ADCAIJ: Advances in Distributed Computing and Articial Intelligence Journal
Regular Issue, Vol. 7 N. 1 (2018), 13 -28
eISSN: 2255-2863
DOI: http://dx.doi.org/10.14201/ADCAIJ20187113 28

Secure data access control with perception reasoning

Abdul Rauf[a], Abdul Hanan Abdullah[a], Abdul Mateen[b], Mahmood Ashraf[b]

[a]Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia
[b]Department of Computer Science, Federal Urdu University of Arts, Science & Technology, Islamabad, Pakistan
abdulrauf2000.pk@gmail.com, hanan@utm.my, abdulmateen@fuuastisb.edu.pk

KEYWORD

Secure Data; Access Control; Context Aware; Entities Management; Reasoning Mechanism

ABSTRACT

In spite of all security issues in the cloud system, distributed cloud environment requires an access control model which should be context aware to handle all issues intelligently. It must include role activation process based on the user's context information. In role activation process, the knowledge of reason used for data collection and usage is declared; this can allow the administrator to declare the policies which are context based. Therefore, there is dynamic activation of role permission due to the association of role with context. The complications in the role based access control model reduced by classifying the users into classes or groups having their own access control standards. Access to specific resources and granting/ denying is based on requesting the user identity. Cloud environments consist of different entities, number of resources and user where general access control model fails to cover all the aspects. Here, in the proposed access control with perception reasoning, entities are extended using Extensible Access Control Mark-up Language (XACML) where trust module monitors the random and dynamic behavior of the user with recognizing and restricting the malicious user for illegal data access. By issuing and identity tag to malicious user includes classification of task and data tag with data in the database.

1. Introduction

Cloud computing is scalable in which users have unlimited ability of processing and storage due to its broad network accessing ability. It is also considered as a reliable service, where users have to deliver different resources across the internet. It promotes organizational production, development and provides novelty of resources. The cloud computing has offered various characteristics such as provide shared infrastructure, dynamic provision of software automation, online accessibility of resources and online meeting [1].
Once the cloud setup is established, cloud services are deployed in terms of business model which are based on requirements. The cloud computing reduces the cost and complexity, to retain and operate processes of computers and networks [2].

Cloud deployment model classifies the clouds into four different categories which are Public, Private, Hybrid and Community clouds. In case of Public cloud, services are introduced over the internet through web

applications and users. However, in Private clouds, users have access of resources which are limited to the customers belonging to that enterprise only. Combination of Public and Private Clouds are called Hybrid which is the third category of cloud. While in Community cloud, resources are distributed among different users for further sharing that are managed by third party [3].

In cloud computing environment, there are some security measures beside its advantages such as different threats and attacks, vulnerabilities, which are classified into taxonomy. These security issues are either from cloud providers or customers. Generally, threat is an attack that affects the resources and other information whereas vulnerability is a flaw that makes it possible [4]. Access security issues [5] are mostly common in SaaS systems; SaaS applications should provide suitable access conditions. It is very difficult to found cloud attack vectors from inside and prevent them from causing data leakage. The cloud can face different attacks from inside and outside position. Another attack is malicious insiders, where the inside position taking over and control the physical security and get into the systems and cause of huge data leakage. It can also cause the removal of security-specific kernel modules thus; transparency, breach notification and compliance reporting can be used to prevent such attacks caused by malicious insiders. Whereas, the ones who can access the virtual machines and can install any software are called malicious system administrator, they can attack through the memory of customer's virtual machine and promoting attacks from the outside position.

Authorization is one of the major information security measure used to avoid several security issues in a cloud computing system by maintaining integrity. Third party authorization could be dangerous for applications and able to access the private information. Moreover, phishing attack made to compromise authorization. Thus, coarse authorization control models illustrated by service management interfaces. System administrators are responsible for managing authorization. Identity management related with the identification of entities. This identification is based on the pure identity, service paradigms and log-on. In this case, pure identity refers to the management of identities irrespective of access and entitlements.

Due to highly distributed cloud environment[6], domain suffered to handling different entities at different cloud regions. In order to fulfill these requirements, a strong relationship is requiring between resources and users. Access to specific resources, granting or denying based on requesting user identity. To deal the dynamics of cloud environment, cloud computing major need is to develop a strong multiple relationship between user and resources. There is reasoning to access these resources. If reason to access is valid then user are allow to access the resources, If invalid reasons, restrict the user to access these resources. Secure data access control with perception reasoning (SDACPR) model introduced to overcome the limitations due to the traditional models in the cloud system by considering it is as configuration points. Further, the enhanced access control model can defines the relationship between multiple entities. In order to define, a strong relationship between resources and user is provided by the Administrator who knows reason to access resources i.e. which user has to access when and what type of data. It will provide secure entity management and privileged authorization to the user without compromising the rights of the end specific users in the cloud computing environments. It also includes identification of random and dynamic behavior of the malicious user, and stops that unauthorized user for illegal data access.

Rest of the paper is organized as follows: section 2 defines the different approaches that deal with various access control models. Section 3 presents and discusses the steps of our proposed role based access control in detail. To evaluate the performance of the Secure Data Access Control with Perception Reasoning (SDACPR) model simulation setup and results are presented in section 4. Finally, section 5 is dedicated for analysis and section 6 concludes the paper.

2. Related Work

RBAC cannot provide us dynamic access control over the resources of cloud computing environment because there is no context aware element. One of these discoveries include the utilization of adaptive access control algorithm according to which the access control is based upon AAC[7], time constraints and context technology. These varying properties are associated with the traditional RBAC model to bring the security by building trust levels for the users. However, such a mechanism lacks the location constraints and has difficulty in

measurement of these trust levels. Distributed RBAC[8] and cloud optimized RBAC models[9] are associated together to provide increased scalability and flexibility to the system by allowing the single data manager to control. In order to get the certifications according to the requirement of the system but such system finds it difficult to deal with heterogeneity and security levels/ domains. Another access control model which includes semantic access control scheme in association with RBAC[10] is used in the health care units under various attributes but it is unable to deal with the complexity of the environment. These health care units utilize another access control model that is based on the association of TRBAC and workflow authorization depending upon the active/ passive workflows that ultimately activates the permissions and could result in certain security problems[11]. On the other hand, more than one role was assigned to an individual user. In case of RBAC, association with ontology framework in which the ontology domains control the hierarchical roles[12]. Later ABAC and RBAC were associated which results in the formation of ARBAC model that enhances the privacy of system. . Another way by which the privacy of the RBAC enhanced is the association of role activation process based on the context information.

