International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 20 No. 1 Jan. 2016, pp. 233-241

http://www.ijisr.issr-journals.org/

Access Control Model for Data Stored on Cloud Computing

Adnan Ahmad Malik[1], Bilal Hussain[2], and Syed Ozair Hussain Kazmi[1]

[1]Computer Science, CS Department University of Agriculture Faisalabad, Punjab, Pakistan

[2]Computer Science, CS Department GC University Faisalabad, Punjab, Pakistan

ABSTRACT: Cloud Computing (CC) is a internet based computing technology having shared scalable infrastructure that can be used as service by users. Simply CC can be referred as hardware & software deliverable using internet that is also as a service. An outstanding innovation & technology getting popular due to lower-cost, flexibility and scalability as per user's requirement. Regardless of its popularity large organizations, enterprises are reluctant to move on cloud computing due to its security issues, especially user's data security. Organizations have expressed concern over data security as their confidential and sensitive data needs to be stored by service provider at any location globally, that's why security can't be compromised at all. CC has different security issues at different levels like software security, platform security, infrastructure security etc. This research shall take a review and to focus on user's data security i.e. data storage security issues and how to minimize unauthorized access to data, then available solutions will be presented and an access control model will be suggested. It'll help the reluctant users to easily decide to shift on cloud while understanding the risks associated with CC.

KEYWORDS: Access Control Model, Cloud Computing, Data Security, Infrastructure Security, Organization's Data, Platform Security, Unauthorized Access.

1 INTRODUCTION

Cloud computing is promising solution for accessing and using resources over internet. It's powerful and processing and storage solution which is provided on-demand. Cloud provides services to users and has the ability being scalable and reliable. It scales it's and improve its capacity by adding more hardware as per need, which allows to deal the growling need of cloud day by day. User can access his own or hosted data and applications from anywhere in the world. Resources in cloud are shared among many users. These recourses are provided as service on an need bases, as the resources increase when user wants more and decreases when need it less.

In cloud computing, we can get services from geographically spread the sources, instead of from remotely available server. There is no pet definition of cloud computing, but we can say that it is a collection of geographically spread servers known as master computer, offering the demanded services to end-user as and when required on pay per use policy. There are mainly three kinds of services provided by cloud which are SaaS, IaaS, and Paas Amazon EC2 bright is a bright example of cloud computing. Cloud has changed the concept of software development style, as it has become more web centric. Many companies are providing cloud service, currently some prominent are Google corporation , International Business Machines(IBM), M.S (Microsoft), Amazon Inc., Virtual Machine (VM)ware & EMC.

In cloud computing, we can get services from geographically spread the sources, instead of from remotely available server. There is no pet definition of cloud computing, but we can say that it is a collection of geographically spread servers known as master computer, offering the demanded services to end-user as and when required on pay per use policy. There are mainly three kinds of services provided by cloud which are SaaS, IaaS, and Paas Amazon EC2 bright is a bright example of cloud computing.

Corresponding Author: Adnan Ahmad Malik

Fig.1. Cloud Computing

NIST - National institute of standard and technology describes the cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (e.g. networks server, storage applications. And services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. The cloud is being seen as important and vital in the IT industry as time goes on and will impact more on information technology for the society. Cloud infrastructure is mainly relay on deliverable service those are based on servers with different levels of virtualization technology.

2 ACCESS CONTROL MODEL

An access control model (ACM) is a collection of components & methods which determines the legitimacy of user activities by the legitimate users based upon pre- configured access permissions and privileges described in the access security policy [2]. The fundamental goal of any access control model is to restrict a user exactly where he should be able to perform normal activities and protect information from unauthorized access.

There is a vast variety of methods, models, technologies and administrative capabilities used to propose and design access control model. Thus each access control model has its own attributes, methods and functions, which derive from either a policy or a set of policies. Cloud computing is a shared & open environment, which has its own characteristics and features such as on-demand services, mobility, multi-tenancy, and ubiquitous. Thus, cloud service providers need a powered access control model for controlling entrance to their resources with the ability to monitor precisely who accesses them. They should have the ability to deal with dynamic and random behaviors of cloud consumers, heterogeneity and diversity of services.

