A Trust and Reputation-based Access Control Model for Virtual Organizations

Majid Arasteh, Morteza Amini, and Rasool Jalili
Data and Network Security Lab (DNSL)
Department of Computer Engineering,
Sharif University of Technology
Tehran, Iran
{arasteh@cert., amini@, jalili@} sharif.edu

Abstract—**Virtual organization (VO) is aimed to provide inter-organizational collaborations. Constructing a VO necessitates provision of security and access control requirements which cannot be satisfied using the traditional access control models. This is basically due to special features of VOs; such as temporality, unknown users, and diverse resources. In this paper, after expressing our assumption on a framework for VOs; the concept of organizational trust and reputation is used to establish an access control model for VOs. Each member of an organization inherits its organizational reputation. Resource providers announce the behavior of their interacting users to their organization manager. According to the received feedbacks, organization managers calculate the new amount of trust for each guest organization. Afterwards, the VO manager calculates organizations reputation by integrating trust values received from organizations. A selfish organization may use the other organization resources and not offer any resources to the requester organizations. To overcome this problem, we use single policy and authorization system for all members of the VO. By combining resource providers' policies, a unique policy for each shared resource in the VO will be formed. In VOs there are various and heterogeneous entities, to address this challenge and preparing common perception we suggest using ontology in the virtual organization. The advantage and usefulness of the proposed method is compared with the conventional approaches.**

Keywords- Access Control; Virtual Organization (VO); Organizational Trust; Organizational Reputation.

I. INTRODUCTION

The term Virtual Organization (VO) at first was used by Mowshowitz in 1994. In the literature, there exist various synonyms for VO, such as Virtual Corporation, Virtual Enterprise, and Virtual Company. [1]. VO is rather a new concept that enables real organizations to federate their resources to achieve a common goal [2]. VO consists of diverse resources, geographically distributed, temporal, and dynamic organizations [3, 4]; due to which, providing security and access control are one of the main challenges in VOs.

Resource sharing and collaboration among parties are of the main goals of VOs. A VO consists of various resources such as processors, storages, data bases, softwares, and humans. An access control system in a VO is a security service which is used to prevent unauthorized access to such resources.

This paper proposes an access control model for a virtual organization, based on the concept of organizational reputation. The proposed model has three important features: 1) trust and reputation is used to add dynamicity to access control decisions; 2) a single and common access control policy is used in VO. Current access control models which are used in distributed systems are not suitable for VOs. We introduce selfish organization as an attack in the VO, and subsequently to address this challenge and for some other reasons such as scalability we use a common policy to access shared resources. A common access control policy for VO is yield by composition of real organizations policies. 3) An ontology has been developed and used to prepare common perception between organizations. According to the defined ontology, all members would have a common perception of entities (subjects, objects, actions, and policies).

In the remainder of this paper, the related work is reviewed in Section 2. In Section 3, a framework is introduced for virtual organization. Section 4, introduces an access control model for virtual organizations. In Section 5, the implementation of an access control system based on the proposed model is described and experimented results are presented. Section 6 concludes the paper.

II. RELATED WORK

Life cycle of virtual organization has four stages [1, 2, 5, 6]. At the *initial stage*, each organization creates a profile containing its objectives, subjects, available objects, and policies. At the *formation stage*, the VO manager selects suitable organizations (according to the available profiles), and sends a request to them for joining to the VO. The first level of access control is done in this stage (i.e. over joining the members). At the *operation stage*, shared resources are available for utilizing by members of the VO. The second and important level of access control is done in the operation stage (i.e. over resources). When a VO reaches its objectives, at the *dissolution stages*, the VO ends its activities.

Access control prevents unauthorized access to the resources and controls granting or denying of access requests. Classic and traditional access control models make decisions

978-1-4673-2386-4/12/$31.00 ©2012 IEEE

based to the users' identity and utilize their simplicity advantage. However, they are not suitable for dynamic environments with unknown users; such as VOs.

Condor and Legion are two common grid computing environments that enable us to create VOs [7, 8]. Resource management mechanism in Condor is similar to the UNIX style access control. Beside the read and write privileges, Condor uses more access control modes for making decisions. Legion is an object oriented middleware for Grid environments in which resources are considered as objects and accesses to them are done through functions defined on objects. In Legion, each object is responsible for enforcing its own access control policies.

