Three-Layer Access Control Integrated with Policy Enforcement Point

Nader Shahata

Cyber Security Research and Development Center, Natioanl Institute of Informatics
Tokyo, Japan
Email: nader [AT] nii.ac.jp

ABSTRACT— ***Cloud computing reflects significant risks which is associated with federal agencies and regulations. Any vulnerability that is initiated in the software or platform of the vendors will lead to the leakage of the data, as information may be related to more than one organization. Likewise, next generation solution provide assistance to the legacy system along with the provision of robust, elastic and low cost knowledge based tools of deeper exploration and understanding for processing massive data right to the end users. Moreover, the next generation solution business analytics provides in depth understanding of company clientele and product presentation***

Keywords— Cloud Computing, Security, Distributed Systems, Network Systems.

1. INTRODUCTION

A number of application sources are related with cloud computing. In fact, these sources are managed by several commitments including proper license of open source. Similarly, in order to fulfill all the requirements regarding licensing address issues and migrating risks are involved. However, new risks are not introduced by cloud computing but other applications that are included in cloud contains risks. Like any other software, applications are distributed but not shared in cloud computing. Therefore, no calculation and investigation is needed for incorporating restrictions of copy left licenses.

2. BACKGROUND

In order to decrease system failures for future procedures, risk analysis is needed for identifying all the critical systems on the network. Moreover, daily backups are required on daily basis and a performance is also required for checking the integrity of the backup at the same time.

2.1 Role-based (RBAC) Access Control Decisions

The PDP proactively moves on the complete section of the state in the current case that enables to relate a session at Session Description Protocol (SDP). Likewise, RBAC also support role based encryption as well [1].

2.2. Bloom Filters

The bloom filters were introduced by Burton Bloom in 1970's. Since then, it is a world renowned concept, specifically in the data storage market. Moreover, in network literature Bloom Filters are getting wide attention nowadays, as one of the reasons can be its space efficient structure that can be integrated in distributed cloud applications [2]. The most visible and prominent factor associated with the increase in size of bloom filters and the reduction on the same time as well. The difference between the Cascade Bloom Filters and the Bloomier filters is that the main purpose is to symbolize and test for membership in randomized function while, on the other hand; the aim is to check for the binary access [3]. As a result, with complete functions related to the formation as well as the insertion of the Cascade Bloom filters is observed. The practical algorithms regarding the general Bloomier filters are still unlearned [4].

2.3 CPOL

The reduction in the evaluation time related to the access control queries can be achieved via utilization of caching mechanism and by implementing the policy evaluation framework. Furthermore, the cache techniques guarantee proper reliable cache. The concept of access control risks defines the fuzziness of distinction via restricting an access and as a replacement; every access is in relation to the potential impairment and utility. In disseminated systems, every node constructs its own cache in association with the other nodes in order to achieve precise cache. The proposed solution incorporates the relationship of objects and subjects in a typical database. However, there is still a requirement for learning the subject and object space.

2.4 Software Assurance Maturity Model (SAAM)

The SDP enforces the theoretical framework SAAM to utilize responses from authorized requests. In addition, if PDP is unavailable the heuristics supplies a substitute for the conservative authorization responses [5]. The SAAM supposes that the caches related to the PDP responses are utilized to conclude accurate replies. Moreover, collecting the comebacks is not an innovative impression within the access control domain. These are utilized for the improvement of systems competency and compatibility. As a result, additional advances only figure out accurate mechanisms for authorization that has effectiveness for resolving frequent queries [5]. New queries can be determined by the SAAM with the help of space extensions in order to support the estimated responses. Alternatively SAAM provide more rich sources for authorization responses as compared to the previous approaches. It offers a methodological approach in order to authorize recycling via generic model of authorization queries and responses [5]. Moreover, SAAM also provides responses arrangements and policies. SAAM is basically a domain-specific approach thus providing fault tolerance and performance enhancement for the access control mechanism. Following are the three basic classification of the fault tolerance solution [5]:

- Failure masking via information redundancy for instance correction of errors and checksums.
- Time redundancy for example repetitive invocations.
- Physical redundancy such as data replication.

The fault is covered with the SDP through the demanded decisions for controlling access. The primary physical redundancy methods for the distributed systems are away from the small number of systems. Moreover, if the scale reaches thousand, it became technically and economically less feasible [5]. By utilizing SAAM, the authorized responses are cached while the active authorized information is simulated, and linear scalability is allowed for the number of PDPS's and PEP's. Now the latest concepts, methods and strategy algorithms are produced that are associated with the new decisions of access. The secondary and approximate authorization model (SAAM) delineates the philosophy of primary vs. secondary and accurate vs. approximate authorizations [5]. In fact, the approximate authorization responses are concentrated from the cached initial responses and then offer the other source related to the access control decisions for the servers that are unavailable or slow [5]. However, the efficiency to calculate authorizations enhances the consistency and presentation of the access control sub-systems and the application systems [5]. System operations incorporating SAAM are dependent on the type of access control policy that it deploys. A research was conducted that proposed a solution for calculating secondary authorizations with compliance of policies mentioned in Bell-LaPadula model. Likewise, a dominance graph is defined along with its formation and usability for developing secondary response to an authorized request [5].