2.1 WHY CONVENTIONAL ACMS CAN'T BE USED

There are certain reasons exist, some of them are listed below.

- Cloud is very complex and sophisticated due to the dynamic nature of the cloud's resources [3].
- Entities those are cloud based are likely to reside in varied trusted domains and may be located in different countries that have various rules and regulations. Thus, they may not trust each other as per requirement [4].
- Conventional access control models in cloud would suffer from the lack of flexibility in attribute management and scalability.
- Heterogeneity, ubiquitous and variety of services [5].
- Diversity or variety of access control policies and various access control interfaces can cause improper interoperability [6].
- Dealing with a large number of users, different classification, high dynamic performance, mobility features and changes in high frequency is part of cloud [7].
- Different access permissions to a same cloud user, and giving him/her ability to use multiple services with regard to authentication and login time [7],[8].
- Sharing of resources among potentially untrusted tenants, multi-tenancy and virtualization, mechanisms which helps to support transfer customers' credentials across layers to access services and resources are crucial aspects in any access control model that is going to be deployed in cloud computing [9].

3 MANDATORY ACCESS CONTROL MODEL (MAC)

Mandatory Access Control (MAC) model, a central authority-in command for giving access decisions to a subject that request access to objects or information in objects. In order to secure access to objects and the information that flows between objects, MAC assigns an access class to each subject and object in system. An access class is a security level that is used to secure the flow of information between objects and subjects with dominance relationship. Object classifications are security labels that are used to classify objects based upon the sensitivity of information they have. Subject clearances are security levels used to reflect the trustworthiness or rules of subjects. The early formula and most well-known relationships were proposed by Bell and LaPadula in 1973. This model is also known as multilevel security and uses only two properties no-read-up and no-write-down properties.

The Belle-LaPadula model has concentrated on securing and controlling data flow, but protecting the confidentiality in a system is not the only goal in securing information. Hence, Biba (1977) used the same principles utilized by BelleLaPadula model to propose a model for protecting the integrity of objects. Although the mandatory access control model provides protection against information flow and indirect information leakages, it does not guarantee complete secrecy of the information either in the BelleLaPadula model or the Biba model both are vulnerable. For example, any un classified subject can write into top secret objects, and could cause improper modifications to objects and violate their integrity.

In fact, this model is very expensive and difficult to deploy and does not support separation of duties, least privileges, and delegation or inheritance principles. Dynamic activation of access rights for certain tasks is not supported in this model. Moreover, it does not support time and location constraints. It needs a precise management system for dealing with system components that reside either inside or outside of the model. For instance, processes and libraries are considered as trusted components, but sometimes they need to break MAC principles. Thus, they might need to reside outside of the MAC model. Furthermore, over classify subjects or objects can happen in it.

The BLP still does not deal with the creation or destruction of subjects or objects. Security labels are not flexible and convenient for task execution. MAC requires a central authority to determine what information should be made accessible and by whom. For example, a manager might want to access information about a staff member, but s/he should not be able to have full access to the members file, as s/he could access and reveal sensitive information of member such as bank account details. As cloud computing is going to use current web applications to deliver their services to users, MAC has to deal with a lack of sophisticated semantic models, which represent and communicate privileges and constraints that are provided via access control policies[9]

4 DISCRETIONARY ACCESS CONTROL MODEL (DAC)

The Discretionary Access Control (DAC) model, grants the owners of objects the ability to restrict access to their objects, or information in the objects based upon user identity or a membership in certain group. DAC model is generally less secure than mandatory access control model i.e. DAC < MAC secure, so it is used in environments that do not require a high level of protection. However, DAC is the most used model in commercial operating systems such as UNIX and Windows-based platforms because it is more flexible and easier to be utilized than other models. There are two ways to implement a discretionary access control (DAC) model, this can be achieved via identity based access control or by means of an access control matrix (Access Control List (ACL)) or capabilities) [4].

