cloud monitoring services are being proposed but only sparse amount of them are under usage.

A. MonPaaS: MonPaaS: An Adaptive Monitoring Platform as a Service for Cloud Computing Infrastructures and Services

This paper provides a monitoring service for the cloud computing environment especially the Platform-as-a-Service, and this paper involves providing a monitoring solution for both the cloud user and the service provider [7]. This system enables the cloud user to see the complete view of the entire cloud monitoring service, and the cloud user can only see resources owned by them.

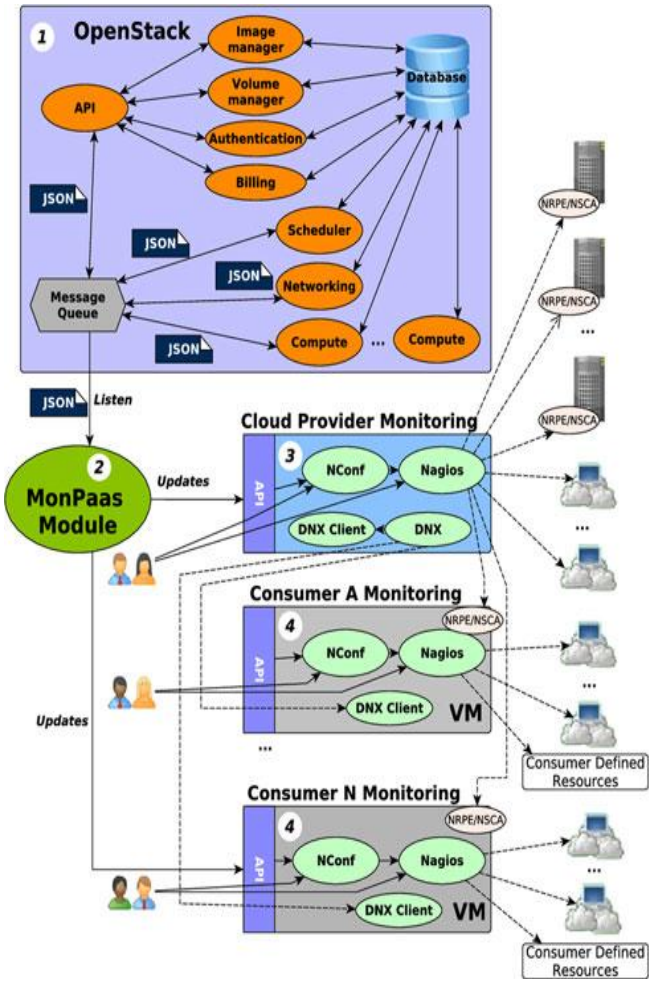

Fig.1 MonPaaS Architecture

And the adaptive service allows the cloud user to specify what resources have to be monitored and controlled by the cloud monitoring service. The cloud user can also control the information gathered regarding their resources by the monitoring service. In order to set a cloud monitoring service in a system in the view of cloud service provider Nagios has to be installed along with the NConf and DNX [1]. Where this NConf is used to provide a graphical interface to view the complete cloud computing infrastructure.

B. PORs: Proofs of Retrieveability for Large Files

This paper proposes a method, proofs of retrievability(PORs). A POR enables a user (verifier) to determine that an archive (prover)"possesses" a file or data object. It introduces a sentinel-based POR Scheme [9]. Here verifier stores only a single cryptographic key and a small amount of dynamic state for each file. To protect against corruption by the prover, it also employ error-correcting codes. The sentinels, which constitute the content of a POR proof, are generated independently of the bit string whose retrievability they are proving. It applies a symmetric-key cipher and a stream cipher. The permutation step in this protocol serves two purposes. First, it randomizes the placement of sentinels such that they can be located in constant time and storage; only the sentinel generation key need be stored. The second purpose relates to error correction. It erasure codes which are more efficiency as a class than general error-correcting [3] codes is also introduced which operate in linear time. Advantage is it provides quality-of-service guarantees. Drawback is efficiency to provide regular checks of file retrievability. Disadvantage is it yields weaker security and some computational overhead occurs.

