Journal of Network and Innovative Computing
ISSN 2160-2174 Volume 4 (2016) pp. 106-115
© MIR Labs, www.mirlabs.net/jnic/index.html

Tr-OrBAC: Towards a Trust Framework for Collaborative Systems in Critical Information Infrastructures

Nawal AIT AALI, Amine BAINA, Loubna ECHABBI

STRS Lab., National Institute of Posts and Telecommunications
2, av. Allal El Fassi, Madinat Al Irfane, Rabat, Morocco
{aitaali, baina, echabbi}@inpt.ac.ma

***Abstract*: A collaborative system involves several organizations collaborating in order to ensure the continuity of their Critical Infrastructures. However, some malicious behaviors may occur, causing disturbances in the information systems. This may be fatal when it comes to Critical Information Infrastructures. In order to avoid such behaviors, building trust between collaborating organizations is necessary, especially, between their entities. Indeed, trust allows cooperating and sharing resources in a secure way. In this paper, we present our approach named Tr-OrBAC: An Organization Based Access Control that relies on trust between organizations, especially for Critical Information Infrastructures. Our aim is to allow each organization to take collaboration decisions by evaluating trust of participating entities using Fuzzy Logic. In order to illustrate the efficiency of Tr-OrBAC, we use the Electrical Grid as a case study.**

Keywords: Access Control, OrBAC, Trust Management, Collaborative System, Critical Information Infrastructure, Electrical Grid, Fuzzy Logic**.**

I. Introduction

Protection and security of Information Systems are nowadays so crucial. The organization that has a completely new role as CISO (Chief Information Security Officer)[1] is becoming a standard. This is even more crucial when it comes to Critical Infrastructures (CI)[2] , and their Critical Information Infrastructure (CII). These CII usually involve several organizations that collaborate in order to accomplish their mission [3]. This collaboration gives rise to a Collaborative System [4]. However, some malicious behaviors, such as providing incomplete information, may occur [5] and thus harm the information systems of organizations participating in the collaboration.

The most used method to secure collaboration between different entities is controlling access to resources using collaborative access control model such as O2O[6], PolyOrBAC[3], Multi-OrBAC[7], Virtual Organization[8] … However, these models do not treat the trust[9] as an important indicator while taking collaboration decisions. This may be relevant especially when collaboration occurs between unknown organizations.

As a consequence, leaning only on service access control[10] is not sufficient to protect a collaborative system. Indeed, access control is applied after the creation of the system, without taking the reliability into consideration. The solution is to evaluate the trust before establishing collaborative system; seek the identity of the organization, its reputation [11], its activities, its operational history [12], and the satisfaction [13] of other collaborating organizations. Hence, we propose a trust model for collaborative systems that integrates trust into the well-known OrBAC [14] access control model. Usually, OrBAC enables the access control within a single organization. Our contribution lies on using OrBAC for collaborative systems by adding a trust parameter in the generated security rules[15]. Evaluating trust of participating entities is possible using Fuzzy Logic [16]. We use the Electrical Grid [17]as an example of a critical infrastructure in order to illustrate our approach.

The remainder of this paper is presented as follows: in section 2, we present the different requirements that must be taken into consideration when it comes to collaborative systems. In section 3, we present the related works. In section 4, we introduce our approach Tr-OrBAC; we present its global architecture, its modelization using UML and the use of the fuzzy logic to calculate the trust score. Section 5 is reserved to discuss the electrical grid as a case study to illustrate our approach. After discussions in section 6, we conclude the paper and we present some perspectives in section 7.

II. Collaborative Systems Requirements

Since their appearance, the Critical Infrastructures attract a careful attention from governments, research laboratories, projects, programs... seen the important role of such infrastructures in the development and the continuity of the country. Generally, each country defines its critical infrastructure according to its needs and its requirements. A clear definition was proposed and granted by industrial countries: 'Critical Infrastructures are generally defined by a set of organizations, facilities, equipment and services, essential for the good functioning of the socio-economic activities of a nation and any malfunction leads to serious results which threaten the development of the nation' [2].

In the recent decades, the critical infrastructures integrated the new information technologies. This generated a new type of infrastructure named: Critical Information Infrastructures

(CII); they generally present the information systems of CI. These CII are characterized by the collaboration between different organizations and information systems in order to perform and achieve some missions and operations. This helps to ensure the continuity and the success of CII. This collaboration is achieved by sharing resources and data as well as user access to resources to complete tasks.

To protect the CIIs, their collaborative systems must be secured. In this sense, a study of the characteristics and requirements of collaborative systems is crucial to choose the best methods to secure them. Among the requirements that must be considered for securing the collaborative systems, we cite:

- **Collaboration** [18]: The different organizations within the collaborative system must work together to perform the necessary tasks to ensure the continuity of CIIs.
- **Autonomy**[19]: Each organization has its own activities, resources, users, data. During the collaboration, it must ensure that no changes have been applied to its entities, and each organization must be autonomous in managing its resources.
- **Interdependence** [20]: Generally, the collaborating organizations are interdependent: each one of them depends on the others. This interdependence is necessary to achieve a successful collaboration, but ensuring that a failure of an organization does not influence the other.
- **Access control**: The objective of the collaboration between organizations is to share the resources/services and to allow the users to access to data in another organization. Thus, in order to secure these services, each organization applies an access control on services.
- **Trust Management**: The collaboration should be carried out even if the organizations are unknown to each other. Each organization establishes the trust towards other organizations before starting to share the resources.
- **Flexibility**: The main goal of collaborating organization is the achievement of tasks and the success of CII. For that, the Organizations should be flexible while putting its condition, negotiating the objective of the collaboration, the activities to be performed and the regulations to be respected during the collaboration.
- **The scalability** [21]: The organizations may expand geographically and their resources are situated in different locations. This extension should not affect the availability of the shared resources between organizations in the collaborative system.
- **Decision making**: The collaboration is indispensable within the CII. But, the security of data and resources is in the first priority. Therefore, every organization must take the collaboration decision according to the computed trust score and the shared resources.

