Hindawi
Security and Communication Networks
Volume 2018, Article ID 7938727, 15 pages
https://doi.org/10.1155/2018/7938727

Research Article

Trust Management in Collaborative Systems for Critical Infrastructure Protection

Nawal Ait Aali, Amine Baina, and Loubna Echabbi

STRS Laboratory, National Institute of Posts and Telecommunications, Rabat, Morocco

Correspondence should be addressed to Nawal Ait Aali; nawal.aitaali@gmail.com

Received 3 February 2018; Revised 6 June 2018; Accepted 14 June 2018; Published 24 July 2018

Academic Editor: Sherali Zeadally

Due to the necessity of Critical Infrastructure (CI) Protection against different threats, several security policies must be applied among the organizations of CI. Based on our conducted study about the different constraints and requirements of the collaborative systems within CI, we reached a security solution: Tr-OrBAC. Its principle is to evaluate the trustworthiness of collaborating organizations based on relevant trust criteria aimed at enhancing collaboration decision-making. The taken decision presents the attribution of the access to the desired service based on calculated trust score which is the result of the combination of the trust criteria values. Generally, the desired services do not meet the same criticism, security requirements, sensitivity, etc. Also, the collaboration context varies from a set of collaborating organizations to another. In this sense, the importance of each trust criterion depends on the desired service and the collaboration context. In this paper, we focus on detailing the trust criteria used in our approach for collaborative system security. Then, we analyze the context variability with the trust evaluation process. In addition, we present a case study to demonstrate and illustrate the feasibility of our solution for CI protection, especially the electrical grid.

1. Introduction

Due to the importance of various Critical Infrastructures (CI) [1] in the development and the continuity of the country's socioeconomic activities, these infrastructures integrate information and communication technologies (Critical Information Infrastructure: CII) [2] which facilitate the performance of their activities. In addition, the revolution of new technologies, known in recent decades, has also affected these Critical Information Infrastructures; in each second, new services have appeared, resources are shared, and data are disclosed. This revolution led to the emergence and the establishment of collaborations between organizations (collaborative system) [3] in order to achieve the various operations. These latter (operations) are necessary for the proper functioning and the progress of the information systems of these organizations in particular and the CII in general. The purpose of developing collaborative systems is, therefore, to share several resources and services between organizations, if necessary, in order to carry out the operations or to delegate to an organization the task to perform an activity itself [4].

Although this collaboration brings several benefits to Critical Information Infrastructures (the continuity of their activities, the diversity of services offered, and sharing resources), it threatens the security of collaborative systems and their constituent organizations; due to the competition between collaborating organizations, an organization that requests the access to resources and services from another organization may introduce and commit malicious activities that destroy the service provider. To address these threats, a set of security procedures must be considered including the authentication of collaborating organizations, the authorization management, and then the access control by enforcing a set of security rules that manages the access between organizations in a secure way. In the case of centralized systems (the existence of a centralized authority) [5], the management of interorganizational access is ensured by this authority given that it is acquainted with the behavior and the activities of these organizations. Despite the fact that the centralized systems are more secure through the use of a centralized trust unit which controls the behavior of collaborating organizations, these organizations lose their autonomy and their privacy [6], besides their collaboration

decision-making [7]. In this context, the decentralized systems (peer-to-peer) become more important. In peer-to-peer systems [8], the organizations are more autonomous, and each one is responsible for managing the access to its resources in order to keep the sensitive and Critical Information and data more confidential.

However, the need to perform an essential operation in the Critical Infrastructure requires collaboration between organizations even though they do not know each other. In this sense, the organizations having malicious intentions [9] threaten the shared resources and services offered by other organizations. For this reason, each organization must evaluate the reliability of the requesting organization before assigning it the access rights to its services and resources. This evaluation is based on the requester's history in order to evaluate its behavior in past collaborations for predicting its behavior in future collaborations. In this context, we present in this paper our trust model named Tr-OrBAC [10]. It aims to secure shared services between organizations through the trust evaluation of organizations. This evaluation is made by calculating the proposed trust criteria (satisfaction, reputation, and recommendation) that are based on each dimension and characteristic of collaborative system. Depending on the collaboration context, the importance of these criteria varies from one context to another. For this reason, we use the AHP method [11] for multicriteria analysis to assign to each criterion a coefficient indicating its importance in a given context. The calculated trust score allows the service provider to make its collaboration decision and to generate the appropriate trust rules that manage the access to the requested service.

In order to demonstrate the feasibility of the proposed solution (Tr-OrBAC) in a context of interorganization collaboration in particular, and in a Critical Infrastructure in general, we detail an example of collaboration within the electrical grid/power grid [13].

The protection of the power grid is considered critical and essential as each CI depends on its own power grid. Besides, any malfunction of this grid leads to serious consequences and material losses as it is the case of the 2003 blackout [14]; such a power surge in western New York and Canada caused a power outage and, consequently, a blackout in eight states of America was raised. This led to serious industry and business aftermaths (financial losses), in addition to the deterioration of the health of patients in hospitals. And the airports of the affected states were seriously disrupted by delays and cancellations of flights, besides the subways and the trains stopping.

The main cause of this disaster was due to the failure of a transmission line (for reasons of cable expansion). Therefore, the load has been redistributed on alternative lines; those relays are not equipped with overload encroachment detection, which has evoked the interruption of the other transmission lines. A second time, the redistribution was performed on the remaining lines which lead to a high load and a high power oscillation. As a result, the power grid has collapsed.

In this context, the operations and activities within the power grid are more critical and must be carried out by entities deemed reliable. To this end, we present in this paper an example of collaboration between the electrical grid organizations by dealing with the various threats and attacks that affect its information system; then, we demonstrate the application of the proposed solution.

For this purpose, we detail, in Section 2, the related works by analyzing and discussing the different existing researches that treated the presented security problem. In Section 3, we introduce the architecture of our proposed solution Tr-OrBAC, its global steps, and the related preliminary concepts. Then, we explain, in Section 4, our mathematical model for trust evaluation by analyzing the different used trust metrics. After this, in Section 5, we introduce a case study (electrical grid) in order to demonstrate the feasibility of our solution; (1) we present the global architecture of electrical grid, (2) we discuss the encountered security issues, and (3) we take an example of collaboration context and we apply our trust model before discussing the obtained results. At the end, in Section 6, we conclude the paper and we present our perspectives.

2. Related Works

The collaborative systems within Critical Infrastructures have the same characteristics as collaborative systems established in such a context. This collaboration may or may not be based on the existence of a central entity that manages the communications and the exchanges between organizations. We thus distinguish between centralized, decentralized (more particularly peer-to-peer), and hybrid [15] collaborative systems. As we mentioned in the introduction, peer-to-peer systems have advantages over centralized systems with regard to the autonomy of organizations and the confidentiality of their data and information. But, the great concern of these organizations belonging to this system focuses on the security of access to their services. This access is threatened by the existence of several attacks that affect the services and the organizations in general. In this sense, we distinguish between two categories of attacks: an access attack and a denial of service attack. The first attack is an attempt to access a service by an unauthorized collaborator (user, organization), which threatens in particular the confidentiality of information and data. This attack is also unknown as "Hijacking" [16], while the second attack aims to make the service inaccessible to other collaborators by flooding it with a large number of requests and messages sent by the attacker [17], which prevents the good functioning of the service. Therefore, it will be saturated and it does not accept other access requests. In this context, it was obvious that the peer-to-peer systems attract many researchers' attention.

To secure peer-to-peer systems, trust management is considered the key to the success of the security. Ruohomaa and Kutvonen [18] describe trust, its origin, and some of its definitions, besides the objectives and missions of a trust management system. Mousa et al. [15] present a detailed and interesting survey that discusses the different types of trust systems, their classifications, and the definition and characteristics of each type especially for participatory sensing.