C. SiRiUs:Securing Remote Untrusted Storage

This paper presents SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. It implement a security mechanism that improves the security of a networked file system without making any changes to the file system or network server. SiRiUS is designed to be easy to install and is intended to be used until a new network file system is deployed with adequate access control and data integrity abilities. SiRiUS is designed to handle multi-user file systems where users frequently share files. SiRiUS [15] appears as a local file system with the standard hierarchical view of files and directories. A SiRiUS client on the user's machine intercepts all operations to the SiRiUS file system and processes the requests before transmission to the remote file server. The type of network file system exported by the remote file server is hidden from the user. All cryptographic operations including encryption and signing are done by the client before the results are placed on the file server. All SiRiUS users maintain one key for asymmetric encryption and another for signatures that called as user's master encryption key (MEK) [11] and master signing key (MSK). Files stored on the file server are kept in two parts. One part contains the file meta data and the other the file data. The file meta data contains the access control information while the file data contains the encrypted and signed contents. The file data is encrypted with a symmetric cipher using a unique key for each file called file encryption key (FEK). The signing key is called the file signature key (FSK). Advantage it is easy to install and used to secure removable storage devices such as USB hard drives and compact flash devices. Disadvantage is it cannot prevent a "sledgehammer" denial-of-service attack.

This paper extended the proof of retrievability (PoR) model by using an elegant Merkle hash tree (MHT) construction to achieve fully dynamic data operation [13]. It propose a general model for data storage using public verifiability, in which blockless verification is achieved and also has a function to provide fully dynamic data operations, such as block insertion, which is not well defined in most of the schemes. Three different network entities can be identified as follows: Client : is an organization or an individual who relies on the cloud for maintaining their data or computation, can be either individual consumers or organizations; Cloud Server Storage (CSS): an entity, maintained by a cloud service provider, has significant storage space and computation resource to maintain clients' data; Third Party Auditor (TPA): a TPA [6], which is the monitoring system not available in the cloud user's system, is used to monitor the cloud service provider in order to detect any violation of data or resources .MHT is an authentication service which is relied in order to determine trust in the overall cloud monitoring environment. This method involves generating a binary tree which maintains the data which is encrypted and secured, it also maintains the hashed value of the secured data. It present a BLS-based construction that offers both public verifiability and data dynamics. Then it adopts the blockless approach, and authenticates the block tags instead of original data blocks in the verification process. Advantage is Efficiently in supporting data dynamics. Disadvantage is its low performance.

III. TRUST BASED ACCESS CONTROL SERVICE

Trust relations between users and cloud computing platform will be established according to user's behavior and trust degrees will be calculated by the trust model. Combined with RBAC technology, dynamic access control in cloud computing environment will be implemented. In accordance with the multi-domain character, this paper introduced trust into access control model and established a trust based multi-domain access control model in cloud computing environment. The main difference between trust based multi-domain access control and the traditional access control mechanism is that users visit local domain and cross-domain respectively by means of two different kinds of access control policies [12][16]. In trust based multi-domain access control model, when a user logs in, the system shall verify user's identity first. If the identity is trusted, the user's identity will be authorized.

Trust levels reflect users' behavior trust in this model. Authorization is no longer a static mechanism based on identity trust, but a dynamic mechanism combined with identity trust and behavior trust. Therefore, this model realized the combination of user's identity trust and behavior trust. The overall framework of trust based multi-domain access control model is shown in Fig.2.

A. OpenStack logging handler

This module is used for maintaining the logging details of the cloud users, it defines a context object for each function, also a uuid instance is maintained which makes it easier for the admin to find a related message in a particular instance.

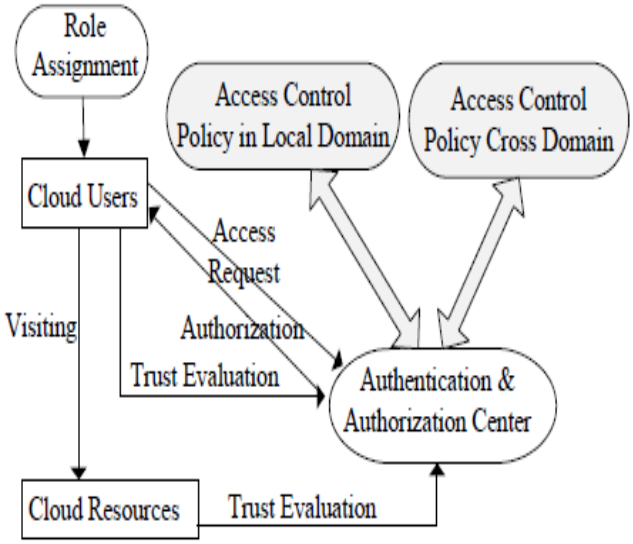

Fig.2 Overall framework of trust based multi-domain access control

B. *Sheduler*

Compute uses the nova-scheduler service to determine how to dispatch compute and volume requests. For example, the nova-scheduler service determines on which host a VM should launch. In the context of filters, the term host means a physical node that has a nova-compute service running.