OGSA is a framework developed by Global Grid Forum (GGF) [7, 9, 10]. Globus toolkit is the reference implementation of OGSA. Globus uses Gridmap for mapping users' identity in the VO to the local identity[11]. Each resource provider in the VO should maintain an ACL, which contains user's identities and their permissions. Any update in VO policies and users should apply in every resource providers Gridmap file, otherwise conflict would happen. To solve these problems authorization systems like CAS, VOMS, PERMIS, Shibboleth, and Akenti were introduced [9, 10, 12].

Push and pull are two basic models for authorization system in distributed systems, such as VOs [9, 11, 13,14]. With the push model, a user sends his request to the authorization system. After authorization, the system issues and returns message as a certificate to the user; then the user pushes the certificate to the resource provider. Some authorization systems like CAS and VOMS, support the push model [15]. In the pull model, a user sends his request directly to the resource providers; then the resource provider forwards the request to the authorization system. After authorization, the system issues and pulls the user's permission as a certificate to the resource provider. Some authorization systems such as Akenti [15] support the pull model. In both the push and pull models, resource providers make the final decision on allowing or denying the access requests of the users.

In VOs, some organizations may join only due to their sole benefit. They may use other organizations resources and does not allow others to utilize their resources through strict policies. We define selfish organizations threat as a great concern in the virtual organization, and propose another model especially for virtual organizations and grid computing which addresses selfish organizations concern.

III. Our Assumed framework of virtual organization

Three topologies for VOs have been appeared in the literature[14, 16]:

1. Supply-chain VO in manufacturing industries.
2. Star VO in construction industries.
3. Peer to Peer VO in creative and knowledge industries.

The peer to peer topology is the most common topology where all nodes have direct relationship with each other without any hierarchy. Our assumption on VO framework is based on the peer to peer topology.

Distributed systems which want to reach a common objective, mostly depend on a central node. Resource management, monitoring, scheduling, and preparing security are some duties of the central node. Our assumed framework is based on a central node too.

Due to the lack of unique and general accepted framework for VOs, our assumption on an appropriate framework for VOs is illustrated in “Fig. 1”, which consists of the following six features:

1. Each participating organization in VO has a manager (OM), responsible for managing the resources and enforcing the policies in the organization. Inter organizational communications and transactions are permitted by OMs.
2. The VO has a manager (VOM) which is responsible to manage all the resources and enforce the policies in the VO. Each OM may play the role of VOM. VOM determines the objectives and rules of the corresponding VO and announce them to OMs. The VOM sends an invitation to the suitable organizations. The OMs according to the received announcement decide whether to accept or reject the invitation.
3. Organizations have intra and inter-organization policies. Intra-organization policies are used against the local requesters. Inter-organization policies are used against the other organization requests and often are stricter than intra organization policies.
4. Each organization shares subset of its resources in the VO.
5. VOM describes ontology for the VO, and distributes it among organizations. The ontology helps participating organizations to reach a common perception about the VO entities.
6. OMs and the VOM are trusted entities, and do not involve malicious activities.

The scenario in the proposed framework is as follows. Initially, a user sends his request to the corresponding OM. If the user requirements cannot be satisfied by his local organization, the OM decides whether forward the request to VOM. If the OM prohibits the user to access his local resources, he will be prohibited from access to the VO resources as well.

The framework consists of nine stages.

1. A user sends his request to his corresponding OM.
2. According to the available resources and its own intra-organization policies, the OM decides to grant or deny the received request.
3. The OM sends response to the user. Based on the response, the user can/cannot use the resource.
4. If OM responses positively, but there is not enough available resources, the OM will forward the request to the VOM.

5. The VOM according to the available resources and its policies decides whether grant or deny the received request.
6. The VOM sends response to the user by mediation of the OM. If response is positive, user can use VO resources; otherwise he will be prohibited using resources.
7. When interactions between the user and the resource provider are done, the resource providers send feedback to their OM about the behavior of the user.
8. The OMs also send their opinions (feedback) about other organization based on their users behaviors in using the resources to the VOM.
9. The OMs combine the received feedbacks from their resource providers, and the VOM combine the OMs opinions, and uses them for making dynamic and precise decisions in future.