To satisfy the requirements cited above, a set of approaches was proposed. Based on our research, the access control and the trust management are the most suitable models to secure the collaborative systems. In the next section, we present the existing access control models and the trust systems.

III. Related works

In order to ensure a good functioning of its information system and to secure the different interactions with other organizations, each organization is based on two main security models: Access Control and Trust Management.

The access control is one of the most important strategies to ensure the information systems security. It is based on the principle that each organization administrator manages the access authorization attributed to the users in order to access to the resources. The goal is to verify and to ensure that the resources will not be accessible and used illegally. Two types of access control models are proposed: Traditional and Collaborative:

A. *Traditional Access Control Models [22]*

Four families of traditional models have been proposed: DAC [23], MAC [24], RBAC [10] and OrBAC [14].

1) DAC: Discretionary Access Control

It allows users to use their identities in order to access to the desired resources and some users may provide, discretionary, their own access permissions to other users. However, it is difficult to apply this model when the number of users increases.

2) MAC: Mandatory Access Control

The principle is that each user and file has some classes of security and the users do not have the right to change these classes. Only the system administrator can confirm to the user the access permission. The implementation of MAC becomes complicated when the number of users and files increases.

3) RBAC: Role Based Access Control

The principle of RBAC is to group users having the same functions in a single role and the security rules will be applied on the role and not on the user. Thus, RBAC is applied in the large companies having an important number of the users.

Generally, the users do not exercise the same activities and do not access to the same resources. Therefore, other security rules must be applied and other entities should be present in these rules. In this sense, OrBAC model was proposed.

4) OrBAC: Organization Based Access Control

OrBAC model solves the RBAC problem by creating abstract entities (Role, View, Activity) [14] separated to concrete entities (Subject, Object, Action) [14]. The aim of this separation is to apply the security rules on abstract entities, and to each entity of this type, a concrete entity is associated. Besides, OrBAC defines some relationships linking abstract entities with concretes ones:

- Employ relationship

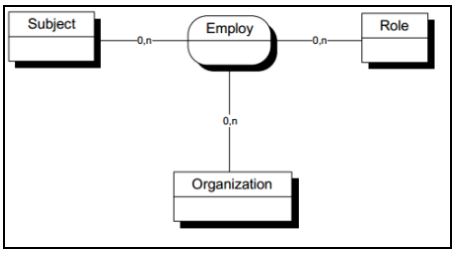


Figure 1. Employ Relationship [14]

A subject can play a role in organization. This role links subject with organization by the relation: Employ (org, s, r) taking 'org' is organization, 'r' is role and 's' is subject. In this case, 'Employ' relationship means that organization 'org' employs subject 's' in role 'r' as presented in the figure 1.

- Use relationship

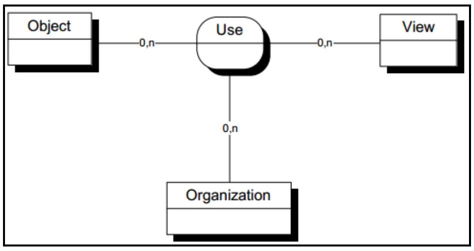


Figure 2. Use Relationship [14]

A view is a set of objects, the 'Use' relationship groups view, organization and objects. The figure 2 describes the Use (org, o, v) which means that 'org' uses object 'o' in view 'v'.

- Consider relationship

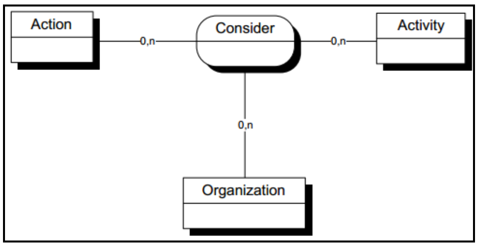


Figure 3. Consider Relationship [14]

An activity is a group of actions, the 'Consider' relationship (figure 3) groups organization, activity and action. Consider (org, α, a) means that 'org' considers that action 'α' falls within the activity 'a'.

A fourth abstract entity in the OrBAC model is Context which defines the situation in which the security policy will be validated, for example Normal, Emergency, Critical...

OrBAC defines four types of security rules: Permission, Obligation, Prohibition and Recommendation. Let's take an example for permission rule, it has the form: Permission (org, r, v, a, c) which indicates that in organization 'org', the role 'r' can perform the activity 'a' on view 'v' in context 'c'.As mentioned before, OrBAC presents two types of entities: abstracts and concretes. Each type has its security rules.

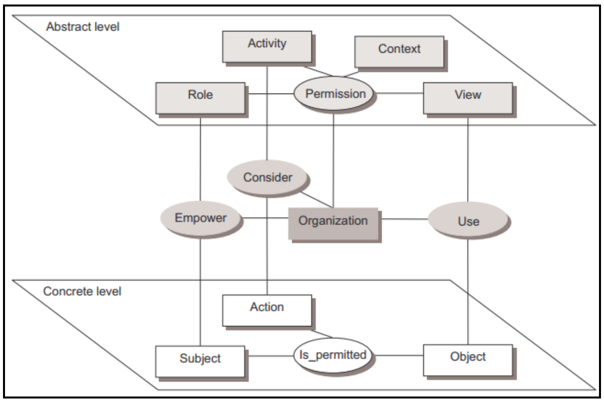


Figure 4. OrBAC model [14]

In abstract entities: The administrator defines security rules through abstract entities (roles, activities, views) without worrying about how each organization implements these entities.

In concrete entities: The response of a user access request depends on rule, belonging organization, played role, instantiated view and activity. In this sense, concrete security rules are expressed through the rules: Is_permited, Is_prohibited, Is_Recommended and Is_Obliged containing subjects, objects and actions.

To summary the principle of OrBAC model, figure 4 presents its different components and relationships.

The major drawback of traditional models, mentioned above, is that they cannot be applied in a collaborative environment. Then, the solution is to use the collaborative access control models.