By detailing the existing works on trust management, they are classified into two categories: trust systems based on the exchange of certificates and trust systems based on the reputation and the calculation of various trust criteria. In the literature, several approaches have been interested in exchanging certificates between different entities in order to manage the trust. Winsborough and his colleagues [19] proposed a trust negotiation method based on the exchange of certificates between the user and the server. Z. Liao, H. Jin, and D. Zou proposed an approach [20] which aims to secure the exchange of certificates between the different actors. On the one hand, the certificates are hidden to increase the security level of personal data. On the other hand, the certificates have a lifetime; they are active for only one session of trust negotiation; at the end of the session, the certificates will have no effect. The same approach was used by Frikken et al. who proposed a protocol that hides the certificates and the security policies exchanged in a network, in order to ensure their security [21].

The exchange of certificates is not the only way to ensure the trust between different entities. Using the experiences of other entities is one of the most used techniques to manage the trust. In this sense, several parameters and criteria have been proposed to secure the access between the different entities. Each entity uses these criteria to calculate a total trust score to assign to another entity and decides the provision of the requested service. These trust criteria are the subject of several research efforts; the Power Trust model [9] offers powerful mechanisms for trust management in a network that can be threatened by malicious activities. This model is based on the concept of "power nodes" which are the most reliable nodes in the network. These nodes can be replaced by other ones if they become less active. The principle is that each node can communicate with the power nodes to calculate the trust score of another node [22] based on the interactions between the different nodes of the network. In contrast, the Peer Trust model [23] uses specific factors to calculate the global trust score. Thus, it is easy to implement it, but these factors are not always delivered by trusted nodes, which increases the probability of having malicious activities. The EigenTrust model [24] calculates the global trust score quickly using the existence of trusted nodes in the network, named "pretrusted nodes". But, these nodes can leave the network which leads to reliability loss. Also, the SecTrust [25] model aims to secure the trust management based on the use of public keys. However, the parameters used to calculate the trust in this model are insufficient. The SORT model [26] presents trust evaluation algorithm that allows each entity to evaluate the reliability of another entity based on local information that indicates its old interactions and recommendations. These models, cited above, are the base of new approaches for managing the trust in peer-to-peer systems. In [27], the authors propose a trust management model for wireless sensor networks, based on (1) Bayesian techniques for evaluating the direct trust score of an entity and (2) the entropy technique for calculating the weights attributed to each trust value. In [28], a model based on the principle of blockchain is proposed to manage the access and to protect the personal data. Also, a model named GenTrust [29] is added to the list of the trust management models which are applicable in peer-to-peer systems.

Other models have also been proposed aiming to manage the trust between the organizations when collaboration must be established between them (establishment of the collaborative system). These models combine the principle of access control and trust evaluation; we cite Trust-OrBAC [30], TOrBAC [31], Multi-Trust_OrBAC [32], TBAC [33], TrustAC [34], Trust-Based Context-Aware Access Control [35], Trust-Based Access Control [36], etc.

After studying these models, we conclude that they can not be applied in a collaborative system within Critical Infrastructures; this system (in CI) is established according to a well-defined context between CI organizations [12], which can be an emergency context, critical context, etc. And each context requires a specific trust management process. However, the models listed above manage the trust between entities in an identical way. Therefore, our strategy is to provide a dynamic trust model that takes into consideration the context of collaboration and shared services in trust management process. In this sense, the next section deals with our proposed solution, named Tr-OrBAC.

3. The Framework of the Tr-OrBAC

In this section, we aim to present the proposed security solution, its architecture, its several concepts, and the essential element for its construction.

3.1. Presentation and Architecture of Tr-OrBAC Framework. Based on our research on Critical Infrastructure (CI), we studied the different requirements and needs of the collaborative systems within the CI [37]. Among these requirements, we note the following:

(i) **Multiorganizations**: the collaborative system is characterized by the existence of several collaborating organizations; each organization has its own rules and policies for securing its resources and users. Thus, how do we create this system while respecting the different rules and policies in various organizations?

(ii) **Access control**: the objective of collaboration is allowing other organizations to use the accessible and available resources in another organization to perform tasks in the Critical Infrastructure. How can we keep access control on the resources and services while enabling successful collaboration?

(iii) **Trust management**: different organizations collaborate even if they are concurrent and unknown. Therefore, how can the organizations trust each other? What are the most important criteria used by different organizations to build trust between them?

(iv) **Malicious activities detection**: information systems of different organizations are managed by human being. Therefore, during collaboration, different concurrent organizations may generate malicious activities. How can organizations ensure that the organizations in a collaborative system are not malicious?

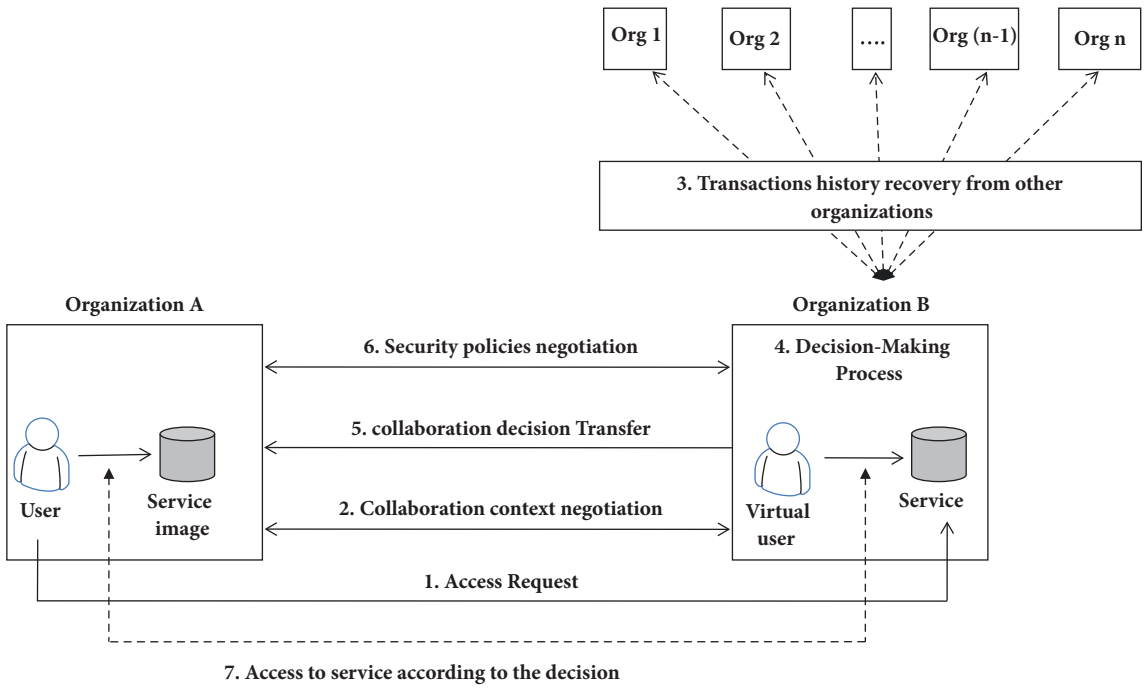

Figure 1: Global architecture of Tr-OrBAC.

What steps must be taken into account to prevent the production of malicious activities in the collaborative system?

Regarding the importance of these requirements, we proposed a security solution [7] while taking into account the autonomy and the confidentiality of the collaborating organizations and their services. In this sense, our solution is developed in order to secure the access to the desired services of the organizations and to avoid any attacks threatening them. The principle is to allow each organization offering a service to evaluate itself the reliability of the organizations wishing to gain access to its services and to make the collaboration decision based on the relevant trust criteria. After taking the collaboration decision, the organization providing the service (service provider) generates the appropriate trust rules for the requester. Therefore, our solution does not need an authority or super organization (central entity) to manage the access between organizations; the objective is to allow each organization to be autonomous in its decision as well as in the security management of its services and its resources.

Thus, our solution is based on a decentralized architecture; it consists of several steps in order to make the collaboration decision between organizations and to generate the trust rules.