In fact step 9 should be done periodically, e.g. every three months.

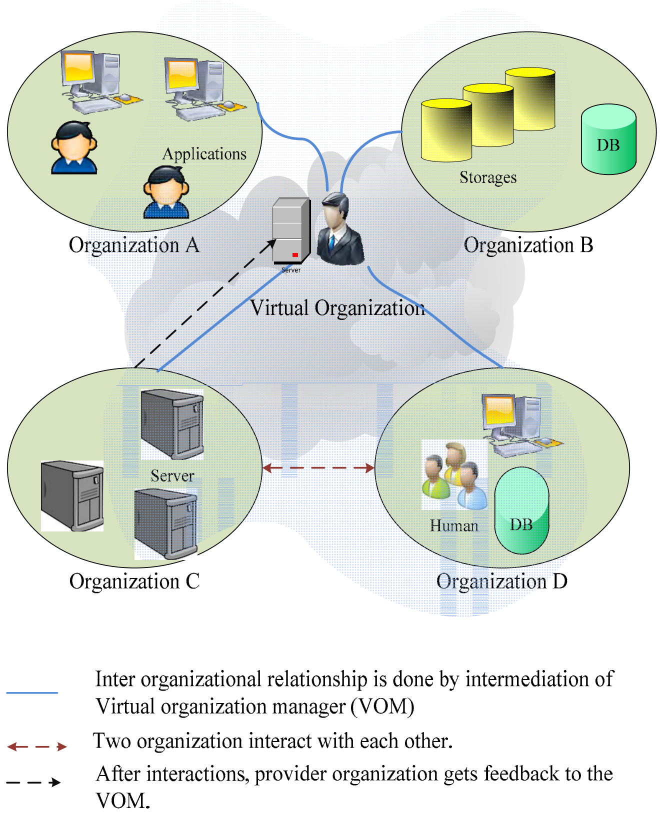

Applications
Organization A
Storages
DB
Organization B
Server
Virtual Organization
Server
Organization C
Human
DB
Organization D
Inter organizational relationship is done by intermediation of Virtual organization manager (VOM)
Two organization interact with each other.
After interactions, provider organization gets feedback to the VOM.

Figure 1. The proposed framework for virtual organization

A. *Ontology*

Virtual organization consists of many organizations, and each organization could have different kind of entities. Different perception among different organizations about common entities is one of the great challenges in VOs. To address this challenge, using the ontology of VOs is introduced.

By using ontology, we can provide a formal representation of a shared conceptualization of a particular domain. The VOM defines ontology and gets it to the OMs. Every organization should provide their entities according to the available ontology. Access control policy can be defined in the two levels of individuals and concepts.

IV. AN ACCESS CONTROL MODEL FOR VIRTUAL ORGANIZATIONS

Our proposed access control model for virtual organization includes three important parts. At the first part, according to the received feedbacks organizational trust and reputation will be evaluated by OMs and the VOM respectively. At the second part, a unique and common policy will be applied in the VO. By composition of inter organizational policies of the participating organization a unique and common policy for the VO will be yield. User's authorization in the VO will be based on the obtained policy. VO common policy consists of two sections. The first section is the minimum organizational reputation that needed to access resources. The second section relates to contexts and constraints. Finally, at the third part, ontology is used for preparation of common perception between all organizations. Unlike authorization systems, our proposed model does authorization only for one time. “Fig. 2” illustrates the general view of the model. In this picture C(O) and P(O) refer to the context and constraints policy.