B. Collaborative Access Control Models [18]

The collaborative access control models permit the management of the security policies in multi-organizational environments [25] and the collaborative systems. These models allow the organizations to share the resources by controlling the access to each resource.

We talk about two types of Access Control: Centralized and Decentralized:

1) Centralized Access Control[26]

It is based on the existence of the authority which gathers all the security rules of the organizations and unifies them in a single system. Also, the presented authority manages the access to each resource of each organization. This raises some problems about the privacy and the autonomy of the organizations.

2) Decentralized Access Control[27]

This type of access permits to each organization to manage its security rules without going through an authority. This avoids the privacy problems.

In literature, Different decentralized access control models were proposed. They allow the collaboration between the participating organizations while keeping the control on each access to resource. Multi-OrBAC, O2O, Poly-OrBAC, and Virtual Organization present the most popular and used collaborative access control models. They are based on the OrBAC model.

These models provide great advantages to satisfy the need of the collaboration between organizations. However, some problems were not treated in these models and especially the trust. Also, the applied security rules in these models present some problems regarding the organizations autonomy and privacy. Finally, these models require the integration of new technologies concepts. This needs more resources and processing space and storage.

After presenting an overview about the access control, we reserve the next section to present the existing works on the trust management.

C. *Trust Management*

The trust concept [9] is an important tool in human life; it facilitates the interactions and the transactions between the unknown entities that can produce malicious activities during the achievement of transactions.

The Trust systems are classified into two categories [28]:

- **Policy-based trust systems:** These systems use security policies to determine whether an entity is authorized to access.
- **Reputation-based trust systems:** These systems use the interactions, the experiences of the entities in order to evaluate the trust and to make the trust to another entity.

These systems (The reputation-based trust systems) can be classified into two categories:

- **Centralized systems**

The existence of a central unit is required to be interviewed by each entity wishing to know the reputation score of another entity.

- **Decentralized systems**

This type of system does not need a central entity. Each entity registers itself the various interactions and experiences with other entities to be reuse in other transactions.

To establish a trust system, a set of entities is essential: S. and L. Kutvonen Ruohomaa[9] established a study to identify the necessary elements to manage the trust between two entities, we are talking about:

- **Trustor**: presents the service provider.
- **Trustee**: is the service requester; it requires the access to the trustor services.
- **Action**: it involves the use of services, provided by the trustor.
- **Trust decision**: It is based on a balance between the risk and the trust. This decision has an effect on the trustee.

In order to manage the trust between different entities, a set of techniques is essential; we talk about the certificate management between different actors and the calculating of a set of parameters as: reputation, recommendation, Satisfaction…

The establishment of the trust requires the intervention of other actors to approve the reliability of the entities. Trust management in a collaborative system is essential, based on the calculation of several parameters. In the literature, several trust evaluation parameters between entities were discussed. We talk about reputation [11], recommendation[29], satisfaction[13], number of interactions[11], and popularity[12]; updated after collaboration[11], size history... All these parameters depend on history; the history of each entity influences its reliability in future collaborations with other entities. Consequently, we are interested to discover the history of each entity and in particular, the past activities of its elements: users and resources.

Combining the trust management with the access control is among the issues treated by researchers. Trust-OrBAC [25], TrustBAC [30], TOrBAC [31], and Multi-Trust_OrBAC [32] describe the integration of the trust in the generated security rules of access control.

TOrBAC model adds a confidence index[31] to security rules in OrBAC model. The principle is: a user connects to a TTP (Third Trust Party)[33] which permits him/her to create a session after authentication and to obtain a confidence index at the beginning of the session in order to use it in each access request. This model is applicable within a single organization, that’s why, the same authors propose Multi-Trust_OrBAC.

Multi-Trust_OrBAC permits to use the same principle as TOrBAC in the collaborative system. The two models [31] and [32] do not enable the detection of the users having malicious activities only after their connections and the access to the various data. This presents a great limit of these models and the serious consequences can result.

Trust-OrBAC model requires the establishment of a prior trust by integrating the concept of the situation that depends on the desired object and the activity to be performed by the user. This model is based also on OrBAC model.

Table I. Comparative study between models

Support elements	***TOrBAC***	***Multi-Trust_ OrBAC***	***Trust-OrBAC***	***TrustBAC***	***Trust-PolyOrBAC***
OrBAC	+	+	+	-	+
Collaboration	-	+	+	+	+
Authentication	*	*	*	*	+
Trust Management	+	+	+	+	+
Session	+	+	-	+	-
User evaluation	+	+	+	+	+
Resource evaluation	-	-	-	-	+
assignment of roles	-	-	+	+	-
Extensibility	-	+	+	-	+
Autonomy	-	-	+	+	+
Periodicity	-	-	+	+	+
Prior Detection of malicious activities	-	-	+	+	+
Organization evaluation	-	-	+	+	+
Time influence in the calculation of the trust	+	+	+	+	+

TrustBAC is based on the same principle of Trust-OrBAC expect that this model (TrustBAC) presents an extension of RBAC[10] model. We note that Trust-OrBAC, Multi-Trust_OrBAC and TOrBAC are based on the OrBAC model while TrustBAC is based on the RBAC model.

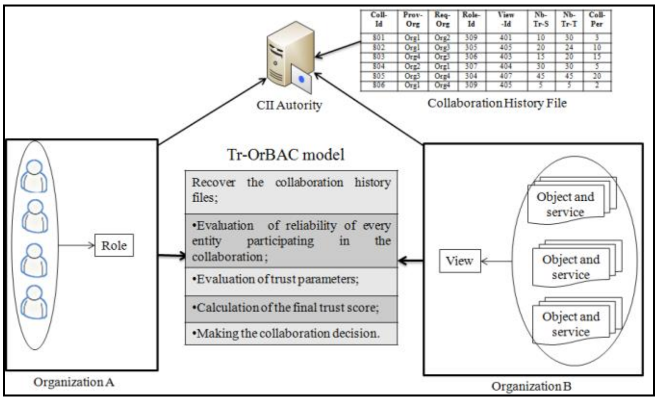
In addition to these models, we presented, in our preview work, our approach: Trust-PolyOrBAC [34]. It is based on the integration of new layer of the trust between the authentication step and the access control step.