The DAC depends on allowing owners of the objects to control access permissions to objects, yet it has many drawbacks when it is utilized in cloud. For instance, there is no mechanism or method to facilitate the management of improper rights (e.g. risk awareness), which owners of objects can give to users. Occasionally users are required to use privileges that reveal information about objects to third parties. For instance, a user can only read a file in a company, and then s/he can copy file contents to another file in order to pass it to another user. The DAC have not the ability to control information flow or deal with Trojan horses that can inherit access permissions [8], [10].

On the other side, a user may pass their rights to another user, and that can violate the integrity and confidentiality of objects. Finally, it cannot be scaled enough for cloud computing.

5 ROLE BASED ACCESS CONTROL MODEL (RBAC)

Role-based access control (RBAC) is considered as a natural way to control access to resources in organizations, enterprises, firms. The motivation behind RBAC comes from considering “a subject’s responsibility is more important than

whom the subject is about" [9] In the RBAC model, a subject can have more than one role or be a member of many groups. For example, an employee within an organization can be a member in secretaries group and employees group [10].

Task-Role Based Access Control (T-RBAC) model is another access control approach that has been proposed, that is based upon the RBAC model (Oh and Park, 2003). However, it assigns permissions to tasks instead of roles. Users in this model are assigned roles, which are assigned tasks that have permissions relevant to it. It uses the workflow authorization model for synchronizing workflow with authorization flow work togaher. The scheme has used tasks to support active access control and roles to support passive access control.

The RBAC model has many advantages compared to, DAC and MAC models, yet it has its own difficulties and problems, issues when it is deployed in the real-world. Firstly, picking the right roles that represent a system is not an easy task to do and dividing subjects into categories based upon roles might make things worse [11].

Roles in the RBAC model, classify subjects in a number of possible categories; thus each subject has to have a role in order to access the system. Despite that, roles can give a subject more rights than s/he necessarily needs to have, with a possibility of having another role which could lead to the violation of the access security policy.

It fails to handle these issues:

- It does not provide any kind of sensitivity level to the information. For example some information is more sensitive than others such as the medical history in a patient file.
- Relationships are defined according to identities not just roles such as the doctor patient relationship. E.g. a paediatric doctor should not be allowed to access a patient file in the psychology department of hospital.
- It does not support the delegation principle, which is a need in organization for dealing with absences of their staff. Furthermore, it does not consider the time and location constraints, which are utilized for restricting access to system files and minimizing the probability of information leakage. It also fails to deal with dynamic and random behaviors of users.
- It does not support active responsibilities of staff as it does not separate tasks form roles. Moreover, dynamic activation of access rights for certain tasks is not supported.
- The RBAC has to deal with a lack of sophisticated semantic models to represent and communication privileges. For instance, a doctor in a remote area might not be able to access the system via cloud computing due to lack of syntactic and semantic support. It also has to deal with a semantic gap between the user authentication mechanisms and the authorization mechanisms.
- In cloud computing, there is a large demand for testing and verifying access control functions, which are considered as static tests. There are also other dynamic compliance functions that can be used as support functions; for example reporting alerting privileges or conflict of rules and monitor the system current states. For instance, a doctor who has full access to patients' files in his/her department should not be allowed to move, copy them to another place or even access them from home should be restricted [12].
- Before utilizing the RBAC in cloud computing, it has to assure granting access decisions in a reasonable time and according to system requirements. For example, the response time is critical in many applications such as a health care system. A consultant away from a hospital needs to access the system in a timely manner, disregarding a number of access requests to the RBAC and distance.
- Any critical infrastructure service provider who aims to migrate to the cloud, with thousands of users, hundreds of roles, and millions of permissions face a tremendous task that cannot realistically be centralized by a small team of security administrators that makes it so difficult to migrate [14].

In a health care system, there is always a sequence of operations will need to be controlled. For example, a doctor in order to give a patient the right treatments, s/he needs to check the patient's physical conditions, look at the patient's medical history and asks for tests or scans. S/he might ask for help from another doctor or transfer some information to another hospital. Each one of the last operations needs a different set of permissions. Thus, the RBAC may not be able to ensure access for a continue of operations in cloud computing.