Before presenting and discussing the different steps in our solution, we assume that the authentication phase of the collaborating organizations is already established and validated. Generally, in order to ensure the access to services and resources, two important levels of security must be validated: authentication and authorization management of accesses between organizations [38]. In our context, our trust model focuses only on the authorization management between organizations, respecting their confidentiality and autonomy. This authorization is presented in this paper by a model which is based on a set of trust criteria to evaluate the reliability of the requester and to generate the appropriate trust rules. Thus, we deal in principle with the authorization management aspect; we focus on the various problems encountered in the authorization management, the proposed solutions, methods, and existing techniques. This is why we considered that the authentication phase is assured [39]; several researches and works were intended to address and discuss authentication issues. Therefore, we assume that the organizations in our system are authenticated but they do not yet have the permission to access external services. Thus, Figure 1 presents a global architecture of our solution; it is based on seven steps; it begins by sending a service access request and it ends by responding to that request and generating the appropriate trust rules.

Step 1 (access request). This step triggers the establishment of a collaborative system when a service access has been requested. In this sense, the two organizations negotiate the collaboration context.

Step 2 (collaboration context negotiation). In this step, the organizations define the context of the collaboration given that each context type requires a specific trust evaluation process as we will explain all through this paper. Therefore, we discuss three types of contexts: normal context, emergency context, and critical context.

In the case study section, we will discuss and demonstrate the feasibility of our solution in the specific context. The presentation and the implementation of the other contexts are the subject of other papers.

Step 3 (transactions history recovery from other organizations). After the determination of the collaboration context, the organization providing the service contacts other organizations which have already established the collaboration with the requester organization in order to recover the necessary information for evaluating the reliability of the requester.

Step 4 (decision-making process). After discussing the collaboration context and recovering the necessary history files, the organization providing the service evaluates the requester reliability based on its history with other organizations in order to choose the appropriate access type. In this sense, we analyze the history files according to three trust criteria; satisfaction, reputation, and recommendation, also based on the chosen collaboration context. The objective behind this analysis is to generate collaboration decision which presents one of the following access types: permission, recommendation, and prohibition.

Step 5 (collaboration decision transfer). In this step, the organization providing the service transfers the established decision to the requester in order to discover the taken decision. And then, based on this decision, the two organizations agree on the trust rules.

Step 6 (trust rules negotiation). The two organizations negotiate the trust rules to decide which user has the access to the service in order to perform an action when we mention the collaboration context and the calculated trust score. We depend on the OrBAC model to generate the trust rules of the Tr-OrBAC model.

Step 7 (access to service according to the decision). The last step presents a response to the first one and it achieves the collaboration process by giving the access to the desired service according to the established decision.

Therefore, the proposed solution consists of a set of concepts, metrics, notations, data, etc. In this sense, we reserve the following parts of this section to present the necessary elements for more understanding of the functioning of our security solution.

3.2. Preliminary Concepts (Trust, Context, Service, User, Trust Criteria, Trust Score, and Trust Rules). In the following subsection, we aim to detail several concepts used in our proposed solution and, thereby, the relation between these concepts.

(i) **Trust:** *trust* is a complex term, defined in several research areas. This concept is an important tool in human life; it facilitates the interactions and the transactions between the foreign agents that can produce malicious activities during the completion of transactions. Until today, a unified definition for trust does not exist; the definitions are provided according to the use of the trust concept and its application areas. It may be attached to risk [40]; the level of trust is defined according to the risk that it can be produced. And it may depend on the situation [41] experienced by the actors. However, other researchers define trust as a bet on the future actions of others [42]. In our case, we define trust as a decision, taken between different collaborators based on a set of *trust criteria* which permit evaluating the behavior of the collaborators in future collaborations.

(ii) **Trust criteria**: in order to build trust towards a collaborator, some criteria must be fulfilled, named *trust criteria*. These criteria vary according to the objective of the collaboration (the access to a service), the collaboration context, the collaborators history, etc. In our proposed solution, we rely on three trust criteria (satisfaction, reputation, and recommendation) which we will define in the next subsection. The combination of these criteria permits assigning to each requester organization a *trust score* indicating its reliability.

(iii) **Trust score and trust threshold**: as we said, the *trust score* is calculated from the combination of the *trust criteria*. This score is compared to the *trust threshold* which is determined by the collaborators community. Based on the determined threshold, a collaborator whose trust score is calculated is considered either unreliable or reliable. ***Ts*** and ***Tt*** present, respectively, the *trust score* and *trust threshold*.

(iv) **Collaboration context:** the *context "C"* is defined as any information that characterizes the situation of an entity or that specifies the concrete circumstances in which the organizations grant the permissions to different users to perform several activities [43]. In our proposed solution, the context means the circumstance in which an organization requests the service access from another organization. Possible values for context are emergency, critical, and normal; we define the following:

Normal context: this context regroups all ordinary collaborations which can be defined by access to some files or directories in order to perform ordinary activities like consultation, reading, writing, checking, etc.

Emergency context: this context presents most emergency situations which require the collaboration between organizations and the intervention of other actors to perform some emergency activities (the load shedding in the power grid, the coverage of an area for a surprise event in the case of telecom operators, and the provision of a Microgrid with the energy necessary for its operation in case of failure (smart grid)).

Critical (sensitive) context: when the resource or the service contains sensitive data and information such as the personal information about the users and the organizations in general, the context is considered critical. A good example of a critical context is the defense domain which is considered a very Critical Infrastructure.

Consequently, in each context, specific trust criteria are required with varying weight of importance according to

Table 1: Relationship between resource, activity, service, and context.

Resources/Objects	Activities	Service	Context
Archives, Databases of activities and productions of the organization	Consulting, adding, modifying, checking	Normal	Normal
Electrical system, intra-organizational information system	Activating, turning off, deleting, adding	Emergency	Emergency
Accounts, personal information, secret activities	Consulting, adding, modifying, deleting	Critical	Critical

context. These criteria are used to evaluate the reliability of the requester organization wishing to be granted access to *a service* in a specific context.

(v) **Service:** we define a service by "the access to Resource/Object in order to perform an Activity". Thus, each service type "S" consists of a unique couple of Resources/Objects "O" (having the same characteristics such as security level, criticism) and Activities "A" (having also the same characteristics). This service is presented as ***S(O,A)***. In this sense, we associate with each service a collaboration context; consequently, each service type determines a collaboration context. We distinguish three categories of the services according to the Objects and Activities as presented in Table 1.

(vi) **User:** the *user* presented in our solution aims to gain access to a service in another organization for performing specific activities. This user may be an engineer, administrator, technician, director, etc. It depends on the desired service, the collaboration context, and the activities to be performed.

(vii) **Trust rules:** the objective of our solution is to generate the trust rules which manage the access to a service in a secure way. These rules are based on the OrBAC rules in which we add a new parameter "*Ts*" that indicates the trust score of the requester organization.

After presenting the different concepts used in our proposed solution and their preliminary notations, we discuss in the following section our mathematical model for calculating the trust of different collaborators in a collaborative systems.

4. Mathematical Model for Trust Evaluation

The trust evaluation in the proposed solution focuses on each dimension of the collaborative system:

(i) The realization of successful and completed transactions between organizations/collaborators.

(ii) The interaction between all the system collaborators (team and collaboration spirit).

(iii) The recommendation of the collaborators towards an entity for realizing a specific activity.

(iv) The determination of the collaboration context (the objective of the collaboration).

These different dimensions allow us to establish our trust model in a collaborative system. Like any trust model, the proposed model is based on three trust criteria which permit calculating a total trust score. Then, this score is compared to a trust threshold in order to take the collaboration decision and to generate the appropriate trust rules for the service access.

4.1. Trust Metrics. As we have mentioned above, the trust evaluation in our solution is based on three trust criteria, also named trust metrics. The calculation of these criteria is based on the collaborative system aspects.

4.1.1. Satisfaction Criterion. The ability to perform successful collaborations, within the collaborative system, presents one of the criteria that evaluate the reliability of an entity. An entity that accesses the resources of other entities and performs activities without malicious behavior is considered a trustworthy entity that has successfully accessed another entity. For this, we consider that any successful access is equivalent to the satisfaction of the entity providing the service.