In order to summary the cited models, we present their advantages and limits according to the collaborative systems requirements. We present in the table 1, the different discussed models. We base as criteria, several collaborative systems requirements. After studying and comparing these models, we conclude that we cannot apply them in our context. In the next section, we will present out approach Tr-OrBAC: A trust model applicable in the collaborative system.

IV. Tr-OrBAC: Securing the collaborative Systems

A. *Tr-OrBAC Architecture*

In Critical Information Infrastructures, the organizations wish to collaborate in order to perform important tasks for the continuity of these infrastructures. Each organization allows the users (Engineer, technician, trainers…) of other organizations to access to its available resources and to obtain several services. In this sense, we apply an access control model to control all types of access to different resources.



Coll-Id	Prov-Org	Req-Org	Role-Id	View-Id	Nb-Tr-S	Nb-Tr-T	Coll-Per
801	Org1	Org2	309	401	10	30	3
802	Org1	Org3	305	405	20	24	10
803	Org4	Org3	306	403	15	20	15
804	Org2	Org1	307	404	30	30	5
805	Org3	Org4	304	407	45	45	20
806	Org1	Org4	309	405	5	5	2

CII Autority
Collaboration History File
Tr-OrBAC model
Recover the collaboration history files;
•Evaluation of reliability of every entity participating in the collaboration;
•Evaluation of trust parameters;
•Calculation of the final trust score;
•Making the collaboration decision.
Role
View
Object and service
Object and service
Object and service
Organization A
Organization B

Figure 5. Global architecture of Tr-OrBAC

Normally, in a single organization, the administrator knows all the users in this organization and applies the OrBAC model to generate the security rules; the administrator defines the role having the right to access to a view in order to perform an activity in a specific context. However, in a collaborative system, the administrator of an organization does not necessarily know the users of all collaborating organizations. Thus, the trust management is essential in this type of systems.

Our strategy in Tr-OrBAC model is securing the different entities contributing in the collaborative systems. In one hand, our aim is to secure the resources against any malicious activities, generated by a user. And in the other hand, our goal is to secure the user by preventing any access to malicious resources.

In order to establish Tr-OrBAC model as presented in the figure 5, we assume that:

- Every organization is responsible to assign each user to the appropriate role, to group objects with the same characteristics in view and the actions in the activity, by applying OrBAC principle. After, our model is applied on abstract entities: the role, view and activity;
- The Organizations are authenticated and certified by the authority (CAA) of the CII;
- Each organization sends to CAA its logs to be record after each collaboration;
- Each organization is autonomous to take its collaboration decision after evaluating the reliability of the entities of other organizations participating in the collaboration.
- The CAA provides to each organization the necessary history files of another organizations and the trust threshold in order to calculate the trust parameters and then to calculate the final trust score.

In order to detail Tr-OrBAC approach, the next section presents its components:

B. *Modelization of Tr-OrBAC*

In this section, we define a proposition to model our approach. Figure 6 shows our trust model classes that we explain in next paragraphs.

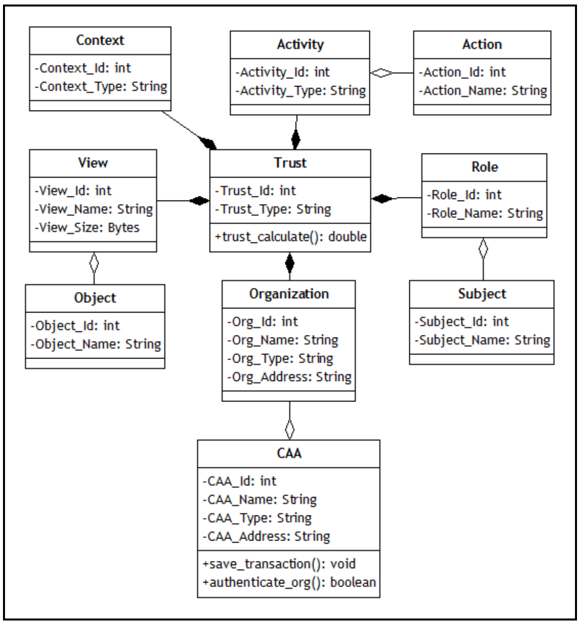


Figure 6. Modelization of Tr-OrBAC in UML

Tr-OrBAC is based on the OrBACentities which are five components: organization, view, role, activity and context. We model them by classes in UML. We add otheressential classes to our approach.

CAA class is dedicated to record all types of transactions between collaborating organizations. It is also used to authenticate and certify each new organization in the CI.

Trust class is the main class of our model; different security rules are defined and applied in this class and in which we evaluate the trust of different actors (role and view).

To evaluate the trust in our approach, a set of parameters are calculated. Then, we apply the Fuzzy Logic in order to calculate the total trust score and then to take the collaboration decision.

C. *Trust parameters evaluation*

In our approach, after collaboration, the organization sends the collaboration logs to the authority of CII in order to save different logs and use them in the future collaborations. These logs are considered as the history of the organizations. We therefore conclude that the history presents the most important parameter for evaluating the trust between organizations. From the history, we calculate other parameters which are necessary to establish our trust model. We extract three trust parameters deemed relevant for evaluating the trust in the collaborative systems within Critical Information Infrastructure. These parameters are: satisfaction, reputation and recommendation.

We note first that organizations in our collaborative system are certified and authenticated by the infrastructure authority. We assume that the organizations are reliable. However, they may contain malicious resources or some users that generate malicious activities. Thus, we will not consider all the organization malicious. It is in this context that we must evaluate the trust of each user and resource. The trust parameters on which we base to calculate the trust of users and resources are the same.

We note that our objective is to integrate the trust concept in OrBAC model. Therefore, each organization administrator is responsible for assigning concrete entities to abstract entities. Then, the trust parameters are applied on abstract entities (role and view). After calculating the trust score, a trust variable will be added in the abstract rules of OrBAC.