6 ATTRIBUTE BASED ACCESS CONTROL MODEL (ABAC)

The Attribute Based Access Control (ABAC) model relies on a set of attributes associated with a requester or a resource to be accessed in order to make access decisions. There are many ways to define or use attributes in this model. An attribute can be a user's work start date, a location of a user, a role of a user or all of them. Attributes may or may not be related to

each other [4]. After defining attributes that are used in the system, each attribute is considered as a discrete value, and values of all attributes are compared against set of values by a policy or decision making point to grant or deny access [15].

These kinds of models are also known as either Policy-Based Access Control (PBAC) or Claims Based Access Control (CBAC). Moreover, a subject does not have to be known in advance to the system, it just needs to authenticate itself to the system then provide its attributes simply. However, reaching an agreement about what kind of attributes should be used, and how many attributes are take into account for making access decisions is a complex task in cloud computing environment. This model has not been presented and implemented for well-known operating systems [6],[7].

Proposing a security policy that can work accurately with this kind of access control model is essential, because the security policy is responsible for selecting the important attributes that are used to make access decisions.

7 RISK-BASED ACCESS CONTROL MODEL (RBAC)

Risk-Based Access Control model was proposed to deal with multinational organizations that face various kinds of policies and regulations. This model strives to use different kinds of risk levels with environmental conditions and use the principle of "operational need" in order to make access decisions. In Quantified Risk Adaptive Access Control (QRAAC), risk is calculated as risk ¼ V*P, where V is the information value that reflects the sensitivity level of the resource, and P is the probability of unauthorized disclosure, which reflects the responsibility of the user. The security policy in this model is dynamic; it is changed according to a variety of risk levels stated in the security policy [12],14].

However, this model is difficult to deploy in cloud because of the amount of analysis required and number of systems to be merged to compute risk levels. It needs expertise level that can deal with the model. Finally, security policies and environmental conditions need to be standardized as they play a crucial role on making access decisions [6].

8 ARCHITECTURE OF PROPOSED ACCESS CONTROL MODEL FOR CLOUD

Based on the analysis of the research carried out in the area, the architecture for the access control model in cloud computing environments is shown in the Figure

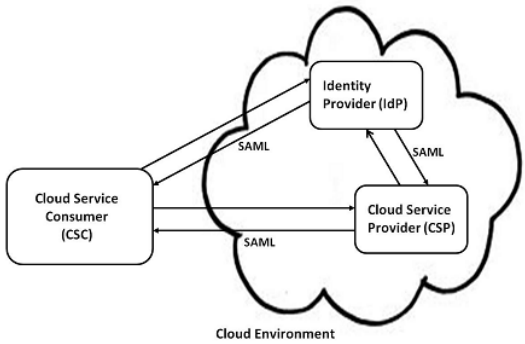

Fig. 2. Architecture of Access Control Model for Cloud

- Cloud Service Consumer (CSC)
- Cloud Service Provider (CSP)
- Identity Provider (IdP).

8.1 CLOUD SERVICE CONSUMER (CSC)

Cloud Service Consumer (CSC) put forward the request for the required resources or services hosted by the Cloud Service Providers (CSPs). Proper authentication of the CSC is necessary to ensure that unauthorized users can not access the services from the CSPs. The cloud users may subscribe to a variety of services depending on their organizational structure and requirements and normally they are charged based on a as pay-per-use model. The main functional modules/components of the Cloud Service Consumer (CSC) component are

- Trust Provider (TP)
- Access Control Request Handler (ACRH)
- Identity Provider Selector(IdPS)

8.1.1 TRUST PROVIDER (TP)

Cloud Computing involves multi-domain environments and the trust is an important part which needs to be built between the service provider and service consumers. The mutual trust between the service provider and service consumers and also between the providers of various services and the identity providers has core importance especially in the case of distributed systems like cloud computing or other computing service. This module also takes into account the trust values or information of the entity from other Trusted Third Parties (TTP).