A major property of this process involves delegation principle[13], reason mechanism and security environment. These properties maintain a hierarchal order in which the roles assigned to the users after which the task grabs the permission. Usage based access control (UBAC)[14], Service based access control (SBAC)[15] and Trust based access control TBAC [16] are not role based. In UBAC, main feature is attribute mutability and policies are combined with the application, so that policy and application become independent from each other. In this model subject attached with attribute and object is consider as entity, with these object there is associated rights. This model verifies user access periodically for authorization but this model does not support the private cloud environments. However, with the increase in number of users, data leakage also increases. As compared to UBAC, SBAC is more difficult to implement, and highly unsecure because of transmission of user credential to outside enterprise. It has no control over the information leakage and users are allowed on the bases of their trust level. User, Role, and relationship among different entities define semantically. The broker grants these permissions semantically. In Trust management models, trust is associated with the identity and behaviors, based on the concept of experience to access trust correlation and its deviation. There may be a direct or indirect trust. Nevertheless, in multi-domain environments of cloud, this strategy fails badly. Sometime, this strategy presents false recommendations and that's why not an ideal method to deal with the security. Contract RBAC[17] model do not provide the context reasoning for administrator or user and cannot protect information leakages. The set of locations related to entire factors of the cloud computing system is known as the spatial state which is not defined. In context RBAC[18], where integrity breach is used, trust level platform loss credibility, integrity assurance in full life cycle, and trust relationship is not defined. Mostly in ARBAC[19], bahviour of the user are un-controlable, no protection of data from the unsecure access, and no access control within the cloud envoirnment. It was earlier implimented in the grid envoirnment. ABAC[20] is not appropriate for the Multi-Tanancy of the cloud envoirnment [5]. In this model, there is no such machanism for registration of devices and entity management. The trust mangment model which is presented in [21] also fail to escape the false recommendations. Ontology based access control[22], detects and prevents insider intrusion, but fails to protect the system agianst intruders. The access control model comparison is shown in Table 1.1 having columns context-awareness parameter like time, location and platform trust, malicious insider, malicious outsider and cloud environment support.

Table 1.1: Comparison between various Prevailing Models.

Access Control Models	Context			Malicious Insider	Malicious Outsider	Cloud Environment Support
	Time	Location	Trust			
DAC	×	×	×	×	×	×
MAC	×	×	×	×	×	×
RBAC	×	×	×			√
UBAC	√	√	×	×	×	√
SBAC	√	√	√	×	×	√
TBAC	×	×	√	×	√	○
ARBAC	√	√	×	×	×	○
CA-RBAC	√	√	√	×	×	√
Contact-RBAC	×	×		×	×	√
Ontology-RBAC	√	√	×	√	×	√

Legends: "√" supported "×" unsupported "○" partially supported

The proposed access control model is the combination of role and task that is promoted by the T-RBAC followed by the assignment permission. Tasks are classified into sub-tasks and task instances by using the Principle of Dependence. This classification grabs permission to the various users to access resources. Furthermore, the security mechanism followed by an authorization process, which is divided, into three stages. According to this, the first stage refers to the starting activity, which followed by the core activity and finally the end condition. These mechanisms initiated by the workflows, which are either active or passive[23]. Due to highly distributed cloud environment, domain suffered to handle entities at different cloud regions. Certain relations in T-RBAC model[24] includes user-role assignment, task-role assignment and permission task assignment to overcome the deficiencies. In cloud computing environment, the user is only able to access the resources if he/she comes with a valid reason to access the data. Only the individual with the permission can get the resources after undergoing authentication and authorization[25]. That's why our proposed model uses task role based access control (TRBAC)[26].

The proposed model consists of objects, which are applications that logically bound in it representing the departments in an organization for flexible cloud environment. Multiple domains linked together by reasons and domains, where roles act as participants for preceding the job functions by the employees in order to access resources, and used for entity management. The Proposed Access Control model is appropriate for highly distributed cloud computing environment; there is registration of user as well as devices. The RBAC mechanism roles are arranged in the hierarchy according to their respective applications. These roles are assigned and separated dynamically or statically to avoid any loss of information. The RBAC model which uses the knowledge of reason for data collection and its use, can allow the administrator to declare the policies which are context based. User credentials are protected and there is no third part involvement. The streamlines policy management and enhanced control is applied on access as well as administrative policies. Reason mechanism is implemented using extended XACML entities. After identification of malicious user by trust module, identity tag is issued to stop this user for illegal access to data. Following diagram shows the working of the proposed access control scheme.

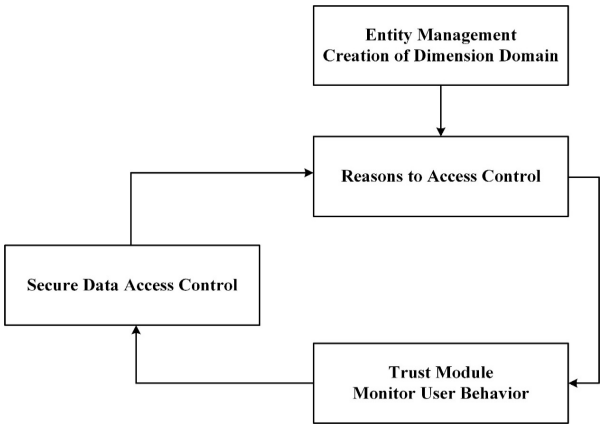

Figure 1: Working of the Proposed Access Control Model.

3. Secure data access control with perception reasoning

The traditional RBAC can be extended by using the knowledge of reasoning can allow the administrator to declare the policies which are context based. The extended RBAC with reason to access role assignment model is shown in Figure 2. By adding these role helps organization to know which user can perform what operation and on which object for what reasons. Different resources and user are managed creating dimensional domain. So all entities are logged and binding in extended RBAC environment. Trust module monitors the behavior of the user and identify if there is malicious user. After that an identity tag is issued to malicious user, classifies the task and attaches data tag to data according to tits sensitivity. This will restrict the malicious user to access the secure data.