C. *Access Control Policy in Local Domain*

The main method of introducing trust into RBAC model is taking trust degree as the basic property of cloud users and cloud services and resources. The authentication and authorization Center (AAC) is in charge of access control authentication, authorization and trust management in local domain. While in cross domain, access control and trust management are the responsibility of both master authentication and authorization center (MAAC) and AAC [14]. In local domain, every time when any cloud service or resource is been requested to be accessed by a user, AAC would see user's trust degree to ensure that the user's trust degree meet the trust threshold. If it is so, the user's request would be allowed and processed for further steps of verification. The structure of access control in local domain is shown in Fig.3.

The access control process in local domain is as follows:

(1).In RBAC, cloud user will request to role assignment before it sends an access request and obtains the corresponding access rights indirectly. It also needs further measures such as trust management to decide whether a user can use their access rights.

(2).The cloud user sends an access request including user ID, password and ID of the requested resources or services to AAC. AAC authenticates the user's identity first and then authorizes the user based on its trust degree obtained from trust management. Authorization process is as follows:

①The decision database initializes security policy in local domain;

②The decision implementation end delivers user's request to the decision end;

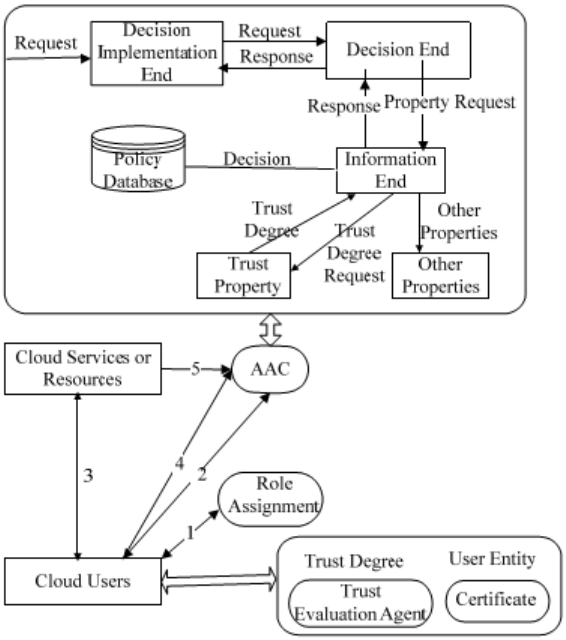

Fig.3 Access control structure in local domain

③The decision end delivers the request to the information end;

④The information end obtains information of user's trust degree and other properties and returns it to the decision end;

⑤ The decision end makes an access control decision according to user's information and current security policy;

⑥The decision implementation end returns the result to the user entity. If the user's access request is permitted, then provide the user a certificate, so that the user obtains the permission to use the access rights corresponding to its roles.

(3).The cloud user executes its access control privileges and visit cloud services or resources.

(4).In the end, the user evaluates the performance of cloud services or resources. The trust evaluation agency would compute a new trust degree and send it to AAC.

(5).The cloud service or resource provider also gives an evaluation of the cloud user and returns it to AAC.

D. *Access Control Policy in Cross Domain*

As users usually need to access cloud services or resources of different security domains, a safe and effective access control method is necessary. The cross domain actually refers to the access of data to a particular cloud from various different organizations or different domain for data access and processing. Research about cross-domain access control problems in cloud computing environment is not much, but it cannot be ignored. RBAC applies to the closed network environment and is unable to meet the security requirements of the multi-domain environment [8]. Therefore, role association is required. Role association means converting roles of one domain into roles of another domain. The structure of trust based access control in cross-domain is shown in Fig.4.

Cross-domain access control process is as follows:

(1).Bob's role in domain A will be assigned by role assignment center of A, so that Bob can obtain his role in

domain A. Alice's role in domain B will be assigned similarly by role assignment center of B.

(2).Bob sends a request to AAC of domain A. AAC figures out Bob's trust degree and judges whether Bob has the permission of visiting the target domain according to local security policy

(3).AAC of domain A sends the request to MAAC. MAAC looks up trust relations between domain A and domain B and then checks if access should be allowed. If it is allowed, AAC will provide Bob a certificate.

(4).Bob sends Alice his access request, certificate and his role in domain A.