8.1.2 ACCESS CONTROL REQUEST HANDLER (ACRH)

This module deals with the access requests when the CSC tries to access the services hosted by the service provider. It also then establish contact with the Identity Provider Selector (IdPS) module so that the Identity Provider (IdP) could be selected to meet the identity management requirements for the communication between the entities.

8.1.3 IDENTITY PROVIDER SELECTOR (IDPS)

The service consumer must has to select a suitable Identity Provider (IdP) in order to get the identificantion token, so that it can be used to access the various services hosted by the Cloud Service Providers (CSP).

8.2 CLOUD SERVICE PROVIDER (CSP)

The Cloud Service Provider hosts and provides a variety of services and/or resources for the service consumers. In order to avoid unlawful or unauthorized access, proper authentication and authorization of the CSCs are compulsory at every stage of access. The cloud computing enables the service providers to present many services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). In SaaS service, the softwares can be used by the user without actually purchasing or installing the required software on the user's computer. For example Google Apps. In PaaS service, the development platform provided from the cloud service providers and the users can use that platform to design and develop cloud-based applications. e.g. Google App Engine. In IaaS service, the computing infrastructure like CPU/processor cycles, storage space etc. are provided by the service providers and the users can utilize these resources as per their resource requirements. For example Amazon S3, Elastic Cloud (EC2) etc. In order to gain effective interaction between various service domains and user domains, the service providers wil support the identity federation by integrating the security tokens using standards such as SAML or OpenID generated by the Identity Providers.

The major different modules of the Cloud Service Provider (CSP) are given below

- Authentication (AuthnN)
- Authorization (AuthzZ)
- Policy Conflict Manager (PCM)
- Identity Provider Selector (IdPS) and
- Trust Provider (TP)

8.2.1 AUTHENTICATION (AUTHN)

This module verifies the identity of the requestor by interacting with the identity provider component by using identity tokens such as SAML assertions. The CSP has many IdPs enlisted in its trusted domain. The CSP and the CSC agree on a specific IdP for subsequent interaction between them.

8.2.2 AUTHORIZATION (AUTHZZ)

This module verifies the access rights of all cloud service consumer (CSC) and initialize the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP) components. PEP contacts with PDP for validity of the access request. PDP accesses the local policy database stored alongwith the CSP. PDP also contacts with the Policy Conflict Manager (PCM) model to solve the

policy conflicts, come out of various users trying to access different resources in an organization at the same time. Proper break-glass mechanism needed to be implemented with the PDP in order to handle emergency access requests. The decision made by the PDP is implemented properly by the PEP.

8.2.3 POLICY CONFLICT MANAGER (PCM)

In order to satisfy any access request by any of the cloud user, the access control mechanism has to make sure that the organizational rules and security policies are enforced thoroughly & properly. Policy conflicts, faced by the various access requirements and made by different users are handled by this module before taking any final access decision.

8.2.4 IDENTITY PROVIDER SELECTOR (IDPS)

The role of identity provider selector module in the CSP is to select the trusted IdPs in its domain. IdPS interacts with the trust provider model to get the current trust value of different IdPs. This module do interacts with client or CSC to determine the IdP to select it for authenticating the user before accessing the services hosted on the cloud server, and then selection is based on various factors such as the type of the service requested and preference of user for security and privacy. CSP contacts with the identity provider for authentication of the cloud user.

8.2.5 TRUST PROVIDER (TP)

The role of trust provider module at the cloud service provider (CSP) is to calculate the trust value of cloud service consumers based upon different parameters such as the previous experience with the customer & the current repo value collected from other trusted third parties (TTP). This module also find out the trust values associated with the different identity providers again based on the aforesaid mentioned factors to decide upon the identity providers to be selected as truthful. This trust calculation should adopt dynamic mechanisms as the trust values of a variety of entities change from time to time during transactions.