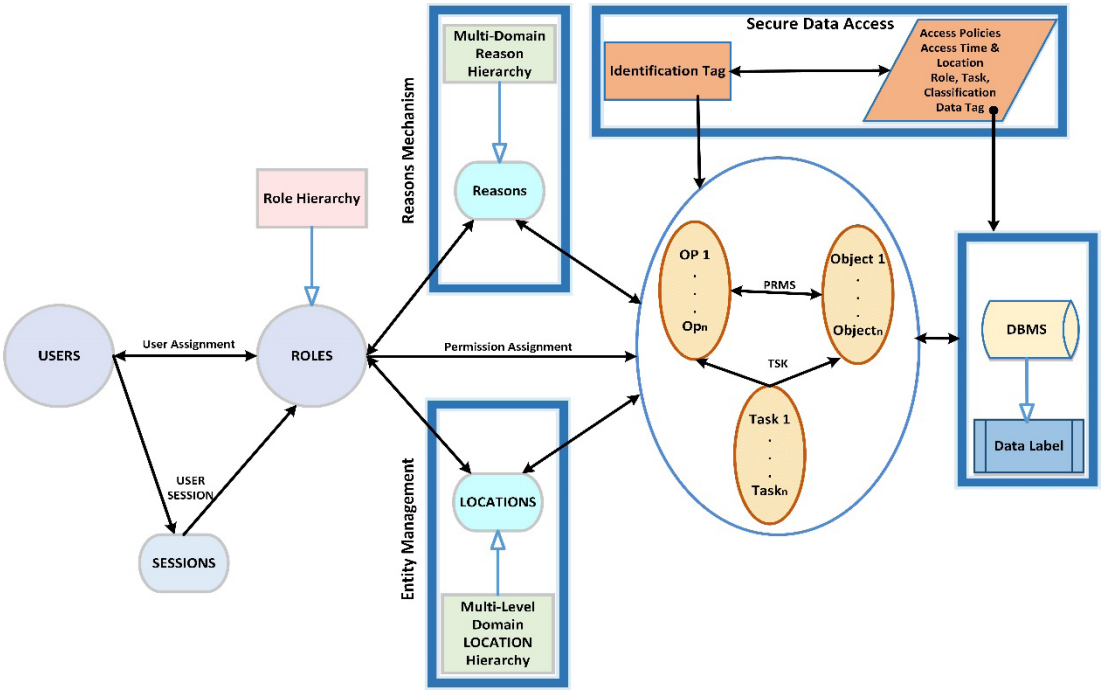

Figure 2: Secure Access Control with Perception Reasoning.

3.1. Basic Functions ⊢|Extended Entities

1. Set of subject $\vdash SUBJECT\ (subject)$
2. Set of User $\vdash Users(user)$
3. Set of objects $\vdash OBJ(obj)$
4. Set of Operation $\vdash OP(op)$
5. Set of TASK $\vdash TSK\ (tsk)\ \ | TSK = 2(OP\ \times\ OBJ\ \times\ Role)$
6. Set of permissions $\vdash PRMS(prms)$ | PRMS = $2(\mathrm{OP}\ \times OBJ)$
7. Set of physical locations $\vdash PL(pl)$
8. Set of logical locations $\vdash LL(ll)$
9. Set of Role $\vdash Role(r)$
10. Set of Session $\vdash Session(s)$
11. Set of dimensional reasons $\vdash DRS(drs)$
12. Set of dimensional reasons role $\vdash DRSR\ (drsr)$

3.2. Administrative Functions ⊢| Add / Delete, Activate / Deactivate Role

1. User role assignment $\vdash UA \subseteq\ USER\ \times\ DRSR$
2. Permission role assignment $\vdash PA\ \subseteq\ PRMS\ \times\ DRSR$
3. Reasons location assignment $\vdash RSLA \subseteq\ RS\ \times\ LL$
4. Dimensional reasons role and dimensional reasons $\vdash DRSRA\ \subseteq DRSR\ \times\ DRS$
5. Dimensional domain and dimensional reasons $\vdash DD_{DRS} \subseteq\ DDi\ \times\ DDj\ \times\ DRS$
6. Dimensional reasons and location $\vdash DA\ \subseteq DRS\ \times\ LL$
7. User Assignment (UA) $\vdash UA\ \varepsilon\ USER\ \cap\ DRSR$
8. Dimensional Reasons Role Assignment (DRSRA) $\vdash DRSRA\ \varepsilon\ DRSR\ \cap\ DRS$
9. Permission Assignment $\vdash PA\ \varepsilon\ PRMS\ \cap\ DRS$
10. Subject and user showing one-to-one mapping $\vdash Subject_{user}(s{:}SUBECT)\ \rightarrow\ (u{:}USER)$
11. Subject and dimensional roles showing one to one mapping $\vdash Subject_{roles(s:SUBJECT)} \rightarrow 2DRSR.$
    Formally $\vdash subject\_role \subseteq \{\ drsr\ \varepsilon\ DRSR\ |\ (subject\_user)(s),drsr)\ \varepsilon\ UA\}$
12. Roles and users showing one to one mapping $\vdash assigned\_user(DRSR) \rightarrow\ 2USER$
    Formally $\vdash assigned\_user\ (DRSR) \subseteq \{u\ \varepsilon\ USER\ |\ (u,drsr)\ \varepsilon\ UA\}$
13. Dimensional role and set of permissions showing one to one mapping $\vdash assigned_{prms}(drsr{:}DRSR)\ \rightarrow\ 2PRMS.$
    Formally $\vdash assigned\_prms\ (DRSR) \subseteq \{\ prms\ \varepsilon\ PRMS\ |\ (prms,drsr)\ \varepsilon\ PA\}$
14. Permissions and set of dimensional roles showing one to one plotting $\vdash prms\_roles\$\ (prms{:}PRMS)\ \rightarrow 2DRSR$
    Formally $\vdash prms\_role\ (prms) \subseteq \{\ drsr\ \varepsilon\ DRSR\ |\ (\ prms\ ,drsr)\ \varepsilon\ PA\}$
15. Relation among dimensional reasons role and set of dimensional reasons showing one to one plotting $\vdash assignedDRSR_{drs}(drsr{:}DRSR) \rightarrow 2\ DRS$
    Formally $\vdash assignedDRSR\_drs\ (drsr) \subseteq \{\ drs\ \varepsilon\ DRS\ |\ (\ drsr\ ,drs)\ \varepsilon\ DRSA\}$
16. Multi-level dimensional domain/ multi domain relationship and set of dimensional reasons $\vdash assignedDD\_drs\ (ddi,ddj)\ \rightarrow 2DRS$
    Formally $\vdash assignedDD_{drs}(ddi,ddj) \subseteq \{\ drs\ \varepsilon\ DRS\ |\ (ddi,ddj,drs)\ \varepsilon\ DD\_DRS\}$

17. DRS showing plotting among dimensional domain relationship and another dimensional domain $\vdash\rightarrow assignedDD\ (dd,drs)\ \rightarrow\ 2DD$

    Formally $\vdash\rightarrow assignedDD\ (dd,drs)\subseteq\{\ ddi\ \varepsilon\ DD\ |\ (dd,drs)\ \varepsilon\ DD\_DRS\}$

18. Dimensional reasons and set of logical locations showing one to many plotting $\vdash\rightarrow assigned_{drs}(drs)\rightarrow 2$

    Formally $\vdash\rightarrow assignedL\_drs\ (\ drs\ )\subseteq\{\ ll\ \varepsilon\ LL\ |\ (\ drs,ll)\ \varepsilon\ DRSRA\}$

19. DRS and set of logical locations showing one to many plotting $\vdash\rightarrow assignedDRS_l\rightarrow\ 2DRS.$ Formally $\vdash\rightarrow assignedDRS\_ll\ (ll)\subseteq\{\ drs\ \varepsilon\ DRS\ |\ (\ drs,ll)\ \varepsilon\ DRSRA\}$

3.3. Entity Management in Role Based Access Control

3.3.1. *Domain*

Logical bound over some space is called domain and it contains at least one object or list of objects. This object may be an application in fully or partially ordered domain. Domain represents departmental structure of an organization to provide us flexible means of portioning objects. Purposes and domains create a kind of relationship among domains. Roles represent participants in a domain and provide us a grouping mechanism for various jobs. This grouping mechanism is based on job function performed by the employees represents the organizational structure. Therefore, the system must identify and have complete knowledge of the domain, object and roles [27].