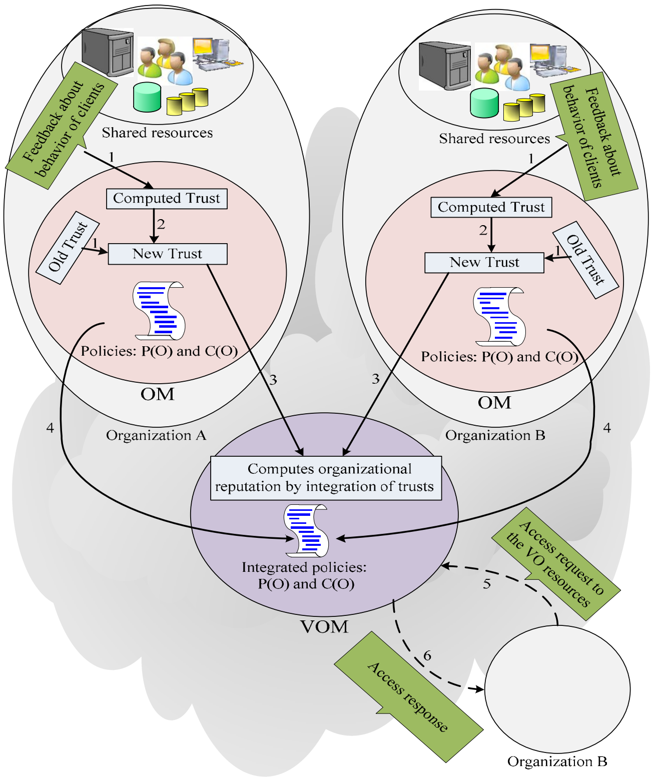


Figure 2. The proposed access control model for virtual organization

A. *Organizational Trust and Reputation*

To make dynamic and precise decisions, organizational trust and reputation are introduced. Trust is defined as the subjective probability that an entity X expects that another entity performs an assumed action on which its benefit depends [17]. Reputation is defined as people's believe about thing's character or standing [18]. Unlike trust, reputation is objective. Reputation value can be calculated through the combination of trust values.

When interaction between two organizations finished, resource providers would send their feedbacks about behavior of the users of the customer organization to their OMs. OMs according to the received feedbacks evaluate trust of the customer organizations. All OMs send their evaluated trust and opinions to the VOM. The VOM computes reputation of the organizations based on the received trust values.

1) Trust Computing

Every organization in the VO should compute its trust to other organization in using its resources. To compute the trust, we use the equation that was introduced by Josang [19]. This equation is based on the beta distribution and is useful for binary events. The beta family of probability density functions is a continuous and indexed by two parameters of α and β. The beta distribution f(p|α, β) can be expressed using the Gamma function Γ as:

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta}$$
$$Where\ 0 \le p \le 1\ , and\ \alpha > 0, \beta > 0$$

According to the beta distribution function the probability of the user trustworthiness in the next request is computed as follows:

$$P(T|P,N) = \frac{\Gamma(P + N + 2)}{\Gamma(P+1)\Gamma(N+1)} = \frac{P+1}{N+P+2} \qquad (1)$$

In "(1)", T denotes the trustworthiness of the user in the next request, P refers to the number of positive observations (here, correct usage of resources), and N denotes the negative observations (here, incorrect or inappropriate usage of resources).

At start of a VO formation, trust of each OM to other ones is set to a default value. Every OM periodically updates its trust values. According to "(2)", the new trust value is the result of the combination of the newly computed trust value and the old trust value. In "(2)", Trust is computed by the "(1)" for the current period of time.

$$Trust_{new} = \alpha Trust_{Old} + (1-\alpha)Trust_{Computed}$$
$$, Where\ \ 0 \le \alpha \le 1 \qquad (2)$$

α is a coefficient that enables OMs to decides how compose old and computed trusts. For example if α is set to 0.5; then new trust is the mixture of old and computed trust with the same effect. We call α as attenuation coefficient.

2) Reputation Computing

Every resource provider organization after giving access to customer organizations (to do their transactions) recalculates its trust to the customer organizations. Every OM sends its trust information to the VOM. The VOM calculates the reputation of each organization based on the trust values of other organization to it. At the beginning of a VO formation, its VOM sets the reputation of each organization to a default value. The VOM stores organizations' reputations in its database, and update them periodically. According to the received trust values and organizations' prior reputation, the VOM updates the reputations as mentioned in "(3)".

$$R'_x = \frac{\sum_{y \neq x} R_y \times T_{y2x}}{\sum_{y \neq x} R_y} \qquad (3)$$

In the (3), R'_x Denotes the new and updated reputation of organization *x*. T_{y2x} indicates trust of organization y to organization *x*. R_y refers to the prior amount of reputation, which the organization y has. According to this equation, organizations with higher reputations have more effect in computing the other ones' reputations.