As a result, the satisfaction of a set of entities towards the behavior of an entity is expressed by the ratio of the number of successful accesses to the total number of accesses (successful and unsuccessful), taking into account the novelty of the accesses and the novelty of collaborations. In fact, the new collaborations are more important than the old ones because they contain new conditions, requirements, needs, activities, services, etc. For this reason, an attenuation function h(i) [30] must be added to the calculation of satisfaction in order to indicate the impact of time on the satisfaction evaluation.

We express the satisfaction to an entity by

$$\mathrm{Sat}\left(\mathrm{Org_A}\right) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} S\left(\mathrm{Org_j}, \mathrm{Org_A}\right) * h\left(i\right)}{n} \quad (1)$$

$$S\left(\mathrm{Org_j}, \mathrm{Org_A}\right) = \begin{cases} 1 & \text{for successful collaboration} \\ 0 & \text{for failed collaboration} \end{cases} \quad (2)$$

- n is number of collaborations already completed.
- m is number of organizations expressing their satisfaction towards $\mathrm{Org_A}$ in collaboration i.

4.1.2. Reputation Criterion. In order to give access to a service (for an organization), the provider of this service looks for the reputation of this organization so as not to destroy the desired service. As presented in [18], "*The Reputation is defined as*

a perception a party creates through past actions about its intentions and norms".

In our collaborative system, the reputation of an organization increases through its honest participation in the trust evaluation of other organizations and, also, through the provision of its services to any reliable requester organization if needed. In this sense, an organization is considered well reputed if it is honestly active in a collaborative system. So, we calculate the reputation of an organization by the ratio of the sum of its honest participations and the availability of its services to the total number of its collaborations as defined in (3):

$$Rep\left(Org_A\right) = \frac{\sum_{i=1}^{k}\sum_{j=1}^{m} S\left(Org_A, Org_j\right) * T\left(Org_A, i\right) * h\left(i\right)}{k} \quad (3)$$

$$S\left(\mathrm{Org_A}, \mathrm{Org_j}\right) = \begin{cases} 1 & \text{if } \mathrm{Org_A} \text{ agrees that } \mathrm{Org_j} \text{ is reliable} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

$$T\left(Org_A, i\right) = \begin{cases} 1 & \text{if } \mathrm{Org_A} \text{ is considered reliable in the Collaboration i} \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

- This means that the Org_A recommends $\mathrm{Org_j}$ (participant) or it gives it the access to the desired service (provider).
- In order to consider just the honest participations and the providing service, we have to add the reliability of the Org_A in the equations: $T(Org_A, i)$.
- h (i) is the attenuation function.
- "k" is the number of collaborations in which Org_A has been a participant in the trust evaluation of an organization or a service provider and "m" is the set of organizations in collaboration i.

The objective of this criterion is to evaluate the ability and the motivation of an organization to secure the collaborative systems and to make its operation succeed by giving the access to its own services, if necessary, and by participating in the evaluation of other organizations, on the one hand, and, on the other hand, to encourage the organizations to behave honestly in order to increase their reputation, and, therefore, to have access to external services.

4.1.3. Recommendation Criterion. In some cases, the organizations recommend and choose one of them to perform an activity which is considered critical and sensitive; this organization must be well reputable within the collaborative system. As defined, "*the recommendation is simply an attempt to communicate the reputation and reliability of a party from one community context to another*" [18]. To this end, the recommendation to an organization must come from a set of organizations that are themselves deemed reliable and reputable. For this reason, we include in the calculation of the recommendation the trust score of the participating organizations in the evaluation as proposed in [36].

The advantage of integrating the trust of the recommender's organizations is to discriminate the malicious organizations in the trust evaluation of an organization and encourage all to participate honestly in the collaborative systems.

The formula for calculating an organization's recommendation is as follows:

$$Rec\left(Org_A\right) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} S\left(Org_j, Org_A\right) * Ts\left(Org_j, i\right) * h\left(i\right)}{\sum_{i=1}^{n}\sum_{j=1}^{m} Ts\left(Org_j, i\right) * h\left(i\right)} \quad (6)$$

- n is number of collaborations already completed.
- m is number of participating organizations in a collaboration i.
- Ts is the trust score of Org_j.
- h(i) is an integrated attenuation function in the equation to give more importance to recent collaborations.
- $S(Org_j, Org_A)$ is satisfaction of the Org_j towards the organization Org_A.

By establishing our mathematical model for the trust evaluation, we were aware that attackers can impersonate reliable organizations in order to access the services of other organizations. It is in this context that we consider all the activities and roles of the organization that requests the access to a service, as all its historical collaborations. These roles are integrated into the presented mathematical equations (of each trust criterion).

4.2. Collaboration Context-Based Trust Evaluation Variability and the Need of the AHP Method. The collaboration between the organizations is established within a context, called collaboration context. Each context type specifies the access to a range of services having the same characteristics and the same criticism level. Given the diversity of services which we classify as: critical, emergency, and ordinary (normal), the collaboration contexts are also classified as critical, emergency, and ordinary (normal). Each context requires a minimum level of trust to approve the reliability of the organization wishing to access the desired service based on one of the dimensions of the collaborative system.

Due to the diversity of the collaboration contexts and the multitude of the collaborative system dimensions to be validated, the trust criteria previously discussed do not have the same importance value; each criterion is considered important in a specific context. For this reason, we associate with each criterion a coefficient that indicates its importance in a given context.

In order to calculate these coefficients, we rely on the AHP multicriteria analysis method [7]. The calculation of the coefficients to assign to trust criteria will be discussed in the case study.

The coefficients associated with the trust criteria (after calculating phase) will be used to calculate the total trust score of the requester organization.

4.3. Trust Score. The definition and the calculation of the three trust criteria lead to calculating a total trust score for the requester entity by combining the calculated trust criteria. Regarding the collaboration context to access, the total trust score is based on the association of a coefficient to each criterion. Equation (7) presents our formula to calculate the total trust score:

$$\mathrm{Ts}\left(\mathrm{Org}, \mathrm{C}\right) = \alpha * \mathrm{Sat} + \beta * \mathrm{Rep} + \gamma * \mathrm{Rec} \quad (7)$$

Equation (7) signifies that the total trust score of an entity/organization "Org" in a specific context "C" is the sum of the values of the calculated trust criteria; each criterion is multiplied by its importance value (α, β, γ) in the given context.

The calculated trust score permits taking the collaboration decision and assigns to each requester entity the appropriate access according to its reliability. For this, the calculated score is compared to the trust threshold defined into the collaborative system (collaborators community) which presents a Reliability Indicator.

4.4. Reliability Indicator (Trust Threshold). To judge that an organization is reliable, we compare its computed trust score with the threshold determined by the organizations of the collaborative system. Several studies have been interested in presenting and proposing appropriate trust threshold in their trust models; in [44, 45], each entity decides its threshold, so it varies from one entity to another as presented in [46]. However, Huu Tran and his colleagues [47] propose to modify the trust threshold to share a file according to its quality and sensitivity. While other researchers adopt the trust score of an entity as a trust threshold, this entity is considered a super peer in its network [48]. Other researchers [22, 49–51] have set the trust threshold in their models at 0.5, while Leligou et al. [52] propose a dynamic trust threshold which depends on the application of the trust model in a specific domain, in order to guarantee a high security and excellent performance.

Regarding our model, since the trust evaluation is dynamic and it depends on the collaboration context between organizations, therefore the trust threshold is also context-dependent; some contexts (e.g., critical) require a high security level and, consequently, the trust threshold must be high in order to give access, only, to the organizations deemed to be completely reliable.

For a simple and understandable reading of our mathematical model, the Notations section lists the used notations and their description.

After we have presented and detailed our mathematical model, we discuss in the next section its implementation in a specific collaboration context in the electrical grid in order to demonstrate its feasibility.