3.3.2 *Physical Layout of Domain*

Object had control using the domain administrator that also organizes network object and logical hierarchy. Each organization has some specific administrative requirement; administrator mostly uses delegation of authority and operation requirement to control various operations. So domain is logical structure that is used to manage administrative requirement of the organization. Some of the key features of the proposed physical layout of domain are:

i. Context Collection.
ii. Reasons Management
iii. Policy Unit
iv. Reason Hierarchy Management.
v. Dimensional Reasons Role (DRS) and Dimensional Domain (DD) Relation Management

Physical layout have the following characteristic, include context collection, reason management, policy management unit, reasons hierarchy management, dimensional reason role and dimensional domain relation management. Physical domain consists of reason module and policy unit. Reason module contains the context collector which uses the contextual information from the context analyzer; this information is generated through context generator in the reason module. The Reason module consists of reason manager, user reasoning mechanism where reasons are activated through the reasons activator and is also responsible to maintain the Reason Hierarchy. Additionally, it also contains Dimensional Reasons Manager (DRS) for maintaining the dimensional reasons at both generalized local hierarchy (GLH) and specific local hierarchy (SLH) level through DRS-GLH allocator and DRS-SLH allocator by means of DRS transmitter. This technique is based on the context values in order to capture the reasons. Physical layout of the domain is shown in the diagram given below that represent trust relationship in the model.

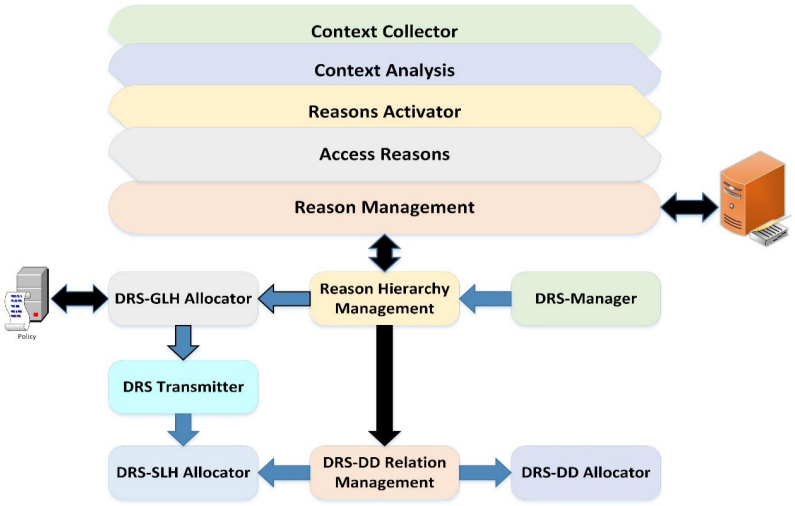

Figure 3: Physical layout of domain.

Response time at GLH is less than that of SLH, but response time increases as the number of logical or physical location defined by GLH and SLH increases. Figure shows the response time for reasoning collection at GLH and SLH, based on user current contextual characteristics.

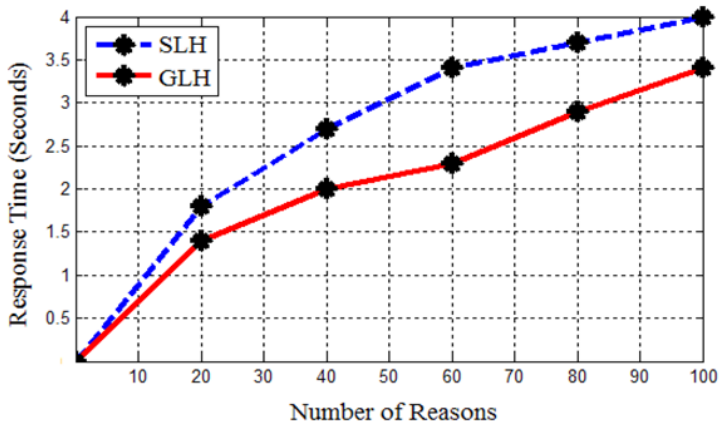

Figure 4: Reason Collection Response Time at GLH and SLH.

3.3.3. *Logical Layout of Domain*

Dimensional domain presents the information through a standardized and logical structure that helps to establish and understand the organization of domains and domain resources in a useful way. Main features of the logical structure of domain are efficiently used to implement policy of the organization, to manage the users and resources and software distribution. It is also used to facilitate public key management and domain-based distributed file system using XACML.

Dimensional Reasons $DRSslh < drsslh,rs,slh >$: this relation shows the location hierarchy at SLH level in the presence of dimensional reason while in case of physical location it is given as $SLH\_Occur\_pl(slh) \rightarrow DRSPS = \{pl1,pl2.....pln\}$ where $pl \in PL$.

In this case, reasons and dimensional domains were linked together through a relationship at SLH and GLH levels which are categorized as Internal Dimensional Reasons relationship and External Dimensional Reasons

relationship given as $(INT\_DRSDD)\ and\ EXT\_DRSDD$ respectively. $(slh\ is\ instance\ of\ glh)$ that shows the dimensional reasoning information defined by the general schema, from where specific schema is initiated.

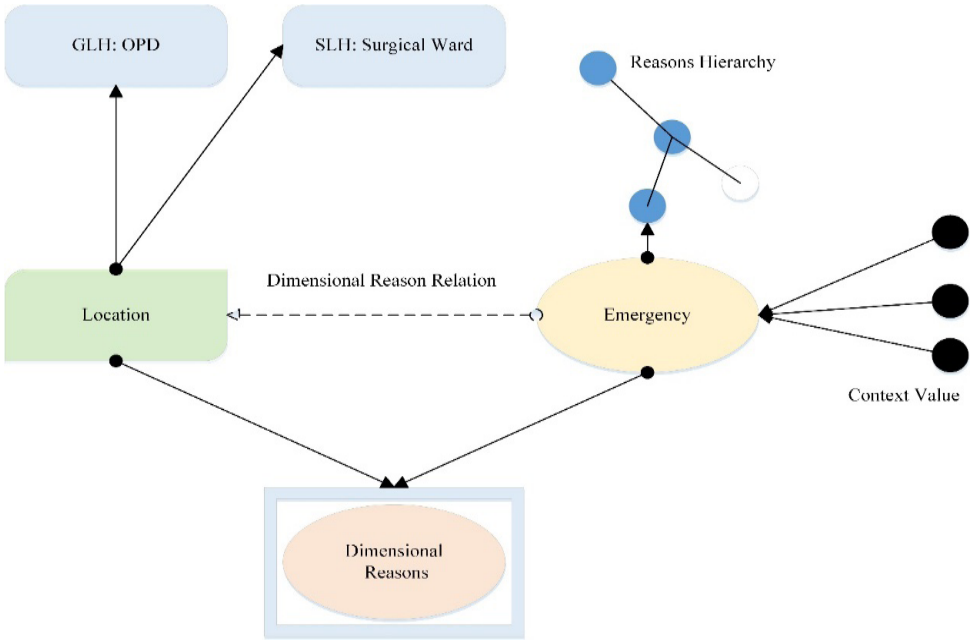

Figure 5: Logical layout of domain.