(5).After receiving Bob's access request, Alice first converts Bob's role in domain A into an understandable role of domain through role association and then checks whether this role has the permission of visiting Alice's resource. If the entity has attained the permission then it can access its resources.

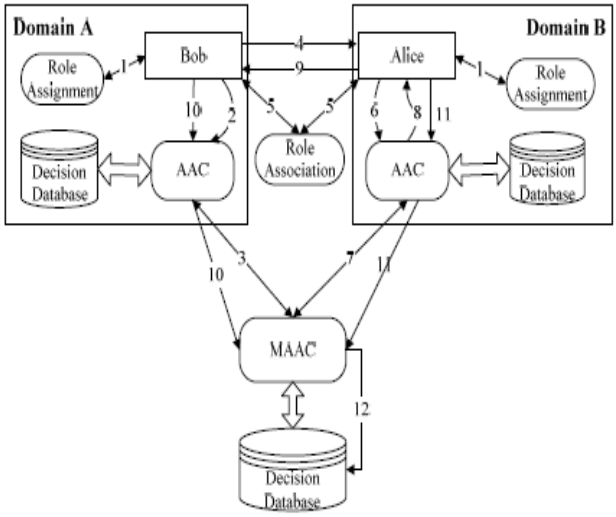

Fig.4 Structure of access control in cross-domain

If it doesn't have the permission, then refuse Bob's access request directly.

(6).Alice passes the certificate to AAC of domain B.

(7).AAC of domain B contacts with MAAC [17]. Where this MAAC is a multi domain's authentication and authorization center. MAAC completes the connection between the two domains and the certificate transmission according to trust degree and role mappings between domain A and domain B. MAAC figures out Bob's trust degree in domain B, then returns the result to AAC of domain B.

(8).AAC of domain B compares Bob's security properties with local security policy, and then returns the result to Alice.

(9).Alice returns the result of authorization to Bob. If the request is permitted, Alice would allow Bob to use her resource; if not, Alice would refuse Bob's request.

(10).Bob evaluates the performance of the requested resource and sends the value to AAC of domain A. Then AAC passes it to MAAC.

(11).Alice evaluates Bob and sends the evaluation value to AAC of domain B. Then AAC passes it to MAAC.

(12).MAAC calculates and updates the mutual trust degrees between domain A and domain B

E. Trust Degree Calculation

Although trust evaluation among different security domains differs from that in single domain, the impact of inter-domain trust is relevant to trust degree of some entity and the behavior of every entity in the domain [10]. Trust relations between users and cloud computing platform will be established according to user's behavior and trust degrees will be calculated by the trust model. In trust based multi-domain access control model, when a user logs in, the system shall verify user's identity first. If the identity is trusted, the user's identity will be authorized. Trust levels reflect users' behavior trust in this model.

IV. PERFORMANCE

A trust based access control mechanism for adaptive monitoring in cloud computing is provided in this paper.

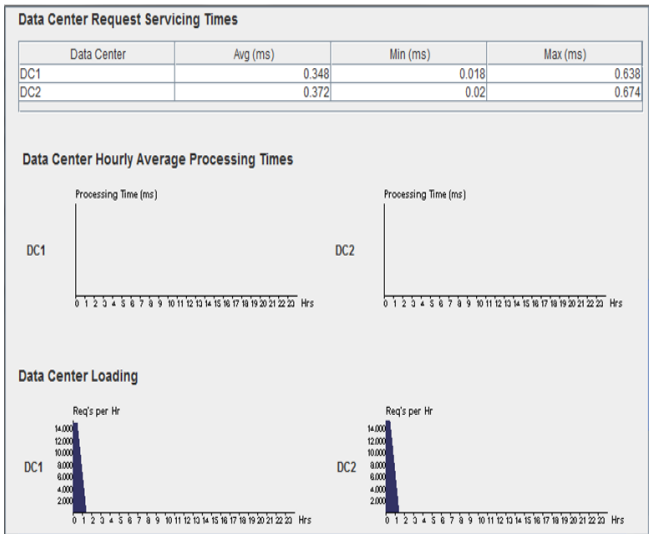

Fig.5 Performance evaluation of data center in the cloud.

The architecture fulfills successfully all the requirements specified such as an monitoring architecture which monitors the cloud service provider and the cloud user based on their trust value. Since it is a cloud service it is capable of providing better disaster recovery, load balancing and adaptive monitoring compared to the other advanced features.

A significant step has been provided which allows the user of this system to provide feedback on other users or service providers, thus creating an adaptive cloud monitoring system based on trust for cloud computing services.