5. Case Study: Experiments and Results

In order to illustrate the feasibility of our solution, we present in this section the electrical grid as a Critical Infrastructure; more particularly, we detail the integration of our solution in a collaborative system within the electrical grid. This section focuses on this issue in order (1) to present the electrical grid architecture, (2) to discuss the different attacks which threaten the presented architecture, and then (3) to apply our proposed solution in the studied collaboration context.

5.1. Introduction. The Critical Infrastructures [53] are defined by a set of organizations, equipment, and information systems. These elements are interconnected to provide a set of services and missions necessary for the proper functioning of the vital organs of the state. With the development of information and communication technologies, these CI are based in the collaboration between their organizations in order to make them more productive, which contributes to the development and the continuity of the socioeconomic activities of the countries. This interorganization collaboration appears in the functioning of the physical entities as well as in the logical entities and the information systems of these infrastructures. Among these Critical Infrastructures that require the collaboration, we mention the power grid, transportation network, the banking system, etc.

Given its importance and its strong dependence on other Critical Infrastructures [37], the electrical grid is one of the infrastructures that attracted the importance of the state by launching research programs and projects; their goal is to make the different operations within the electrical grid succeed in the transmission and the distribution of electricity to the end users without any excessive consumption of this wealth. To achieve this objective, the electrical grid is divided into three major organizations that are equipped with a control system in order to manage the transmission and the distribution of electrical energy.

5.2. Presentation of the Electrical Grid Architecture. The electrical grid consists of several organizations; each category has an important role in ensuring the continuity and the success of the electrical grid and reaching the objective behind its creation which is the distribution of the electricity to each human being, materiel, and organism. Generally, the electrical grid contains three types of organization: distribution, transmission, and generator as presented in Figure 2 which is reproduced from "Figure 2" in our preview work [7]. The electrical grid organizations are associated with one authority in the electrical grid.

(i) Generator Organization. It contains different power plants; it permits generating the electricity from different resources: coal, solar, wind, etc.

(ii) Transmission Organization. It is responsible for transforming the electricity to different voltages and for transmitting it to the distribution organizations. It is managed by Transmission System Operator and contains different substations monitored by National Control Center (NCC) and Regional Control Centers (RCC).

(iii) Distribution Organization. It is responsible for distributing the electricity to the end users. It is managed by

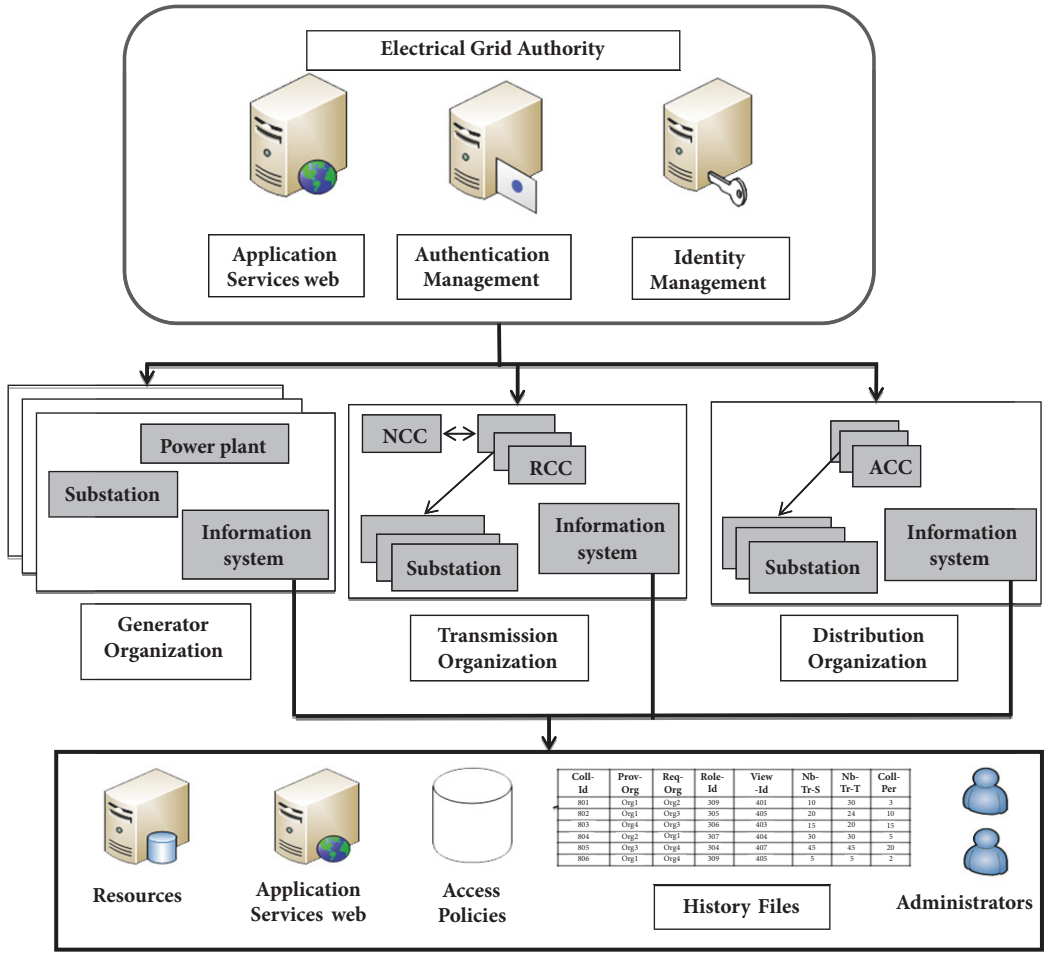

Figure 2: Electrical grid architecture [7].

the Distribution System Operator and it contains different substations monitored by Area Control Center (ACC).

In addition to these categories of organizations, an "*Electrical Grid Authority*" is presented; it has a control over the various organizations in order to coordinate between them.

Each organization has its own information system, its applications, and its own security policies, resources, services, history files, databases, and administrators who manage all these organization components as shown in Figure 2.

Due to the diversity of the electrical grid components and organizations, it is obvious that some security issues may be raised.

5.3. Security Issues in the Electrical Grid. The electrical grid is an indispensable infrastructure that aims to facilitate human life in general and satisfy their different needs. The electrical grid is considered as one of the sensitive parts of the State System in view of its important roles such as the distribution of the electricity to each individual or collective end user.

To achieve this goal, some transactions and collaborations are required between different electrical grid organizations. The aim of the collaboration is to share the required resources and services between organizations in order to successfully implement several operations in the electrical grid. For this reason, an organization needs access to the services of other organizations in order to perpetuate the electric chain which starts from the generation of electricity until its distribution to the end users. Focusing on the security aspects, access to services has some limits; the organization must disclose their personal information and data to allow them the access to the desired service. Also, the service may be accessed by some organization which intends to commit malicious activities (by their users).

We are therefore faced with a major challenge encountered in the electrical grid: it is the security of the services access. In this context, how can we ensure a proper management of electrical systems? And how can we protect the personal data and respect the organization privacy? Also, how can we protect the accessible services against any malicious activities?

To answer these questions, we will introduce an example of collaboration between two electrical organizations in order to illustrate the application of our solution.