B. Inter organization policies

Security policy of each organization consists of two elements; minimum needed reputation (MNR), and context, and constraints. Contexts and constraints express in which situations and when users can use resources. MNR says how much reputation at least a user should have to get an access. The formal definition of organization *i's* policy is as follows.

$P_i = \langle MNR_i, P_i, C_i \rangle$

a. MNR$_i$; is a function which assign to each shared resource *O,* the minimum needed reputation; denoted by MNR$_i$(O).
b. P$_i$ is a function that defines constraints on resources.
c. C$_i$ is a function defined on resources to specify the contextual conditions in which a requester can access objects. C$_i$(O) denotes contextual constraints defined on object O.

C. Combined VO Policy

We want to use a single and common access control policy for VOs. Elimination of a selfish organization is one of the main goals of the single and common access control policy. Single and common policy is computed by composition of the inter organization policies. Selfish organizations are some kind of organizations which are joining to the VO only because of themselves benefit. Selfish organizations use other organizations resources, but by expressing strict policies don't allow other organizations to use their resources. Beside advantage of the common policy, it has a shortcoming too. In this case organizations don't have complete control on their shared resources.

Three common approaches to yield a common and unique policy are as follows:

- The VOM sets a policy and announce organizations. Organizations before joining the VO read the policy and then decide whether join the VO or not. In this way conflict will not happen in the VO policy, but organizations' policies are ignored.
- The VO policy is obtained by the union of the joining organizations' policies. This is the simplest way to combine policies. In this manner conflict would happen among organizations policy.
- The VO policy is obtained by intersection of the joining organizations' policies. In this way conflict does not happen among the combined policies, but it is so strict. If there is no intersection between organizations' policies, then the VO cannot have any applicable policy.

All aforementioned approaches have their advantages and disadvantages. In our proposed approach, we use the combination of the three aforementioned approaches to eliminate their disadvantages and leverage their advantages.

1) Combination of Context and Constrains Policies

We assume that the VOM defines its default policy and at the beginning of the VO announce organizations. Organizations by awareness of the default policy decide whether join the VO or not. To affect organizations common policy about their shared resources, intersection has been done on their policies. To yield single and common policy for each shared resource in the VO, union is done on the VO default policy and the organizations common policies. "Equation (4)" shows the integration of policies to yield the VO's common policy.

$$P_{VO}(O) = P_{VO-Default-manger}(O) \cup \{P_{Org1}(O) \cap \dots \cap P_{Orgn}(O)\} \qquad (4)$$

By "(4)", both of the VO default policy and organizations policies affect in obtaining the VO's common policy. $P_{VO}(O)$ refers to the common and single policy of the VO for object O. $P_{VO\text{-}Default\text{-}manager}(O)$ denotes the VO default policy on object O. $P_{Org}(O)$ indicate the organizations policies on object O.

In the proposed approach for composing organizations' policies, conflict might happen between the VO's default policy and organizations common policy. In this case, conflict resolution should be applied. Using priority between organizations common policy and the VO default policy is the simplest way for conflict resolution.

2) Combination of minimum needed organizational reputation policies

Minimum needed reputation (MNR) in the policies helps the organizations to dynamically make decision. For shared resources in the VO, MNR can be set by the two ways. First, for each shared resource, the VOM itself defines MNR. Second, MNRs of shared resources are computed by integration of the providers MNR, which were defined in their policy.

We want to define MNR for each shared resources in the VO. MNRs of shared resources are computed by the VOM. We suggest using weighted average between organizations opinions to computes resource MNR in the VO. "Equation (5)", shows suggested formula for calculating MNRs.

$$Min_{Reputaion}(O) = \frac{\sum_{i=1}^{k} \mathrm{R}_i \times P_i(O)}{\sum_{i=1}^{k} \mathrm{R}_i} \qquad (5)$$

In "(5)", O refers to the resource which organization i to k shared it. Sharer in their policies for each shared resource set the MNR (*Pi(O)*). R_i denotes to the reputation of sharer organizations.

For example, if a user from organization *A* wants to access resources in the organization *B*, he should send his request to his OM. If the OM doesn't have enough resources and user is a trustee in the organization; then the OM do as follow:

1. Assign a suitable concept to the user.
2. Forwards user's request and concept to the VOM.
3. The VOM according to the received concept and request decides whether grant or deny the received request.