8.3 IDENTITY PROVIDER (IDP)

In Cloud Computing, a user or an organization may subscribe to services from multiple service providers in order to meet the resource requirements. This scenario underlines the urgent requirement for the proper identity management in cloud computing. Federated identity management approach (like Single Sign-On authentication) is required for the current cloud computing scenario. The cloud users in a cloud federation are not required to use multiple credentials each one for every cloud service provider or service they subscribe to. The CSCs can use the identity tokens generated by the Identity Provider (Ping Identity, Symplified etc.). The users exchange the security tokens (normally SAML assertions) generated by the Identity Provider with various Cloud Service Providers in the federation.

8.4 WORKFLOW MODEL FOR THE ACCESS CONTROL IN CLOUD ENVIRONMENTS

The model of workflow for the access control in cloud computing environments is shown in the Figure 3. It is shown in the figure the different steps performed by the CSCs, CSPs and the IdPs during the contact are given below

- A cloud service consumer i.e. (CSC) wants to access and use the service hosted by the cloud service provider and initiates the access request.
- In the first step dynamic trust value of the CSP is calculated by the CSC which is based on the previous transaction performed and the information provided by the trusted third parties (TTP).

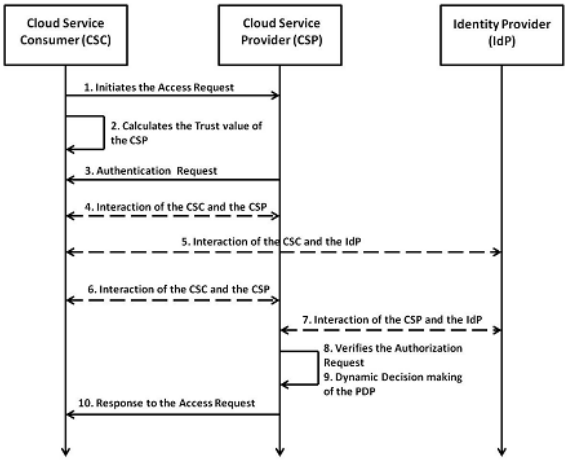

Fig. 3. Workflow Model for the Access Control in Cloud Environment

- The authentication request is sent to CSC by the CSP.
- The CSC communicates with the CSP to decide the suitable IdP based on the type of service request and the security's preferences. It is assumed that the cloud service provider (CSP) selects the IdPs in which is available in its trusted domain relying on the trust values of different IdPs, and also based on the previous history of communication and, the trust and/or reputation value provided by other trusted entities.
- The CSC then communicates with the selected IdP to get the security tokens (e.g. SAML assertions).
- The CSC then contacts with the CSP, using the tokens issued in the step (v) by the IdP.
- CSP verifies and run the authentication process of the CSC by interacting with the IdP.
- Authorization request is handled by the PEP & PDP modules of the CSP.
- PDP decides whether the request could be allowed, by contacting the local policy storage database. It also considers the policy conflict management, dynamic trust management of the CSC and the proper break-glass mechanism for dealing with the user requests.
- The response to the access request is communicated to the CSC.

9 ANALYSIS AND RESULTS

As far as the confidentiality and privacy of the cloud computing scenario is concerned, Distributed Access Control is an issue which needs the proper design and deployment of its solutions. Dynamic trust management of various cloud service providers and cloud consumers requires further research and effective solutions. Protecting the privacy of the various cloud consumers is of paramount importance in the widespread acceptance of the cloud computing paradigm.

The analysis of the work carried out in this area reveals that most of the works do not give effective approaches for the dynamic policy conflict management, and hence needs to be explored further. Also, efficient break-glass mechanism should be associated with the authorization process to deal with the emergency access needs in the cloud environments, while developing an efficient, reliable and scalable access control mechanism.

10 CONCLUSION

The security issue is the biggest barrier when promote and apply the cloud computing technologies on a large-scale. Yet cloud computing security related researches are still at the initial stage. In cloud computing the users' data are stored in the clouds, the confidentiality of the data is facing great challenge. As the key technology of information security, the technology of access control is an important mechanism for privacy protection in cloud computing, and it is also an important approach to avoid the data in the clouds being illegally accessed, distorted and used. With the popularization of cloud computing, people's attention to the confidentiality of data will be continually enhanced, and the researches in this field will get more and more intensive.