5.4. Interorganization Collaboration Context in the Electrical Grid. In order to make the different operations within the

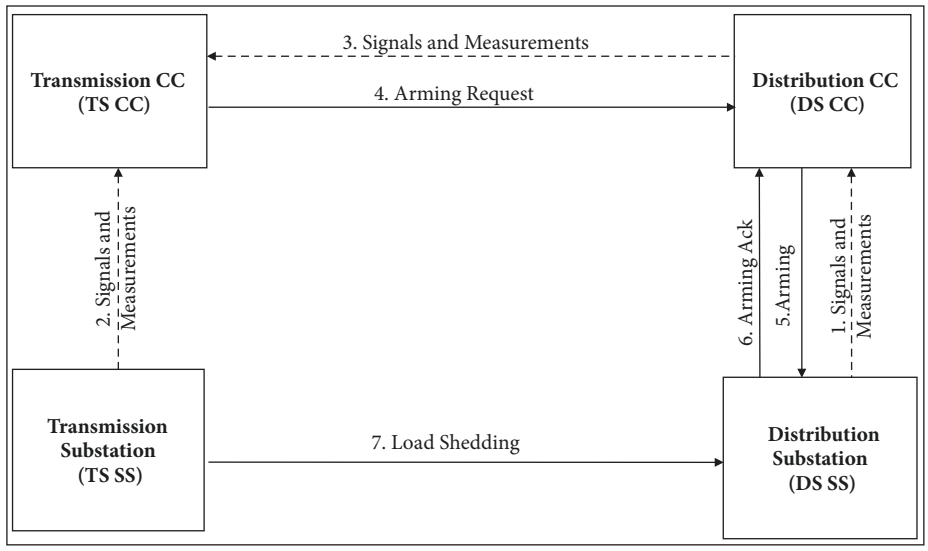

Figure 3: Exchange between distribution and transmission organizations [12].

electrical grid successful, such as the transmission and the distribution of the power energy to the end users (homes, companies, industries, etc.) and in order to intervene in the case of the electric outage and the failure of several components, a collaborative system is established between different organizations of the electrical grid whose objective is to operate the electrical system in a secure and successful way.

In this sense, we deal with, in this section, an example of the collaboration between the electrical organizations, specially the transmission and the distribution organizations. Actually, the choice of this collaboration example is not incidental; the operations carried out between these two organizations are critical and any failure can lead to serious consequences in the electrical grid.

In [12], a very detailed description of the electrical network along with the functioning of each of its organizations has been given. Also, an example of collaboration between the organizations was discussed. In this sense, we rely on this example in order to implement our solution. Figure 3 displays the communications between the transmission and distribution organizations, in which we explore the example of collaboration to be treated while making some assumptions, necessary for the implementation of our security solution for the protection of the electrical grid.

We distinguish four categories of organizations and in each category there is a set of organizations having the same characteristics and performing the same activities and operations.

(i) TS CC: Transmission System Control Centers, which are managed by the TSO (Transmission System Operator);

(ii) TS SS: Transmission System Substation;

(iii) DS CC: Distribution System Control Centers, which are managed by the Distribution System Operator (DSO);

(iv) DS SS: Distribution System Substation.

As [12] has shown, in order to protect the electrical grid for ensuring the continuity of its activities, a set of notification messages is exchanged between the four organizations. In the normal case, the Distribution System Substations (DS SSs) and the Transmission System Substations (TS SSs) send messages and signals containing power voltage and frequency information to the Transmission System Control Center (TS CC). The role of the latter, TS CC, is to control the electrical power system. When the TS CC detects that there is an overload in the power lines, it declares an emergency situation; therefore a set of DS SSs must intervene for an electrical load shedding. This operation must not disturb the distribution of the electricity to the end users. For this, the TS CC contacts DS SSs belonging to the emergency plan. Once the TS CC has determined the DS SS of the emergency plan, the load shedding will be activated. The principle of this operation is that a user (an engineer) of a TS SS activates the load shedding in the DS SSs. Due to human being and the competition between the different organizations, the access to the service (load shedding) may lead to serious consequences in the electrical grid instead of solving the problem. In this sense, the access to the service must be controlled by a set of trust rules.

In order to determine the type of access and the appropriate trust rules, an evaluation of the TS SS (which will be access to service) reliability is essential based on its history and behavior during its old accesses and collaborations with other organizations. Thus, by applying the trust evaluation, the DS SS makes the collaboration decision itself and it becomes more autonomous to generate and apply its security policies in order to protect its services and resources. Consequently, the organizations in our trust model are not based on the super organization (authority) for managing the access among them.

After we have depicted the electrical grid architecture and the collaboration scenario between its organizations in the emergency context, we focus in the next parts on

exploring the implementation of our solution in the mentioned context and on demonstrating its feasibility. More particularly, we focus on evaluating the reliability of the TS SS organization which will be responsible for activating the load shedding in the DS SS organization for the emergency context.

5.5. Experiment Environment. In order to generate the trust rules that reflect the reliability of TS SS organization and to manage its access to the DS SS resources, an authentication step is essential before evaluating the trust and managing the authorization. Generally, the access control consists of authentication and authorization management [54]; thus, we assume that the organizations are well authenticated and we focus on authorization management which is based on the trust evaluation of organizations. This evaluation allows or denies the access between the organizations.

In order to evaluate the reliability of the organization (TS SS) which will delegate its user to access the service of the DS SS organization to activate the load shedding, we present the following simulation environment.

The DS SS organization retrieves the history of TS SS in order to evaluate its reliability and assign it an access type. Table 2 shows an extract of collaborations history of the TS SS organization with the power grid organizations. Due to the lack of real data (actually) of the collaborations within the power grid, we rely on dataset, generated randomly. In fact, the collaboration between organizations is conditioned by the exchange of a great deal of information and data that makes it possible to evaluate the reliability of collaborating organizations. Given the criticality and importance of this data, it is essential to protect them against all attacks and threats by securing the communication and exchanges protocols between the collaborative system organizations. This issue enters into the security of the network layer.

Our objective is initially the security of access to services which is the security of the application layers. For this reason, we have not dealt with the case where the exchanges between the organizations are attacked over the network. Also, this point will be treated in our future works.

In the collaborations history, the TS SS organization had one of the following roles: Service Provider, Service Requestor, or Participant in the evaluation of another organization. So, as explained in our mathematical model, we take into consideration the played roles of organization to evaluate its reliability. Besides the role, the trust criteria scores (satisfaction, reputation, and recommendation) are also recorded for each collaboration.

The layout of the scene is as follows:

(i) We assume that the TS SS organization has already participated in 100 collaborations. In 80 collaborations, the TS SS has been a Service Requestor, and, in 20 collaborations, it was a participant or a provider. Thus, n = 80 and k = 20.

(ii) TS SS has requested the access to the services of other organizations in 80 collaborations and it has achieved 70 successful collaborations.

(iii) In the case when the TS SS was a participant in the evaluation of an organization, it participated honestly in 9 collaborations and it gave the access to its services just in two collaborations.

Besides, during its collaborations with other organizations, the TS SS organization has been recommended by six organizations to carry out activities within the power grid. We calculated the trust score of these organizations, namely, Org_A, Org_B, Org_C, Org_D, Org_E, and Org_F (Table 3). Among these organizations, four of them expressed their satisfaction towards the organization TS SS.

After the determination of the different trust criteria parameters, the coefficients associated with each criterion must be determined. Each coefficient indicates the importance of each criterion in the studied context, that is, an emergency context which signifies the activation of load shedding in the DS SS organization.

The objective behind the use of the AHP method in our solution is to assign to each criterion and each access type a coefficient which indicates its importance compared to others. In our trust model, we calculate three trust criteria: satisfaction, reputation, and recommendation, in order to choose one of the three access types: permission, recommendation, and prohibition. In this context, we reserve the next subsection to discussing the obtained results by applying our trust model Tr-OrBAC.

5.6. Results and Discussion. By analyzing the emergency context as described in this paper, the two organizations TS SS and DS SS must agree to activate the load shedding in the real time: the TS SS activates the load shedding in the DS SS. In this sense, the most important thing is that the chosen TS SS to perform the activity has the habit of performing this type of operations, especially in the emergency context. That is why the satisfaction criterion is more important than other criteria seen as it presents the success of this collaboration type.

Regarding the choice of the appropriate access type, the objective of the collaboration in the emergency context is to permit the TS SS to activate the load shedding. In this sense, the permission access type is more important than the other access types. Based on the analysis of the collaboration scenario, as well as the example of application of the AHP method in [7], we calculate the coefficients associated with the criteria as follows:

- α= 0.62
- β=0.078
- γ=0.3

Consequently, we calculate the three trust criteria:

- Sat=0.875
- Rep=0.55
- Rec=0.61

Then the total trust score is $\mathbf{Ts= 0.62*0.875+0.078*0.55+0.3*0.61= 0.76>Tt}$.