In GLH, set of physical location pl is defined that derives from the logical location ll and can find mapping response time. Figure 6 shows the response time to derive the physical location pl from a given GLH.

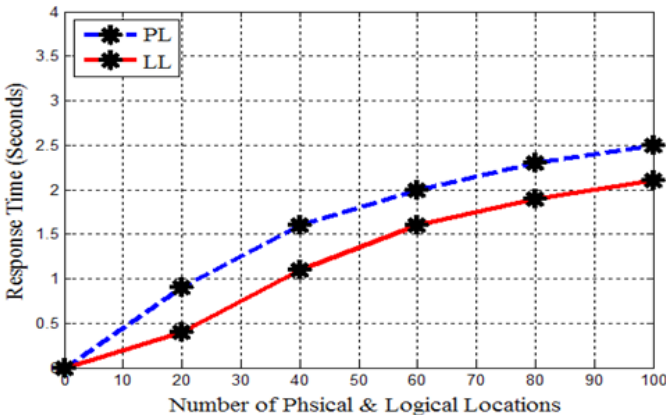

Figure 6: Response time of physical location (pl) & logical location (ll).

3.3.4. *Dimensional Domain*

Dimensional domain is a logically restricted surrounds with either one object or a list of objects and also containing dimensional reasons roles are called Dimensional Domains (DD). The system must recognize this dimensional domain. Dimensional Domain $DD\ <DD, DD\_HOP>\ DD$ is a dimensional domain name, DD_ HOP is a set of logical locations requiring the area restricted by dimensional domain such that:

$DD\_HOP: occurLDD\ (DD)\ \rightarrow\ ll\ \varepsilon\ LL$

Multiple Level Dimensional Domain:

Multiple level relationship if DD_1 and DD_2 then

Multiple Level Domain $(DD1, DD2)$ Æ $(ll2, ll2\ \varepsilon\ occur(DD2)$ Æ $(\exists\ ll1, ll1, \varepsilon\ occur(DD1) \wedge contains\ (ll1, ll2)$ contain (Æ ll_1, ll_2) Logical semantic of the relationship "contain".

Multiple Dimensional Domain:

Multiple Dimensional Domain relationship specified as If $ll_1$and ll_2 be the location such that $ll1\ \varepsilon\ DD1\ \ and\ ll2\ \varepsilon\ DD2$

Multiple Dimensional Domain Overlap

$$(DD1, DD2,\ drs)\ Æ\ (\ ll2, ll2)\varepsilon\ occur\ (DD2)\ Æ\ (\exists\ ll1, ll1, \varepsilon\ occur(DD1) \wedge\ overlaps\ (ll1, ll2)\ \rightarrow\ overlaps\ (ll1, ll2) \quad (1)$$

Multiple Dimensional Domain Disjoint

$$(DD1, DD2,\ drs)\ )\ Æ\ (\ ll2, ll2)\ \varepsilon\ occur\ (DD2)\ Æ\ (\ \exists ll1, ll1, \varepsilon\ occur(DD1)\ \wedge\ disjoint\ (ll1, ll2) \quad (2)$$

The proposed model considers reason as the intention of the user and estimated on contextual basis. According to basic functions $U\ \varepsilon\ Users, R\ \varepsilon\ Roles, T\ \varepsilon\ Time\ interval$ and L-ATR is a set of location attribute, so reasons to access is represented as RSA = U x R x T x L_ATR

3.4. Perception Reasoning

3.4.1. *Dimensional Reasons*

Dimensional Reasons are the set of reasons in which a relationship is established among the two different domains including set of logical locations. $DRSL\ =\ \{ll1, ll2, \ldots., lln\}\ where\ ll\ \varepsilon\ LL$ $DRS\ <\ drs, drl>\ drsa$ is the name of dimensional reason while drl is dimensional reasons location. The interaction among different domains is given in figure according to which dimensional reasons can be defined as:

$<\ Insurance, Hospital, Insurance\ Company\ \{insurance\ claim, Insurance\ marketing\}\ >$

Similarly, reasoning between multiple domains are defined as

$<\ Research, Hospital, University\ \{Laboratory\ Data\ Analysis\}\ >$

3.4.2. *Dimensional Reasons Role*

Dimensional Reason Role is represented as $DRSR\ <\ drsr, drsrl\_ext, drss\ >$ Where, $drsr$ is a role name, $drsl$ is a dimensional reasons location and drss is a dimensional reasons set. $drsrl\_ext\ =\ \{ll1, ll2\ldots., lln\}\ and\ ll\ \varepsilon\ LL$ $drss\ =\ \{drs1, drs2\ldots.\ drsn\}$ such that $drs\ \varepsilon\ DRS$. Function $occur\_ll$ can map logical location into sub-location such that $occur\_ll\ (ll)\ \rightarrow\ 2lt$

3.4.3. *Context Reasoning*

A reason can be captured related to the specific user by limiting each task for a particular reasoning but this is not suitable if multiple reasons exist. This drawback was facilitated by another method in which the reason is forward along with the request to access the task. Reason is the notion of the user for what it is trying to access a certain task given as Reason. $Reason(rs)\ \rightarrow\ DRSR\ x\ T\ x\ L\_ATR$ Introduced the time interval related to Dimensional Reason Role DRSR and attribute are L_ATR. Another relation with respect to session was given $L\_ATR:\ USL\_ATR(s)$ $s\ \varepsilon\ SESSION$. This case utilizes some terms such as role, time and location to capture the reason for a user as in this case the user is assigned by the roles at the same location for what it is requesting for. Minor and major operations reasons are linked together through a hierarchy for safe management as roles and other components in cloud computing environment. Such a hierarchy is given as $sp\ \leq\ sb$ which shows relationship among two different reasons as the constraints assigned to one operation is automatically assigned to another one. Secondly, this relation reasons a concept of General Location Hierarchy (GLH) and Specific

Location Hierarchy (SLH) level in which the reason and location are linked together. Dimensional reason is a link between location and the reason given as $DRS < drs, ll, rs >$.