In the following, we present the used trust parameters. We base on the satisfaction, reputation and recommendation as trust parameters.

Satisfaction is contentment to an entity after a series of transactions. Satisfaction is calculated after the collaboration. It depends on the satisfaction of other organizations that have completed collaborations with the concerned organization. We distinguish between the satisfaction towards a role and the satisfaction towards a view. But, the competition still exists between organizations into a single system. These organizations can give incomplete satisfactions to save them in the CAA as a history and to be used by other organizations. Therefore, we are interested to satisfaction of organizations deemed reputable in the critical infrastructure.

Reputation is the impression that an entity created through past actions on its intentions and norms[21]. We say that an organization has a good reputation if it has been recommended several times for collaboration with other organizations.

Recommendation: An organization is referred recommended if it respects the terms of contracts signed with other organizations for successful collaboration.

We track the same strategy used by Trust-OrBAC and TrustBAC to evaluate our trust parameters[35].

1) *Satisfaction*

The resource provider is based on the equation (1) to calculate the satisfaction of other organizations after their collaboration with the service requester (the role).

(1)

- v is the desired view;
- r is the role who want to access to the view;
- org_i present the organizations whose views were accessed by the role;
- org_A contains the role;
- n is number of collaborations between organizations;
- S presents the calculated satisfaction from the collaboration whereas org_i is the provider organization and org_A is the requester organization.

2) *Reputation*

The calculated reputation is that of organizations providing their satisfaction toward the requester. Equation (2) presents the formula used to calculate the reputation:

$$\mathrm{Re}\,p(org_A) = \frac{\sum_{i=1}^{n} \mathrm{Re}\,c(org_i, org_A)}{n} \quad (2)$$

- org_A : we seek the reputation of the organization A;
- n: number of the organizations collaborating with org_A .
- $\mathrm{Re}\,c(org_i, org_A)$: The recommendation of org_i towards the org_A .

An organization is considered reputable if it's recommended many times.

3) *Recommendation*

The recommendation towards an organization is given by the authority CAA while basing on the history collaborations. This recommendation permits to calculate the reputation parameter. We take that the recommendation value can be '0' or '1', which means that an organization is recommended or not.

After calculating different trust parameters, we use the Fuzzy Logic to calculate the total trust score which is presented by the combination of the cited parameters and then to take the collaboration decision.

D. *Fuzzy Logic Principle*

The Fuzzy Logic [36] presents an extension of classical logic and more flexible than it. It is based on the introduction of the notion of degree in the verification of a condition and it allows different degrees between '0' and '1'. The rules in fuzzy logic are set in natural language which makes this type of logic similar to human reasoning. To establish the fuzzy logic system, a set of concepts and notions must be defined:

1) *Linguistic variables:*

A parameter or a variable is called linguistic variable if its value is expressed in natural or artificial language and not a numerical value. For a system based on fuzzy logic, we define the linguistic variables of input and output parameters. And for each variable, we specify its linguistic values. Each linguistic variable is defined by the triplet (V, X, T).

- V: The symbolic variables. They generally present the system parameters (inputs and outputs) and are presented initially by numerical values;
- X: Reference Set;
- T: A finite set of fuzzy subsets.

2) Membership functions:

The membership function is the representation of fuzzy subsets of linguistic variables. We define each fuzzy subset by a membership function F: X → [0,1].

Several membership functions are described but the most used are the triangular and trapezoidal functions, given their simplicity and usefulness.

3) Fuzzy Knowledge Bases (fuzzy if-then rules):

Generally, fuzzy logic is based on the combination of the input variables to calculate the output variables. This combination is made using Boolean operators AND, OR ... by introducing the concept of if-then rules. These rules are constructed from human expert's knowledge and different previous behavior. These rules permit to present the output variables as linguistic variables.

A fuzzy logic system contains four steps in general: fuzzification, if-then rules, aggregation and defuzzification. These steps are used as follows:

1. Determination of the input and the output of the fuzzy logic system;
2. Selection of the membership functions;
3. Conversion of input numerical values into linguistic variables using membership functions;
4. Determination of the if-then rules and applying them on the fuzzy input parameters;
5. Using deffuzification to convert fuzzy values to numerical values as the output.

In the next section, we explain the evaluation of different trust parameters using the fuzzy logic principle.

E. Trust evaluation using the Fuzzy Logic technique

As discussed in [16], we use the fuzzy logic to evaluate the trust of different entities participating in the collaboration. In this sense, we choose the satisfaction and the reputation parameters as input variables of our fuzzy logic system, and the output parameter is the trust score that permits to take the collaboration decision.

We present the satisfaction parameter by five linguistic values: very low, low, medium, high, and very high. The reputation parameter is presented by five linguistics values: very bad, bad, normal, good and very high. Based on the principle of fuzzy logic used in [16], we generate the output parameter: Trust score, using seven linguistics values: unacceptable, very weak, weak, normal, acceptable, high, and very high. Then, we use the defuzzification method to generate the numerical value of trust score. The figure 7 summarizes all steps described the application of fuzzy logic in Tr-OrBAC.

Satisfaction and reputation numerical values are calculated from the equation (1) and (2);

The Fuzzification method permits to translate the numerical values to linguistic values using the membership functions (Triangular and Trapezoidal membership functions).

Based on the linguistic values and the Fuzzy knowledge bases which presents the human expert's knowledge, we generate the different Fuzzy rules giving the possible linguistic values of the output parameter (trust score).The defuzzification method is then used to translate the linguistic variables to a unique and crisp numerical value.

The objective of using the fuzzy logic in our context is to permit to each organization to be autonomous in making its collaboration decision.

After calculating the trust score, it will be compared to the threshold defined by the CAA in order to generate the security rules and to achieve the collaboration. To summary different steps of Tr-orBAC using fuzzy logic, we present the figure 7.