The calculated score must be compared to trust threshold in order to determine the access type to the requester and to

Table 2: Transaction history of the organization TS SS.

Collaboration_ID	played role	Collaboration_Context	Satisfaction_rate	Reputation_rate	Recommendation_rate
1032	requester	Emergency	1	0,4	0,2
1536	provider	Critical	0,3	0	0
1868	participant	Emergency	0,6	0	0,6
1034	participant	Normal	0,2	1	0,3
1718	provider	Emergency	0,6	0,3	0
1022	provider	Emergency	0,1	0,5	0,4
1519	participant	Normal	0,9	0,8	0,1
1740	provider	Normal	0,9	0,4	0,6
1590	requester	Critical	0,4	0	0
1298	requester	Critical	0,9	1	0,4
1470	requester	Normal	0,9	0,1	0
1760	provider	Emergency	0,7	0,2	0,4
1647	participant	Normal	0,4	0,5	0,9
1457	requester	Emergency	0,1	0,2	0,6
1136	participant	Emergency	0,2	0,7	0,2
1122	provider	Critical	0,8	0,1	0,1
...	...	...	...	...	...
....	...	...	...	...	...

Table 3: Trust scores of recommender organizations.

Ts (Org_A) = 0.7	Ts (Org_B) = 0.6	Ts (Org_C) = 0.6
Ts (Org_D) = 0.3	Ts (Org_E) = 0.5	Ts ($Org_{F)}$ = 0.9

generate the appropriate trust rules. Looking at the context of collaboration, that is, emergency, it does not rely heavily on critical data but rather a critical and urgent activity, which requires a moderately important trust score. In this case, we set the trust threshold in 0.7.

Compared to the trust threshold, the total trust score calculated is acceptable. Then the TS SS organization is reliable and it is permitted to access the DS SS organization in order to activate the load shedding. This access will be done by a user (an engineer) of the TS SS organization. If this user commits malicious behavior, the TS SS will be punished and then its trust score will decrease.

We concluded that the TS SS organization has an acceptable trust score that allows it the access to the service (load shedding activation). By analyzing the results obtained for each criterion, the TS SS organization has an acceptable trust scores for all the criteria (satisfaction, reputation, and recommendation). Therefore, the different roles that an organization can play in the collaborative system (requester, participant, and provider) help to increase its reliability among other organizations in the system as shown by the results of this simulation.

However, regarding the recommendation criterion, we have an organization (organization D) that has a lower trust score but it is satisfied with the collaboration with the TS SS organization and it recommended it. This contradiction leads us to thoroughly analyze the recommendations of other organizations to avoid false recommendations and incomplete (erroneous) satisfactions. This discussion will be the subject of another article.

In order to improve the efficiency of our trust model, we establish a comparative study between our model and the existing works, namely, TOrBAC, Multi-Trust_OrBAC, Trust-OrBAC, and TrustBAC, which combine the trust management and the access control. In [55], we have studied, theoretically, if these models meet the requirements of collaborative systems. However, none of the cited models takes into consideration all the discussed requirements and constraints. In our future works, we will compare the obtained simulation results with the others from established frameworks.

6. Conclusion and Perspectives

Through this article, a new trust model for collaborative systems within Critical Infrastructure is presented, in which an organization controls the access to its services by managing and evaluating the trustworthiness of the requester organization in a specific collaboration context. The proposed evaluation is based on the old collaborations of the requester in order to predict its behavior in future collaboration. Besides, the result of this evaluation is a set of trust rules which indicate the reliability of the requester and justify the assigned access type. For this aim, a mathematical model for trust evaluation was proposed; it is based on three trust criteria (satisfaction, reputation, and recommendation). As the collaboration between organizations is established in a specific context, it is obvious that the trust evaluation process varies from one context to another. In this sense, to each trust criteria value a coefficient (importance value) is added that changes according to the studied collaboration context. These coefficients are calculated based on the AHP method.

In order to demonstrate the feasibility of the proposed trust model Tr-OrBAC and to illustrate its implementation, a case study was integrated in this paper. The power grid is considered the most important Critical Infrastructure and each CI depends on its power grid for ensuring its functioning. That is why we have detailed a collaboration scenario between the electrical grid organizations in order to implement our trust model, more particularly, in an emergency context between the transmission and distribution organizations. The results and the discussion show that our trust model is applicable in the studied context in the electrical grid.

Therefore, this paper gives an overview on our trust model and its implementation in the power grid as a Critical Infrastructure. However, our work in this paper is limited in the illustration of the implementation of our trust model in the emergency context, while the other contexts are not covered in this paper. Also, the data (dataset), used to establish the trust evaluation, are generated randomly due to the lack of real data concerning collaborations between the organizations of the power grid. In addition, when the number of collaborations and recorded information increases, it becomes difficult to rely on these data for the trust evaluation (complicated tasks). Besides, our trust model aims to consider all of the roles played by organizations for evaluating their reliability in order to encourage them to behave and participate honestly in collaborative systems. Nevertheless, we did not discuss how to punish an organization if it commits a malicious action.

These limitations have prompted us to establish a plan for our future works. Firstly, we will discuss the implementation of the other collaborations contexts as well as a comparison of the results obtained of each context being established. Secondly, we aim to collect real data for the simulation part and we rely on the machine learning algorithms for processing and analyzing the collected data. Thirdly, we will discuss and simulate in our future papers how an organization that participates in the evaluation of the reliability of other organizations and one which offers its services increases its trust score and, consequently, it increases its reliability in the collaborative system. Also, we will treat the feasibility of applying our trust model in other CI as banking and telecommunications systems (collaboration between telecom operators).

Notations in the Proposed Trust Model

Ts:	Trust score
Tt:	Trust threshold
C:	Collaboration context
S(O,A):	A Service "S" defined by an Activity "A" performed on an Object "O"
n:	Number of collaborations carried out
m:	Number of organizations expressing their satisfaction towards an organization A
k:	Number of collaborations where Org_A has been a participant in the trust evaluation of an organization or a service provider
(α, β, γ) :	Weight of importance of the criteria according to a specific context
$Sat(Org_A)$:	Satisfaction of the organizations of the system towards the organization A
h(i):	Attenuation function
$Rep(Org_A)$:	Reputation of the organization A
$Rec\ (Org_A)$:	Recommendation of the organization A
$T(Org_A, i)$:	Trust of the Org_A in collaboration i
$S(Org_A, Org_j)$:	Satisfaction of Org_A towards Org_j.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Y. Deng, L. Song, Z. Zhou, and P. Liu, "Complexity and Vulnerability Analysis of Critical Infrastructures: A Methodological Approach," *Mathematical Problems in Engineering*, vol. 2017, Article ID 8673143, 12 pages, 2017.

[2] A. Abou El Kalam, Y. Deswarte, A. Baïna, and M. Kaâniche, "PolyOrBAC: A security framework for Critical Infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 154–169, 2009.

[3] M. Zhou, H. Li, and M. Weijnen, "Grey system: thinking, methods, and models with applications," in *Contemporary Issues in Systems Science and Engineering*, vol. 1, pp. 575–598, Wiley-IEEE Press, Hoboken, NJ, USA, 2015.

[4] A. A. Alsaffar, H. P. Pham, C.-S. Hong, E.-N. Huh, and M. Aazam, "An Architecture of IoT Service Delegation and Resource Allocation Based on Collaboration between Fog and Cloud Computing," *Mobile Information Systems*, vol. 2016, Article ID 6123234, 15 pages, 2016.

[5] A. J. Schmitt, S. A. Sun, L. V. Snyder, and Z.-J. M. Shen, "Centralization versus decentralization: Risk pooling, risk diversification, and supply chain disruptions," *Omega* , vol. 52, pp. 201–212, 2015.