In the VO users identity will be hidden from the VOM and their request will be responded according to the: organization which they belongs to, and their concept.

V. IMPLEMENTATION AND EVALUATION

The case study which is considered in this research is a digital library containing e-books. It consists of four real libraries and 20000 users. The concepts of leveraged ontology are introduced in Table 1.

TABLE I. CONCEPTS OF INTRODUCED ONTOLOGY

Subjects	16 roles (level 0, don't get any permission, and level 15 gets all permissions	
Objects	Wiki, Thesis, Scientific books, Story books	
Actions	Read, Add, Edit, Delete	
Other parameters	Context	Libraries name
	MNR	4 levels: worst, bad, good, best

We implement our proposed access control model and an existence authorization system, and evaluate them.

A. Implementation

We implement proposed access control model and an authorization system by java and MySQL, and evaluate them according to the average response time and the best response time. It was examined by the 100 up to 1100 users that simultaneously send their request to the authorization system. Our results summarized as figures 4 and 5. Each experiment was done for twenty times and their averages reflected.

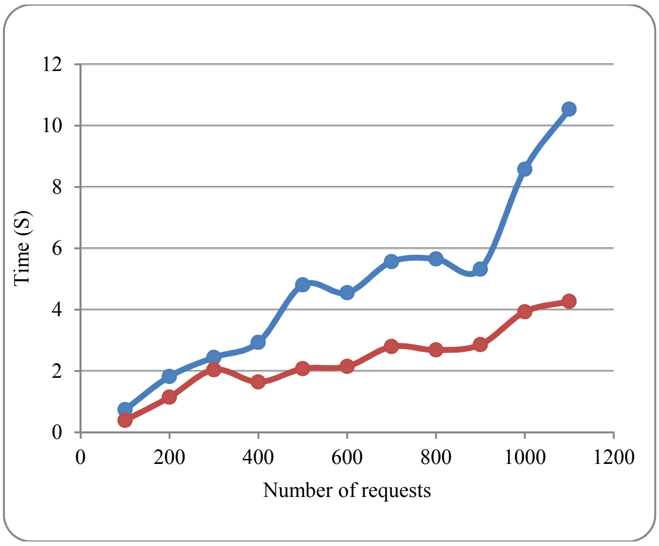


Figure 3. The Average response time

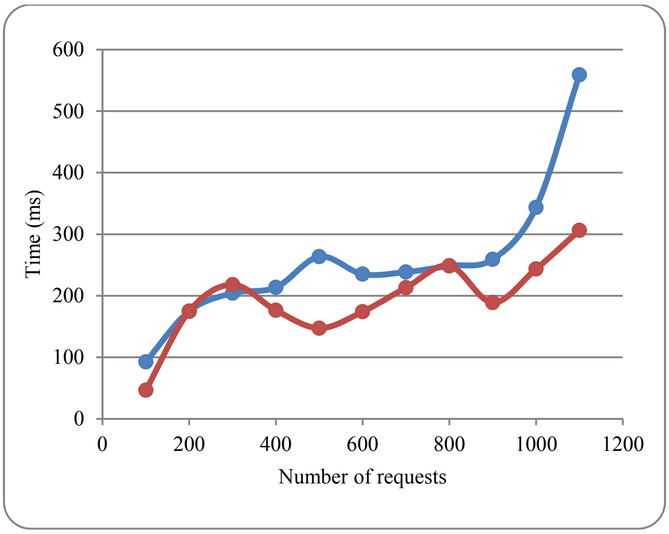
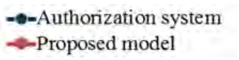


Figure 4. Best response time



B. Evaluation

The characteristics of our proposed model in comparison with some related authorization model are shown in Table 2. To complete table 2 we got help from [15, 20].