ACKNOWLEDGEMENT

The work presented in this manuscript is accomplished under the sympathetic attitude, animate directions, observant pursuit, scholarly criticism, cheering perspective and enlightened supervision of **Mr. NayyarIqbal, Lecturer Department of Computer Science University of Agriculture, Faisalabad**. His effort towards the inculcation of spirit of handwork and maintenance of professional integrity besides other valuable suggestions always serves as a beacon light through the course of my life.

REFERENCES

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," Version 15, 10709,http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf.

[2] Yonghe Wei, Chunjing Shi, Weiping Shao, "An Attribute and Role based Access Control Model for Service-Oriented Environment", in Proc. Chinese Control and Decision Conference, 2010, pp. 4451-4455

[3] Chang. N. Zang, Cungang Yang, "An Object-Oriented RBAC Model for Distributed System", in Proc. Working IEEE/IFIP Conference on Software Architecture, 2001, pp. 24-32.

[4] J.-C. Birget, X. Zou, G. Noubir, B. Ramamurthy, "Hierarchy-Based Access Control in Distributed Environments", in Proc. IEEE International Conference on Communication, 2001, vol.1, pp. 229-233.

[5] Cungang Yang, Chang N. Zhang, "Designing Secure ECommerce with Role-based Access Control", in Proc. IEEE International Conference on E-Commerce (CEC03), 0-7695-1969-5/03, 2003.

[6] Wei Zhou, Christoph Meinel, Vinesh H. Raja, "A Framework for Supporting Distributed Access Control Policies", in Proc. 10th IEEE Symposium on Computers and Communications, 2005.

[7] Yuri Demchenko, Cees de Laat, "Domain Based Access Control Model for Distributed Collaborative Applications", in Proc. Second IEEE International Conference on e-Science and Grid Computing, 2006.

[8] Bo Lang, Zhibin Wang, Qingwen Wang, "Trust Representation and Reasoning for Access Control in Large Scale Distributed Systems", in Proc. 2nd International Conference on Pervasive Computing and Applications, 2007.

[9] Jin Wang, Daxing Li, Qiang Li, Bai Xi, "Constructing Role-Based Access Control and Delegation Based on Hierarchical IBS", in Proc. IFIP International Conference on Network and Parallel Computing-Workshops, 2007, pp. 112-118.

[10] Clara Bertolissi, Maribel Fernandez, "An Algebraic-Functional Framework for Distributed Access Control",in Proc. Third International Conference on Risks and Security of Internet and Systems, 2008, pp. 1-8.

[11] Fujun Feng, Chuang Lin, Dongsheng Peng, Junshan Li, "A Trust and Context Based Access Control Model for Distributed Systems", in Proc. The 10th IEEE International Conference on High Performance Computing and Communications, 2008, pp. 629-634.

[12] Chang Chaowen, Wang Yuqiao, Liu Chen, "Analysis and Design of an Access Control Model Based on Credibility", in Proc. International Conference on Computer Engineering and Technology, 2009, pp. 312-315. Henryk Krawczyk, Pawel Lubomski, "Generalised Access Control in Hierarchical Computer Network", in Proc. 2nd International Conference on Information Technology, Gdansk, Poland, 2010, pp. 121-124.

[13] Lingli Zhao, Shuai Liu, Junsheng Li, Haicheng Xu, Lingli Zhao, Shuai Liu, "A Dynamic Access Control model based on Trust", in Proc. 2nd Conference on Environmental Science and Information Application Technology, 2010, pp. 548-551.

[14] Faith Turkmen, Eunjin (EJ) Jung, Bruno Crispo, "Towards Run-time Verification in Access Control", in Proc. IEEE International Symposium on Policies for Distributed Systems and Networks, 2011, pp. 25-32

[15] Anil L. Pereira, "RBAC for High Performance Computing Systems Integration in Grid Computing and Cloud Computing", in Proc. IEEE International Symposium on Parallel & Distributed Processing, 2011, pp. 914-921.