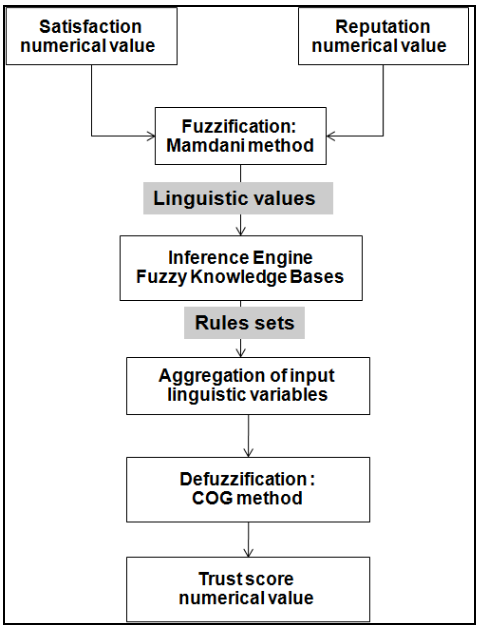

Satisfaction numerical value
Reputation numerical value
Fuzzification: Mamdani method
Linguistic values
Inference Engine Fuzzy Knowledge Bases
Rules sets
Aggregation of input linguistic variables
Defuzzification : COG method
Trust score numerical value

Figure 7. Fuzzy Logic steps in Tr-OrBAC

In order to illustrate our approach, we use in the next section the electrical grid as case study.

V. Tr-OrBAC: Application in Electrical Grid

Our approach will be applicable in many critical infrastructures requiring collaboration between different organizations. Among these infrastructures, we interest to the power grid as Critical Infrastructure, seen that each critical infrastructure depends on its electrical grid. Thus, we must first of all, ensure the security of the power grid and therefore, we secure the other critical infrastructures.

A. Why Electrical Grid?

By examining different infrastructures having a major importance for the security and continuity of a country, we put emphasis on the electrical grid considering that many Critical Infrastructures strongly depend on its electrical grid that must be available 24 hours per day. In this sense, several approaches have been proposed to secure the Electrical Grid Infrastructure such as [2], and more particularly their Information Systems.

Thus, in this paper, we interest to apply our approach in the Electrical Grid. First, we define this kind of Infrastructure, and then, we apply our scenario in its different components (organizations).

B. *Electrical Grid Architecture*

We inspire our architecture of the electrical grid from CRUTIAL project architecture as presented in the following part.

The CII architecture[3]is presented by a set of LANs (Local Area Networks) interconnected by dedicated switches forming a WAN (Wide Area Networks).These switched are named CIS (CRUTIAL Information Switch). Each LAN has its own logical/physical systems, its own applications and access control policy, its own resources and services... Each LAN presents an electrical organization (power plant, substation, companies...), and the WAN interconnects all the organizations belonging to the Critical Infrastructure. The CII is managed and accessed by different actors and organizations (power generation, transmission and distribution companies, regulation authorities...)

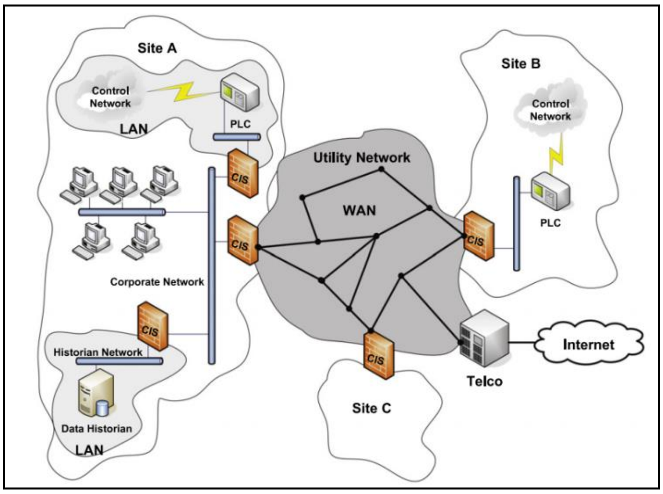


Figure 8. General architecture of CRUTIAL CII [3]

To more understand the presented architecture and the application of Tr-OrBAC on its entities, figure 9 presents a simple architecture containing different organizations forming the electrical grid.

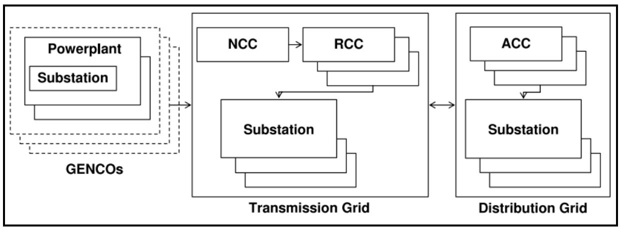


Figure 9. Electrical power grid architecture[27]

- **GENECOs**: Generator Companies (Organizations) contain different power plants; they generate electricity from different resources: Coal, Solar, Wind...
- **Transmission Grid**: is responsible for electricity transformation to different voltages and for its transmission to Distribution grid. It's managed by Transmission System Operator and contains different substations monitored by National Control Center (NCC) and Regional Control Centers (RCC).
- **Distribution Grid**: is responsible for distribution electricity to end users. It's managed by distribution system operator and contains different substations monitored by Area Control Center (ACC).

C. *Implementation of Tr-OrBAC in Electrical Grid*

In order to present the implementation and the application of Tr-OrBAC in the electrical grid, we take as an example an engineer (belongs to a role) of the Distribution Organization. The role wants to access to resources in the Transmission Organization to discover the procedure of transformation of electrical energy to different voltages. The aim is to distribute the electrical energy to the end users according to their needs. This is the objective of the collaboration between the transmission and the distribution organizations. In particular, the various entities into the electrical grid are critical. So, we must seek the best methods to secure them.

Each organization must evaluate the trust of the entity of other organization before collaborating and presenting the possible access. We assume that the distribution organization has already evaluated the reliability of desired resources in the transmission organization. Then, it wants to ask for collaboration. The figure 10 details different steps to establish Tr-OrBAC in the electrical grid.