V. CONCLUSION

In conclusion, this paper discussed access control in cloud computing monitoring environment and proposed a trust-based access control model in multi-domain, which combined with RBAC mechanism. This discussed access

control policies in local domain and cross-domain, respectively. In local domain, access control policy includes role assignment, trust management, authentication and authorization. Besides, access control cross-domain involved as well as role translation. This mechanism converted roles of outer domain into roles of local domain by means of role association. Moreover, it performed trust management, authentication and authorization. In cloud computing, the application of trust-based access control and the consideration of the features of multi-domain can be more intuitive and effective in protecting the security of cloud users and cloud providers monitoring platform.

VI. REFERENCES

[1] Apu Kapadia, Jalal Al-Muhtadi, R. Campbell, et al. "IRBAC 2000: secure interoperability using dynamic role translation," University of Illinois, Technical Report: UI-UCDCS-R-2000-2162, 2000.
[2] Beth T., Borcherding M., Klein B. "Valuation of trust in open networks," Proceedings of the Third European Symposium on Research in Computer Security, Brighton: Springer-Verlag, pp. 3-18, 1994.
[3] Bo Lang, "Access control oriented quantified trust degree representation model for distributed systems," Journal on Communications, Dec. 2010.
[4] Chen Jincui, Jiang Liqun, "Role-based access controlmodel of cloud computing," Energy Procedia 13, pp. 1056-1061, 2011.
[5] Dengguo Feng, Min Zhang, Yan Zhang, "Study on cloud computing security," Chinese Journal of Software, vol. 22, no. 1, pp. 71-83, 2011.
[6] Dongyan Jia, Fuzhi Zhang, Sai Liu, "A robust collaborative filtering recommendation algorithm based on multidimensional trust model," Journal of Software, vol. 8, no. 1, pp. 11-18, Jan. 2013.
[7] Jiyi Wu, Qianli Shen, Tong Wang, "Recent advances in cloud security," Journal of Computers, vol. 6, no. 10, 2011.
[8] Junchang Song, Cheng Su, "Using trust in access control mechanism," Computer Engineering and Design, Oct. 2007.
[9] Junzhou Luo, Xudong Ni, Jianming Yong, "A trust degree based access control in grid environments," Information Sciences, pp. 2618–2628, 2009.
[10] Jφsang A. "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 9, no. 3, pp. 279-311, 2001.
[11] Liangmin Guo, Yonglong Luo, Zhengzhen Zhou, Meijing Ji, "A recommendation trust method based on fuzzy clustering in P2P networks," Journal of Software, vol. 8, no. 2, pp. 357-360, Feb. 2013.
[12] Sadeghi AR, Schneider T, Winandy M. "Token-based cloud computing: secure outsourcing of data and arbitrary computations with lower latency," In: Proc. Of the 3rd Int'1 Conf. on Trust and Trustworthy Computing. Berlin: Springer-Verlag, pp. 417-429, 2010.
[13] Santos N, Gummadi KP, Rodrigues R. "Towards trusted cloud computing,"In: Sahu S, ed, USENIX Association Proc. of the Workshop on Hot Topics in Cloud Computing 2009. San Diego, 2009.
[14] T. Grandison, M. Sloman, "A survey of trust in Internet applications," IEEE Communications Surveys and Tutorials, 2000.
[15] Weiliang Zhao, Varadharajan V, Bryan G. "General methodology for analysis and modeling of trust relationships in distributed computing. Journal of Computers, vol. 1, no. 2, pp. 42-53, 2006.
[16] Wenhui Wang, Jing Han, Meina Song, Xiaohui Wang, "The design of a trust and role based access control model in cloud computing," Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International.
[17] Xuri Chen, Weimin Xu, Wenfeng Shen, "Trustworthiness-based dynamic access control for grid application," Journal of Hunan University (Natural Sciences), vol. 35, no. 7, pp. 85-89, Jul. 2008.
[18] Zhanjiang Tan, Zhuo Tang, Renfa Li, Ahmed Sallam, Liu Yang, "Research on trust-based access control model in cloud computing," Proceedings of 6th ICPCA, 2011.

L V Sowmya Therese, is a PG student at Stella Mary's College of Engineering, Anna University, Chennai. Anh has received Bachelor degree in computer science and engineering from Vins Christian College of Engineering, Anna University, Chennai.

Bastin C Rogers, is an assistant professor in computer science department at Stella Mary's College of Engineering, Anna University,Chenai. He has received his master degree in computer science and engineering from Anna University, Chennai.