3.4.4. *Reasons Hierarchy*

In the proposed model, relation between reasons and location is hierarchal and define as dimensional reason. In big organization for safe management, it is required that general location hierarchy (GLH) for particular user for generalized reasons is defined and all the constraints are applied to each hierarchal part. The specific location hierarchy (SLH) refers to multiple reasons with respect to user. As the reasoning implication request increases, in the same way response time also increases because user constant movement over the spatial domain is defined within the system. Single request takes about 40 milliseconds to compute reasoning from contextual characteristic, which is input for reasoning implication Algorithm. $GLH\_Occur\_ll(glh) \rightarrow DRSLS = \{ll1, ll2, \ldots\ldots\ldots lln\}$, where $ll \in LL$ relation shows a location hierarchy at GLH level in the presence of dimensional reason. Dimensional $Reasons\ DRSslh < drsslh, rs, slh >$ relation shows the location hierarchy at SLH level in the presence of dimensional reason while in case of physical location it is given as $SLH\_Occur\_pl(slh) \rightarrow DRSPS = \{pl1, pl2 \ldots\ldots pln\}$, where $pl \in PL$. In this case, reasons and dimensional domains were linked together through a relationship at SLH and GLH levels which are categorized as Internal Dimensional Reasons and External Dimensional Reasons relationship given as $(INT\_DRSDD)\ and\ EXT\_DRSDD$ respectively. $(slh\ is\ instance\ of\ glh)$ Showing system collect the dimensional reasoning information defined by general schema from where specific schema is initiated. So location garrulity become finer but response time increases.

Dimensional Reasons $INT\_DRSDD < drsDD, DD, rs >$: general relationship presenting the internal Dimensional Reasons within a dimensional domain which can be shown at both GLH and SLH level. Such a relationship at GLH level is given as

$General\ Set\ GS \rightarrow SchemaDomain(DD) = \{glh1, glh2, glen\}$
$Specific\ Set\ SS \rightarrow SpecificDomain(DD) = \{slh1, slh2 \ldots slhn\}$.

On the other hand, External Dimensional Reasons relationship is given as EXT_DRSDD that the access to resources by the users depends upon the request made by them. Dimensional Reason $EXT\_DRSDD < DDi, DDj, rs >$, this shows the external dimensional domain relationship in which contrary to internal dimensional domain relation only a specific reason can impart its constraints to the other as the result of which the access request could be made from all the locations either physical or logical.

3.5. Secure data Access

Proposed an access control system, in which the users are assigned their role according to reasoning mechanism but also classified according to their real jobs. Therefore, every task has a security classification for access and only required permission for completing this task. So this access control is not only ensuring the secure sharing of resources among untrusted users, but also support different access permissions for the same user and allowed the user to use secure multiple services[28]. Reasons mechanism is also used to deal with trusted behavior of users according to their access behaviors and give recognitions to user. In cloud computing system, sharing among various resources take place, which requires a security mechanism for avoiding information leakage and attack of certain intruders. Such models also comprise of certain classifications and some tags such as identity and data tags, which are responsible for accessing of resources and marking of data respectively. This classification is based on the sensitivity of the data lies in a hierarchal order Data tag is attached to the data identified by the system. Hierarchical ordered set of the data tag is utilized which are used to limit access according to the degree of security. A classification of task to access data is $\text{Secured (S)} > Concealed(C) > Isolated(I) > Public\ (P)$ which have to dominate an object data tag before access it. Employ same hierarchy ordered data tag set to classify the tasks. $\forall\ \text{tsk} \in \text{TSK} \rightarrow \text{scl} \in \text{SCL}, \forall\ \text{d} \in \text{D} \rightarrow \text{sl} \in \text{SL}$, task access object $\text{d} \leftrightarrow \text{scl dominate sl}$. The identity tag in untrusted environment $\forall\ \text{stsk} \in \text{STSK} \rightarrow \{ TSK_{R \in UA}, slc, USER_{currentlocation}, tsk, RS\}$ RS is (Context Reasoning) and $\forall\ prms \in PRMS \rightarrow \{Permission\ of\ read, write, execute\ and\ delete\}$ this model support supervision role hierarchy with strict inheritance. In case where one task depends on another

task, classification of tasks is used to complete a particular job. These tasks issue an identity tag to prevent any data leakages. Conferring to system security, data tag information is passed to application employed by the tasks, from top secret to unclassified. Figure given below shows the proposed data access control.

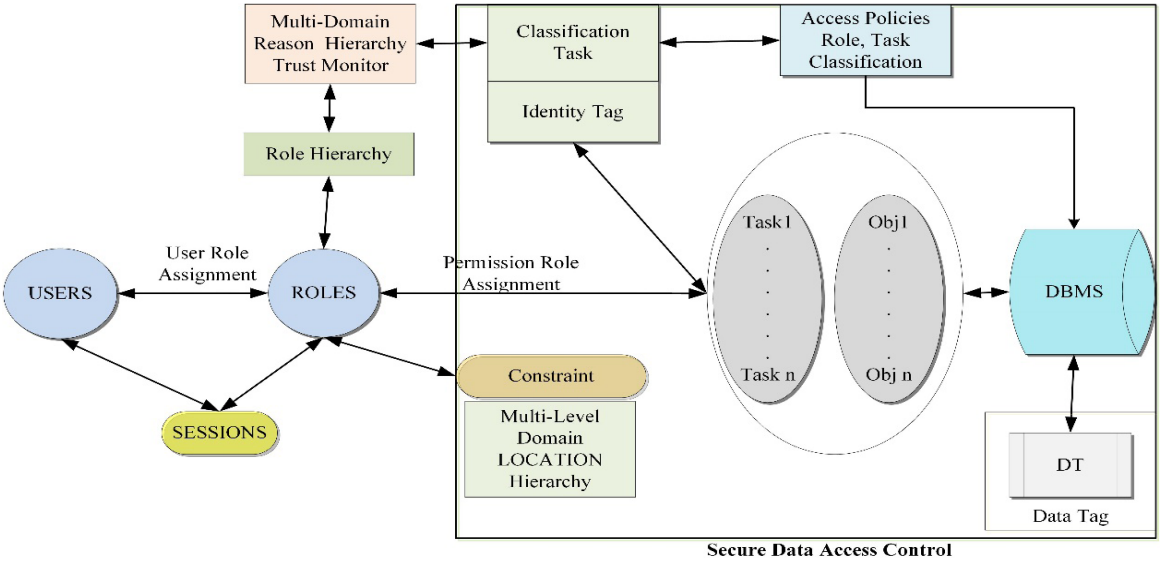

Figure 7: Secure data access control.

4. Simulation and results

4.1. XACML

Extensible Access Control Mark-up Language (XACML) [29] supports the idea of complex permissions used in the systems. Role hierarchies, permissions and permission role assignment are defined. So provide support to implement role-based access control models for the cloud computing environment.

Table 2: Extended Entities of CPR-TRBAC Model.