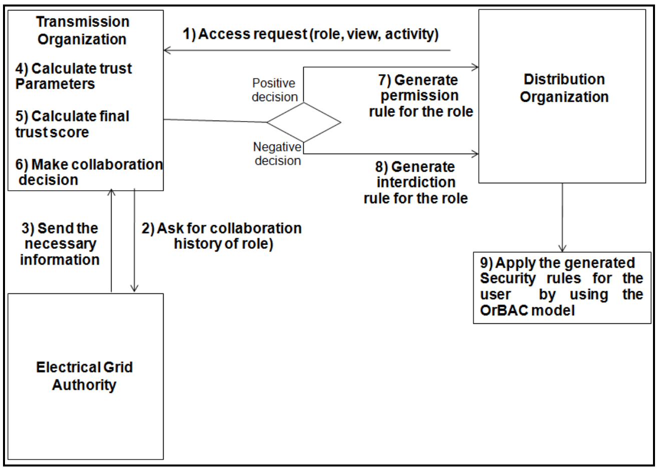

Transmission Organization
4) Calculate trust Parameters
5) Calculate final trust score
6) Make collaboration decision
1) Access request (role, view, activity)
Positive decision
Negative decision
7) Generate permission rule for the role
8) Generate interdiction rule for the role
Distribution Organization
3) Send the necessary information
2) Ask for collaboration history of role)
9) Apply the generated Security rules for the user by using the OrBAC model
Electrical Grid Authority

Figure 10. Tr-OrBAC applied in the electrical grid

Generally, the distribution organization is responsible to assign its users to the roles based on their functions and duties. Thus, a request will be sent by the distribution organization to the transmission one asking the role access to a view (set of resources) in the transmission organization (1).

The transmission organization contacts the Authority of the electrical grid to collect the information, needed to evaluate the reliability of the role (2). In this sense, the transmission organization calculates the trust parameters mentioned above: satisfaction, reputation (4). The calculated parameters leads to calculate a total trust score (5) by applying the fuzzy logic system. And then, compare the calculated trust score with the trust threshold, already defined by the authority.

If the role has an acceptable trust score, relative to the requirements and the security standards set by the transmission organization, the role can access to desired resources to accomplish an activity (7).

Therefore, the administrator of the transmission generates the security rules of the OrBAC model by integrating the trust variable in the rules that determines the type of access attributed to this role.

VI. Interpretation and discussion

The aim behind the proposed model is to permit to each organization to take its collaboration decision according to the evaluation of different trust parameters by using the fuzzy logic. This decision is own for each organization. Therefore, the organization provides to the role the access to the desired view. This access can be:

- **Access without any limits;**
- **Access under the conditions set by the organization;**
- **Access prohibited.**

We associate to each trust score value, an access type as cited below:

If the trust score value belongs to {unacceptable, very weak, weak}, then the generated security rule is the form:

Prohibition ('org', 'role', 'view', 'activity', 'context', 'trust _score')

This means that the service provider 'org' prevents the 'role' to access to 'view' to perform the 'activity' under some 'contexts'. We add in the generated security rules the trust value to justify the type of the rule.

If the trust score value belongs to {normal, acceptable, high, very high}, then the generated security rules is the form:

Permission ('org', 'role', 'view', 'activity', 'context', 'trust_score')

This means that the service provider 'org' permits the 'role' to access to 'view' to perform the 'activity' under some 'contexts'.

- If the trust_score is normal or acceptable, the access is presented with some conditions and limits defined by the organization.
- If the trust_score is high or very high, the access is guaranteed to the role without limits.

VII. Conclusion and Future works

In this paper, we have proposed a framework for Critical Information Infrastructures that enables potential collaborations based on trust evaluation. The main idea was to allow each organization to establish its collaboration decisions with other organizations based on behaviors of different participating actors in the past.

This has been made possible by introducing evaluation of trust entities into the well-known OrBAC model. Our contribution relies on a fuzzy logic technique that calculates and evaluates different trust parameters before proposing a trust score. Furthermore, we have illustrated our approach in the electrical grid as an important CI in every country.

In an ongoing work, we investigate further issues about trust parameters including their limits. Furthermore, the implementation of the proposed approach will be validated using appropriate verification tools.

References

[1] B. Kouns and J. Kouns, "The chief information security officer insights, tools and survival skills", Ely: IT Governance Pub., 2011.

[2] J. Moteff and P. Parfomak, “Critical infrastructure and key assets: definition and identification”, 2004.

[3] A. Abou El Kalam, Y. Deswarte, A. Ba ïna, and M. Kaâniche, “PolyOrBAC: A security framework for Critical Infrastructures”, International Journal of Critical Infrastructure Protection, vol. 2, no. 4, pp. 154–169, Dec. 2009.

[4] A. Baina, A. A. El Kalam, Y. Deswarte, and M. Kaaniche, “Collaborative Access Control For Critical Infrastructures”, in Critical Infrastructure Protection II, Springer, pp. 189–201, 2009.

[5] R. Zhou and K. Hwang, “Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing”, IEEE Transactions on Parallel Distributed Systems, vol. 18, no. 4, pp. 460–473, 2007.

[6] F. Cuppens, N. Cuppens-Boulahia, and C. Coma, “O2O: Virtual private organizations to manage security policy interoperability”, in Information Systems Security, Springer, pp. 101–115, 2006.

[7] A. A. E. Kalam and Y. Deswarte, “Multi-OrBAC: un modèle de contrôle d’acc ès pour les syst èmes multi-organisationnels”, pp. 67 – 85, 2006.

[8] B. Nasser, R. Laborde, A. Benzekri, F. Barr ère, and M. Kamel, “Access control model for inter-organizational grid virtual organizations”, in On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops, pp. 537–551, 2005.

[9] S. Ruohomaa and L. Kutvonen, “Trust management survey”, in Trust Management, Springer, pp. 77–92, 2005.

[10] R. S. Sandhu, “Role-based access control”, Advanced Computer, vol. 46, pp. 237–286, 1998.