TABLE II. COMPARISON BETWEEN THE DIFFERENT AUTHORIZATION SYSTEMS

	CAS	**VOMS**	**Akenti**	**PERMIS**	**Gridmap**	**Proposed model**
Pull/push	Push	Push	Pull	both	Pull	Push
User scalability	✓	✓	✓	✓	✓	✓
heterogeneity	-	-	-	-	-	+
Access control model	RBAC	RBAC	RBAC / DAC	RBAC	DAC	Semantic
Authorization	Centralize	Centralize	Centralize	Centralize	Directly at the resources	Centralize
Administrative overhead	Low	Low	Low	Low	High	Very low
Dynamic decision	-	-	-	-	-	+
Selfish organization	+	+	+	+	+	-
Full control on shared resources	+	+	+	+	+	-

VI. CONCLUSION

Virtual organization (VO) consists of some real organizations that for aiming common goals and sharing their resources connect to each other. Security and access control are important issues in VOs. In the lack of general framework for VOs, at first a framework was assumed; then an access control model for VOs is proposed in this paper. Our proposed model has three important features. First, we use feedback to compute organizational trust and reputation. Making dynamic decisions according to the users behaviors is the main advantage of feedbacks. Second, we use common and single access control policy for shared resources in the VO. For attaining common policy, combination of inter organization policies is used. Decisions are made according to the minimum needed reputation (MNR), and contextual constraints. Third, for preparation of common perception between all organizations, ontology was used.

We introduced selfish organization attack in VOs. A selfish organization uses other organizations resources and by expressing strict policies does not offer resource to other organizations. To address this challenge we proposed using unique and common policies for each shared resource. To obtain a common policy we combined provider organizations policies.

REFERENCES

[1] K. Jacobsen, "A Study of Virtual Organizations,", Project Report, Norwegian University of Science and Technology, Department of Computer and Information Science, NTNU, 2004.

[2] M. Ibrohimovna and S. Groot, "A Framework for Access Control and Management in Dynamic Cooperative and Federated Environments," in 2009 Fifth Advanced International Conference on Telecommunications, 2009, pp. 459-466.

[3] T. Ryutov, et al., "Establishing Agreements in Dynamic Virtual Organizations," 2005, pp. 90-99.

[4] B. Nasser, et al., "Dynamic Creation of Inter-Organizational Grid Virtual Organizations," in Proceedings of the First International Conference on e-Science and Grid Computing (e-Science'05), 2005

[5] L. Huraj and H. Reiser, "VO Intersection Trust in Ad hoc Grid Environment," in 2009 Fifth International Conference on Networking and Services, 2009, pp. 456-461.

[6] S. Crompton, et al., "The TrustCoM General Virtual Organization Agreement Component," 2007.

[7] J. Luo, et al., "A Trust Degree Based Access Control in Grid Environments," Information Sciences, vol. 179, pp. 2618-2628, 2009.

[8] J. Luo, et al., "A Semantic Access Control Model for Grid Services," 2005, pp. 350-355 Vol. 1.

[9] A. L. Pereira, "Role-Based Access Control for the Open Grid Services Architecture-Data Access and Integration (OGSA-DAI)," Wright State University, 2007.

[10] A. Grimshaw, et al., "The Open Grid Services Architecture, Version 1.5," 2005.

[11] L. Pearlman, et al., "The Community Authorization Service: Status and future," Arxiv preprint cs/0306082, 2003.

[12] L. J. Winton, "A Simple Virtual Organisation Model and Practical Implementation," 2005, pp. 57-65.

[13] W. Zhou and C. Meinel, "Implement |Role based Access Control with Attribute Certificates," In Proceedings of the 6th International Conference on Advanced Communication Technology (ICACT2004),, Korea, 2004.

[14] A. Benzekri, "Virtual Organization Security Policy: Specification & Deployment (V1)," VIVACE, 2006.

[15] M. L. C. Hui, et al., "A Context-Aware Based Authorization System for Pervasive Grid Computing," Virtual Organizations, 2011.

[16] B. Katzy, et al., "Reference Models for Virtual Organisations," Virtual Organizations, pp. 45-58, 2005.

[17] D. Gambetta, "Trust: Making and Breaking Cooperative Relations," 1990.

[18] A. Josang, et al., "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, pp. 618-644, 2007.

[19] A. Jsang and R. Ismail, "The Beta Reputation System," in 15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy, Bled, Slovenia, 2002, pp. 41-55.

[20] A. Chakrabarti, Grid Computing Security: Springer Verlag, 2007.