Extended Entities of SDACPR Model using XACML

CPR-TRBAC Entities	XACML Implementation
PHYSICAL LOCATION	<PL>
LOGICAL LOCATION	<LL>
GERNERAL LOCATION HIERARCHY	<GLH>
SPECIFIC LOCATION HIERARCHY	<SLH>
DIMENSIONAL DOMAIN OVER GLH	<GSDD>
DIMENSIONAL DOMAIN OVER SLH	<SSDD>
REASON TO ACCESS	<RS>
DIMENSIONAL REASON TO ACCESS	<DRS>
DIMENSIONAL REASONS ROLE	<DRSR>

4.2. Metrics of Evaluation, Scenarios and Performance

A scenario is developed to calculate the response time and access time in order to implement the reasons implication. Further the situation is extended the scenarios to derive dimensional granularity, dimensional reasoning and dimensional reasoning with role activation. Algorithm steps of scenarios for reason implication are:

i. Calculating the response time and access time
ii. Scenarios to derive dimensional granularity, dimensional reasoning and dimensional reasoning with role activation
iii. Conditions: with authorization & without authorization
iv. Performance measure in milliseconds and seconds

In following figure 8, the graph shows a relation between reasoning implications and response time according to which both are directly proportional to each other. This follows an implications algorithm that referred as input.

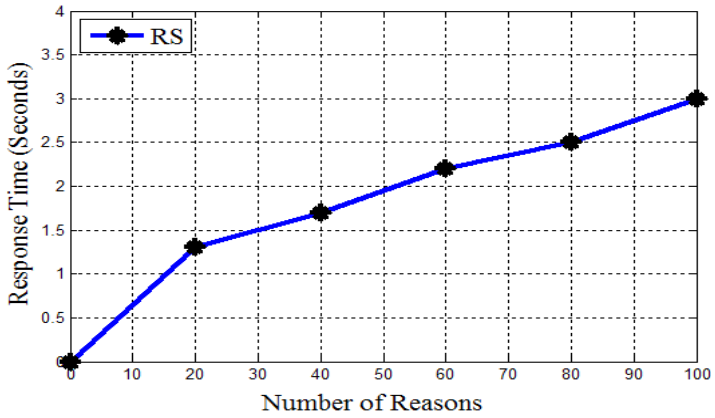

Figure 8: Graph show reasoning implication and response time.

Dimensional reason role and physical location pl, is activated by the system directly. However, in GLH, firstly derive all logical locations ll and finally considers its consistent physical locations. For this reason, dimensional reason role at GLH take more time as compared to dimensional reason role at physical location pl. Following figure shows the response time of dimensional reason role that is defined within system. Response time for dimensional reason role to activate at given GLH is shown in Figure 9.

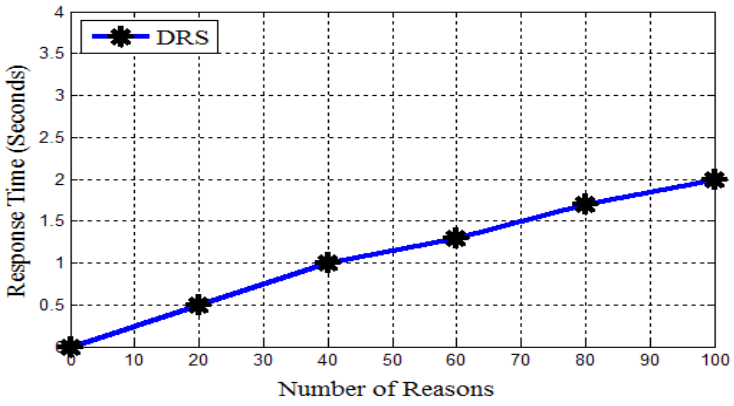

Figure 9: Response time for dimensional reason role to activate.

Above figure shows the response time that is required to enable the dimensional reason role, with different dimensional domain and reasoning. To verify the result enable one-dimensional reason role without reason role hierarchy, and enable several dimensional reasoning role with hierarchy. As hierarchy relationship constraint is applied and assessed on the contextual values, for this reason enabling of dimensional reasoning role done without hierarchy relation is less that is shown in following Figure 10.

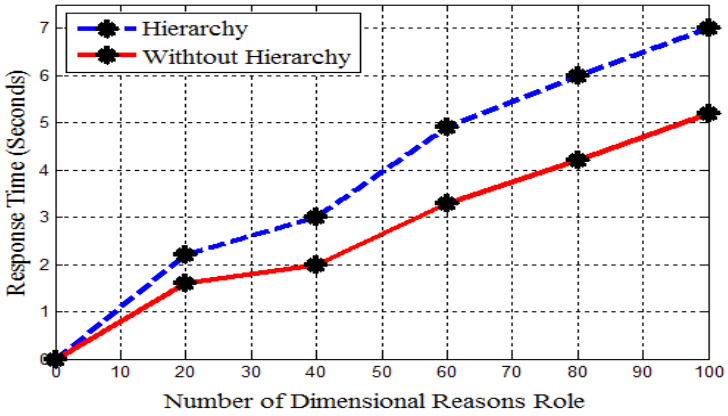

Figure 10: Response Time to enabled dimensional reasons role.

4.3. Analysis

In cloud computing system, users are assigned by the roles which are further assigned by the tasks according to their requirements. These tasks carry permissions that enable users to access different resources. These permissions have certain classifications and data tag that enable the access. Users which have been assigned tasks are under the control of reason mechanism that grant identity tags according to the dynamic and random behavior of the users. Above mentioned proposed security model for cloud is based upon time/ location constraints and delegation principles in order to fulfill the security requirements. Roles assigned to the users are very important for the proper working of the cloud computing system as all the access properties are under its processing. In an organization, these roles could be accounting, secretary and manager roles. Accordingly, the roles are referred as job tittles belonging to a particular user. Another major component of the security model is the task that is assigned to the roles and these tasks ultimately get permissions to the users to enable them to access resources. Each role in the system is assigned with a task that follows an authorization process for safe management of the system. Permissions are assigned to the users through the tasks assigned to them depending upon their dynamic behavior. This security models are based upon certain constraints and principles that are necessary to fulfill the security requirements of the system. Constraints like time/ location and principles like least privilege and SOD, are also important for safe management. Such models are also comprised of certain classifications and tags such as identity and data tags, which are responsible for accessing of resources and usage of data respectively. This classification is based on the sensitivity of the data lies in a hierarchal order from top secret to unclassified. Hence, these classification and tags are important for a system for proper working as without them access to resources is not possible. Another major component of this model is the reason mechanism that plays an important role in the safe management of the system. Identity tags assigned to the users according to their dynamic behavior is issued by the reason mechanism trust module. These identity tags help the users to access their required resources in a safe manner. Therefore the proposed model includes both the tasks and the roles supporting active and passive workflows respectively. Beside this, such a model deal with the large number of users according to their dynamic behavior while using heterogeneity techniques and imposing certain policies for safe management. There are two kinds of security environments, comprising of secure and unsecured environments. Secure environment does not require identity tags as only tasks assigned with roles and permissions are granted to users using reasons mechanism. However, in case of unsecured environment, identity tags are used at each step to maintain security.