[11] M. Hawa, L. As-Sayid-Ahmad, and L. D. Khalaf, “On enhancing reputation management using Peer-to-Peer interaction history”, Peer--Peer Network Applications, vol. 6, no. 1, pp. 101–113, Mar. 2013.

[12] A. Can and B. Bhargava, “SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems,” IEEE Transaction on Dependable Secure Computer, vol. 10, no. 1, pp. 14–27, Jan. 2013.

[13] L. Xiong and L. Liu, “Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities,” IEEE Transactions on Knowledge Data Engineering, vol. 16, no. 7, pp. 843–857, 2004.

[14] A. A. E. Kalam, R. E. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin, “Organization based access control,” in IEEE 4th International Workshop on Policies for Distributed Systems and Networks, Proceedings. POLICY 2003, pp. 120–131, 2003.

[15] N. AitAali, A. Baina, and L. Echabbi, "Tr-OrBAC: A Trust model for Collaborative Systems within Critical Infrastructures", in the 5th World Congress on Information and Communication

Technologies(WICT'15), Marrakeh, Morocco, 2015, under publication.

[16] N. Ait Aali, A. Baina, and L. Echabbi, "Making Collaboration Decision in Collaborative Systems by evaluating Trust using Fuzzy Logic", Submitted to the Fourth International Conference on Networked Systems, Netys 2016, Rabat, Morocco, 2016.

[17] N. Ait Aali, A. Baina, and L. Echabbi, “Trust Management System for Critical Information Infrastructures: Application to Electrical Grid, Submitted to the Second International Conference en Electrical and Information Technologies, ICEIT'16, Tangier, Morocco, 2016.

[18] W. Tolone, G.-J.Ahn, T. Pai, and S.-P. Hong, “Access Control in Collaborative Systems”, ACM Computing Surveys, vol. 37, no. 1, pp. 29–41, Mar. 2005.

[19] R. (Raj) Rajkumar, I. Lee, L. Sha, and J. Stankovic, “Cyber-physical Systems: The Next Computing Revolution,” in Proceedings of the 47th Design Automation Conference, New York, NY, USA, pp. 731–736, 2010.

[20] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies”, IEEE Control Systems, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[21] G. Hedlund, Organization of Transnational Corporations. Taylor & Francis, 1993.

[22] J. Park and R. Sandhu, “Towards usage control models: beyond traditional access control”, in Proceedings of the seventh ACM symposium on Access control models and technologies, pp. 57–64, 2002.

[23] H. C. Van Tilborg and S. Jajodia, "Encyclopedia of cryptography and security", Springer Science & Business Media, 2014.

[24] M. Benantar, "Access control systems: security, identity management and trust models", Springer Science and Business Media, New York, 2006.

[25] K. Toumi, C. Andrés, and A. Cavalli, “Trust-orbac: A trust access control model in multi-organization environments”, in Information Systems Security, Springer, pp. 89–103, 2012.

[26] N. Saxena and B. Choi, “State of the Art Authentication, Access Control, and Secure Integration in Smart Grid”,Energies, vol. 8, no. 10, pp. 11883–11915, October 2015.

[27] A. Baïna, “Controle d’accès pour les grandes infrastructures critiques. Application au r éseau d’énergie électrique”, INSA de Toulouse, 2009.

[28] E. Gaillard, “Les syst èmes informatiques fond és sur la confiance: un état de l’art”, 2011.

[29] S. Wang, “A Community-Based Trust Management Framework in P2P Systems”, in Proceedings of the Second International Conference on Innovative Computing and Cloud Computing, New York, NY, USA, pp. 267:267–267:270, 2013.

[30] S. Chakraborty and I. Ray, “TrustBAC: Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems”, in Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies, New York, NY, USA, pp. 49–58, 2006.

[31] M. B. Saidi, A. A. Elkalam, and A. Marzouk, “TOrBAC: A Trust Organization Based Access Control Model for Cloud Computing Systems”, International Journal of Soft Computing Engineering, IJSCE ISSN, pp. 2231–2307, 2012.

[32] M. B. Saidi and A. Marzouk, “Multi-Trust_OrBAC: Access Control Model for Multi-Organizational Critical Systems Migrated To the Cloud”, 2013.

[33] R. L. Benedicktus, “The effects of 3rd party consensus information on service expectations and online trust,” Journal of Business Research, vol. 64, no. 8, pp. 846–853, 2011.

[34] N. AitAali, A. Baina, and L. Echabbi, “Trust integration in collaborative access control model for Critical Infrastructures”, in 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA), pp. 1–6, 2015.

[35] L. Mui, M. Mohtashemi, and A. Halberstadt, “A computational model of trust and reputation”, in Proceedings of the 35th Annual Hawaii International Conference on System Sciences,HICSS, pp. 2431–2439,2002.

[36] A. Zadeh, “Fuzzy sets,” Inf. Control, vol. 8, no. 3, pp. 338–353, Jun. 1965.

Author Biographies

First Author: Nawal AIT AALI was born in Khouribga, Morocco on March 28th, 1989. She completed her engineering studies of Telecommunication systems and networks from the University of Hassan the first, National School of Applied Sciences from 2007 to 2012, khouribga, Morocco. Currently, she is preparing her Phd in Computer Science at the National Institute of Posts and Telecommunications, Rabat, Morocco, with Critical Infrastructures protection as the domain of her study.

Second Author: Amine Baina is an Assistant Professor at National Institute of Posts and Telecommunications Rabat, Morocco. He had his PhD in Computer Science in "Access Control for critical infrastructure" from the Laboratory of Systems Analysis and Architecture in Toulouse. He had his Computer Engineer’s degree from the National Engineering School of Bourges, France.

Third Author: Loubna ECHABBI is qualified a Senior Lecturer in France, since December 2005 and an Associate member of the team ALCAAP PRISM Laboratory, Versailles. She received her PHD in Algorithms for the allocation and pricing of resources in telecom networks with service guarantees in September 2005. Currently, she is a professor at National Institute of posts and Telecommunications, Rabat, Morocco.