3. THE PROPOSED THREE-LAYER ACCESS CONTROL INTEGRATED WITH PEP

The cloud computing infrastructure incorporates a service creator that demonstrates access control on policies for the end users associated with the cloud service. Though, the end users of cloud applications have maximum control for managing data and for enforcing the related policies. Likewise, cloud computing service providers provide services to their customers in every anticipated level. Moreover, the access control mechanism for cloud computing must be compatible with all these three requirements. Consequently, the paper defines the three layer architecture that is a proposed solution for cloud computing access control and revocation.

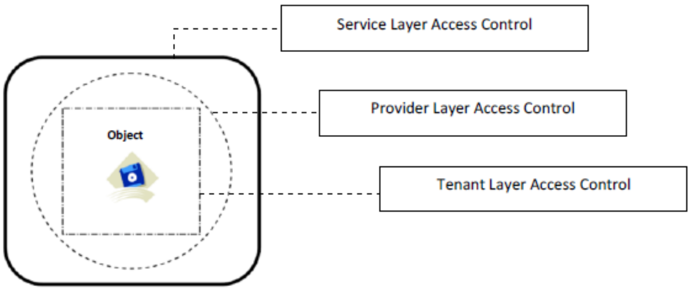
Service Layer Access Control
Provider Layer Access Control
Tenant Layer Access Control
Object

Figure 1.1

As shown in fig 1.1, the service layer of the cloud is acting as enforcement for implementing access control policies. The provider layer is also acting as enforcement for access control policies from the vendor side, and tenant layer is also acting as enforcement for end user access control policies. The three layer architecture is considered as the *"platform as a service"* and securities access control for the services related to SaaS[6]. The following three elements regarding the suggested access control architecture are mentioned below:

3.1. Identity Provider

This component is associated with the end users of the cloud. Likewise, the element identifying the identity for the end users provides the access control service (ACS) usage. At the initial level, the request for granting access to cloud services is sent to the element. Secondly, the authentication process is triggered and after completion, the security token service generates a token and routes it to the ACS via the end user's PEP. This concludes that the end user is accountable for the deployment of policies via PEP.

3.2 Cloud Provider

Now the next element in this architecture is considered to be the cloud provider itself [7]. In the cloud provider the Transform Security Token Service (T-STS) is the core element of the cloud provider. The main features of T-STS are to translate inter organizations' tokens. When the two elements i.e. token and service providers incorporate together than an interoperability has been found. This can be done via mapping of attribute transformation. However, the T-STS include a set of tokens that helps to translation policies. These translated policies can further accomplish via this mapping process.

3.3 Service Provider

The component indicating as a service provider is liable for enforcement via ACS for service creator policies. Consequently, this specific component is not associated with tenant and vendor policies. Only PEP is utilized for policy enforcement on access request.

4. ANALYZING THE PROPOSED METHOD

The analysis proposed method is divided into three steps. This architecture that is involving three steps possess some benefits that are mentioned below:

- Initially, the vendor can integrate its services into cloud based servers at any point easily without any threats. In fact, for different layers the translation of the attributes has no issues with this method. Similarly, the vendors are allowed to use their way of services to add in cloud computing without keeping in mind the risks for the compatibility of the application.
- The second benefit of cloud computing is that a renter is allowed to implement its own policies for the clients other than the policies that are present in cloud computing. Thus, the vendors are allowed to impose strict policies on the cloud services. This provides more control for the cloud computing end users using these services. Moreover, the renters are less worried about mapping their access control policies. In order to translate the attributes the renters has no difficulty for using cloud services.
- According to the vendors choice, the policies can be imposed other than the cloud service policies. Moreover, in different levels of cloud computing, the renter may implement security policies, as well. The translation of attributes does not harm the scalability and the extensibility of the domains in cloud computing. Thus, providing superior interoperability for the cloud computing users.

5. CONCLUSION

In this paper we discussed the ACS which is mainly based on two components the built-in and usage control model. Therefore, the specific access control along with mutability is present in this model. However, if the policies are not followed significantly during the access; the vendor is allowed to terminate the access from the client.

6. ACKNOWLEDGEMENT

I would like to thank Professor Hiroki Takakura for his expert advice and encouragement throughout this research paper.

7. REFERENCES

[1] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Enforcing Role-Based Access Control for Secure Data Storage in the Cloud." *Computer journal* 54.10 (2011): 1675-87. Print.

[2] Moreira, Marcelo Duffles Donato,"Capacity and Robustness Tradeoffs in Bloom Filters for Distributed Applications." *IEEE Transactions on Parallel & Distributed Systems* 23.12 (2012): 2219-30. Print.

[3] Kanizo, Yossi, David Hay, and Isaac Keslassy. "Access-Efficient Balanced Bloom Filters." *Depness Lab* 36.4 (2013): 373-85. Print.

[4] Guo, Deke, "The Dynamic Bloom Filters." *IEEE Transactions on Knowledge & Data Engineering* 22.1 (2010): 120-33. Print.

[5] Crampton, J., W. Leung, and K. Beznosov. "The Secondary and Approximate Authorization Model and its Application to Bell-LaPadula Policies}, Booktitle = {Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies." (2006): 111. Print.

[6] Guptill, Bruce, and William S. McNee. "SaaS SETS THE STAGE FOR 'Cloud Computing' (Cover Story)." *Financial Executive* 24.5 (2008): 37-44. Print.

[7] SecureKey. "SecureKey Divests Hardware Security Token Group." (2013)Print.