6. Conclusion

In this research, various sources of security protection required by the cloud-computing environment are discussed. Task-role based RBAC model was enhance by introducing the knowledge of reasons in order to detect reasons in order to access the specific resource. The knowledge of the reasoning is introduced with the concepts of the dimensional reasoning, dimensional reason roles and other related terms. Dimensional domain is used to define the strong relationship between resources and user. In addition to this knowledge of reasoning, the proposed model named as reasoning RBAC offers the features of the traditional task-role based RBAC models, which is context aware with more flexibility and security. In addition, it encompasses the enforcement and implementation of the access control policies by means of policy syntax that is introduced in its mechanism. It provides a complete time/ location based, context based, reason oriented and temporal based access control in the cloud computing environment. The Proposed access control is implemented in "extensible access control markup language" (XACML) and windows 2012 policy server. Strong relation between users and resources are defined using domain. Such an approach results in a cloud computing environment that is free from security issues, privacy issues and other vulnerable attacks which ultimately leads to the required access control processing. It also provides secure access to data, and defense against malicious insider as well as outside attacks using secure the data access control.

7. References

1. Rittinghouse, J.W. and J.F. Ransome, *Cloud computing: implementation, management, and security*. 2016: CRC press.
2. Garg, S.K., S. Versteeg, and R. Buyya, *A framework for ranking of cloud computing services.* Future Generation Computer Systems, 2013. **29**(4): p. 1012-1023.
3. Kalloniatis, C., H. Mouratidis, and S. Islam, *Evaluating cloud deployment scenarios based on security and privacy requirements.* Requirements Engineering, 2013. **18**(4): p. 299-319.
4. Fernandes, D.A., et al., *Security issues in cloud environments: a survey.* International Journal of Information Security, 2014. **13**(2): p. 113-170.
5. Almorsy, M., J. Grundy, and I. Müller, *An analysis of the cloud computing security problem.* arXiv preprint arXiv:1609.01107, 2016.
6. Raju, R., et al. *A heuristic fault tolerant MapReduce framework for minimizing makespan in Hybrid Cloud Environment*. in *Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference on*. 2014. IEEE.
7. Younis, Y.A., K. Kifayat, and M. Merabti, *An access control model for cloud computing.* Journal of Information Security and Applications, 2014. **19**(1): p. 45-60.
8. Bhargava, R., R. Pramoda, and D. Mudugurki, *Dynamic RBAC Model for Cloud Computing.* 2015.
9. Li, H., et al. *A survey of extended role-based access control in cloud computing*. in *Proceedings of the 4th International Conference on Computer Engineering and Networks*. 2015. Springer.
10. Barati, M., et al. *A new semantic role-based access control model for cloud computing*. in *9th International Conference on Internet and Web Applications and Services, Paris*. 2014. Citeseer.
11. Pandey, S., et al. *Security enforcement using TRBAC in cloud computing*. in *Computing, Communication and Automation (ICCCA), 2016 International Conference on*. 2016. IEEE.
12. Liu, C.-L., *Cloud service access control system based on ontologies.* Advances in Engineering Software, 2014. **69**: p. 26-36.
13. Riad, K., et al. *AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing*. in *Collaboration and Internet Computing (CIC), 2015 IEEE Conference on*. 2015. IEEE.
14. Ghazi, Y., et al., *Usage-Based Access Control for Cloud Applications*, in *Innovative Solutions for Access Control Management*. 2016, IGI Global. p. 197-223.

15. Liu, J.K., et al., *Fine-grained two-factor access control for web-based cloud computing services.* IEEE Transactions on Information Forensics and Security, 2016. **11**(3): p. 484-497.
16. Lin, G., et al., *MTBAC: a mutual trust based access control model in cloud computing.* China Communications, 2014. **11**(4): p. 154-162.
17. Rehman, S. and R. Gautam. *Research on Access Control Techniques in SaaS of Cloud Computing*. in *International Symposium on Security in Computing and Communication*. 2014. Springer.
18. Satoh, I. *Toward Access Control Model for Context-Aware Services Offloaded to Cloud Computing*. in *Reliable Distributed Systems Workshops (SRDSW), 2016 IEEE 35th Symposium on*. 2016. IEEE.
19. Lo, N.W., T.C. Yang, and M.H. Guo, *An attribute-role based access control mechanism for multi-tenancy cloud environment.* Wireless Personal Communications, 2015. **84**(3): p. 2119-2134.
20. Ed-Daibouni, M., et al., *Toward a New Extension of the Access Control Model ABAC for Cloud Computing*, in *Advances in Ubiquitous Networking*. 2016, Springer. p. 79-89.
21. Manuel, P., *A trust model of cloud computing based on Quality of Service.* Annals of Operations Research, 2015. **233**(1): p. 281-292.
22. Choi, C., J. Choi, and P. Kim, *Ontology-based access control model for security policy reasoning in cloud computing.* The Journal of Supercomputing, 2014. **67**(3): p. 711-722.
23. Madani, M.A., M. Erradi, and Y. Benkaouz, *A Collaborative Task Role Based Access Control Model.* Journal of Information Assurance & Security, 2016. **11**(6).
24. Kaur, P.D. and I. Chana, *Cloud based intelligent system for delivering health care as a service.* Computer methods and programs in biomedicine, 2014. **113**(1): p. 346-359.
25. Modi, C., et al., *A survey on security issues and solutions at different layers of Cloud computing.* The Journal of Supercomputing, 2013. **63**(2): p. 561-592.
26. Grewal, R.K. and P.K. Pateriya, *A rule-based approach for effective resource provisioning in hybrid cloud environment*, in *New Paradigms in Internet Computing*. 2013, Springer. p. 41-57.
27. Varadharajan, V. and U. Tupakula, *Security as a service model for cloud environment.* IEEE Transactions on Network and Service Management, 2014. **11**(1): p. 60-75.
28. Lin, C.-Y., C.-H. Fu, and Y.-L. Yeh, *A Lightweight Fine-grained Sensitive Data Access Control Model in a Cloud Computing Environment.* 國防管理學報, 2016. **37**(1): p. 1-14.
29. Chang, V., Y.-H. Kuo, and M. Ramachandran, *Cloud computing adoption framework: A security framework for business clouds.* Future Generation Computer Systems, 2016. **57**: p. 24-41.

8. Acknowledgment

This research, supported by the Ministry of Higher Education Malaysia (MOHE) in collaboration with Research Management Center (RMC) at the Universiti Teknologi Malaysia (UTM) under Vot Number Q. J130000.2528.06H00.