[6] W. W. Smari, P. Clemente, and J.-F. Lalande, "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system," *Future Generation Computer Systems*, vol. 31, no. 1, pp. 147–168, 2014.

[7] N. A. Aali, Y. El Bouzekri El Idrissi, A. Baina, and L. Echabbi, "Collaboration decision making based on AHP method in Tr-OrBAC model: Case study," in *Proceedings of the 4th IEEE International Colloquium on Information Science and Technology, CiSt 2016*, pp. 779–784, Morocco, October 2016.

[8] Z. Yu, J. Zhu, G. Shen, and H. Liu, "Trust Management in Peer-to-Peer Networks," *Journal of Software* , vol. 9, no. 5, 2014.

[9] R. Zhou and K. Hwang, "PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 4, pp. 460–473, 2007.

[10] N. A. Aali, A. Baina, and L. Echabbi, "Tr-OrBAC: A trust model for collaborative systems within critical infrastructures," in *Proceedings of the 5th World Congress on Information and Communication Technologies, WICT 2015*, pp. 123–128, Morocco, December 2015.

[11] T. L. Saaty, "Decision making the analytic hierarchy and network processes (AHP/ANP)," *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, 2008.

[12] A. Baina, A. A. Kalam, Y. Deswarte, and M. Kaaniche, "Collaborative Access Control For Critical Infrastructures," in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi, Eds., vol. 290 of *IFIP – The International Federation for Information Processing*, pp. 189–201, Springer US, 2009.

[13] A. Baïna, *Controle d'accès pour les grandes infrastructures critiques. Application au réseau d'énergie électrique*, INSA de Toulouse, 2009.

[14] E. H. Allen, R. B. Stuart, and T. E. Wiedman, "No light in August: Power system restoration following the 2003 North American blackout," *IEEE Power & Energy Magazine*, vol. 12, no. 1, pp. 24–33, 2014.

[15] H. Mousa, S. B. Mokhtar, O. Hasan, O. Younes, M. Hadhoud, and L. Brunie, "Trust management and reputation systems in mobile participatory sensing applications: A survey," *Computer Networks*, vol. 90, pp. 49–73, 2015.

[16] "Session Hijacking," CEH^{TM} v9, Wiley-Blackwell, 2017: 331358.

[17] "Denial of Service," CEH^{TM} v9 - Wiley Online Library.

[18] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Proceedings of the Third International Conference on Trust Management, iTrust 2005*, pp. 77–92, France, May 2005.

[19] W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated trust negotiation," in *Proceedings of the DARPA Information Survivability Conference and Exposition, DISCEX 2000*, pp. 88–102, USA, January 2000.

[20] Z. Liao, H. Jin, and D. Zou, "A hidden credential based oblivious automated trust negotiation model," in *Proceedings of the ICEBE 2007: IEEE International Conference on e-Business Engineering - Workshops: SOAIC 2007; SOSE 2007; SOKM 2007*, pp. 247–253, China, October 2007.

[21] K. Frikken, M. Atallah, and J. Li, "Hidden access control policies with hidden credentials," in *Proceedings of the WPES'04: Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*, pp. 27-28, USA, October 2004.

[22] H. Zhao and X. Li, "VectorTrust: Trust vector aggregation scheme for trust management in peer-to-peer networks," *The Journal of Supercomputing*, vol. 64, no. 3, pp. 805–829, 2013.

[23] L. Xiong and L. Liu, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004.

[24] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in *Proceedings of the 12th International Conference on World Wide Web (WWW '03)*, pp. 640–651, May 2003.

[25] J. Hu, X. Li, B. Zhou, and Y. Li, "SECTrust: A secure and effective distributed P2P trust model," in *Proceedings of the 2010 International Symposium on Intelligent Information Technology and Security Informatics, IITSI 2010*, pp. 34–38, China, April 2010.

[26] A. B. Can and B. Bhargava, "SORT: a self-organizing trust model for peer-to-peer systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 1, pp. 14–27, 2013.

[27] S. Y. Che, R. J. Feng, X. Liang, and X. Wang, "A lightweight trust management based on Bayesian and Entropy for wireless sensor networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 168–175, 2015.

[28] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proceedings of the IEEE Security and Privacy Workshops, SPW 2015*, pp. 180–184, IEEE, May 2015.

[29] U. E. Tahta, S. Sen, and A. B. Can, "GenTrust: A genetic trust management model for peer-to-peer systems," *Applied Soft Computing*, vol. 34, pp. 693–704, 2015.

[30] K. Toumi, C. Andrés, and A. Cavalli, "Trust-orBAC: A Trust Access Control Model in Multi-Organization Environments," in *Information Systems Security*, pp. 89–103, 2012.

[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 and Engineering*, 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] N. Dimmock, J. Bacon, D. Ingram, and K. Moody, "Risk models for trust-based access control (TBAC)," in *Proceedings of the Third International Conference on Trust Management, iTrust 2005*, pp. 364–371, France, May 2005.

[34] F. Almenárez, A. Marín, C. Campo, and C. García R., "TrustAC: Trust-Based Access Control for Pervasive Devices," in *Security in Pervasive Computing*, D. Hutter and M. Ullmann, Eds., vol. 3450 of *Lecture Notes in Computer Science*, pp. 225–238, Springer, Berlin, Germany, 2005.

[35] R. Bhatti, E. Bertino, and A. Ghafoor, "A trust-based context-aware access control model for web-services," *Distributed and Parallel Databases*, vol. 18, no. 1, pp. 83–105, 2005.

[36] Y. Zhang, Y. Li, Z. Zheng, and M. Wu, "Dynamic Trust-Based Access Control Model for Web Services," in *Advances in Computer Science and Information Engineering*, D. Jin and S. Lin, Eds., vol. 168 of *Advances in Intelligent and Soft Computing*, pp. 527–534, Springer, Berlin, Germany, 2012.

[37] N. Ait Aali, A. Baina, and L. Echabbi, "Trust integration in collaborative access control model for Critical Infrastructures," in *Proceedings of the 10th International Conference on Intelligent Systems: Theories and Applications, SITA 2015*, Morocco, October 2015.

[38] A. T. Murray and T. Grubesic, *Critical Infrastructure: Reliability and Vulnerability*, Springer Science & Business Media, 2007.

[39] J. B. Bernabe, J. L. Hernandez-Ramos, and A. F. S. Gomez, "Holistic privacy-preserving identity management system for the internet of things," *Mobile Information Systems*, vol. 2017, Article ID 6384186, 20 pages, 2017.

[40] A. Jøsang and S. L. Presti, "Analysing the Relationship between Risk and Trust," in *Trust Management*, vol. 2995 of *Lecture Notes in Computer Science*, pp. 135–145, Springer, Berlin, Germany, 2004.

[41] D. H. McKnight and N. L. Chervany, "What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology," *International Journal of Electronic Commerce*, vol. 6, no. 2, pp. 35–59, 2001.

[42] D. Gefen, "E-commerce: The role of familiarity and trust," *Omega* , vol. 28, no. 6, pp. 725–737, 2000.

[43] A. Kalam, R. Baida, P. Balbiani et al., "Organization based access control," in *Proceedings of the POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, pp. 120–131, Lake Como, Italy.

[44] S. Song, K. Hwang, R. F. Zhou, and Y.-K. Kwok, "Trusted P2P transactions with fuzzy reputation aggregation," *IEEE Internet Computing*, vol. 9, no. 6, pp. 24–34, 2005.

[45] X. Kang and Y. Wu, "A trust-based pollution attack prevention scheme in peer-to-peer streaming networks," *Computer Networks*, vol. 72, pp. 62–73, 2014.

[46] N. Stakhanova, S. Ferrero, J. S. Wong, and Y. Cai, "A Reputation-based Trust Management in Peer-to-Peer Network Systems," in *Proceedings of the ISCA PDCS*, vol. 4, pp. 510–515, 2004.

[47] H. Tran, M. Hitchens, V. Varadharajan, and P. Watters, "A trust based access control framework for P2P file-sharing systems," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, p. 302, USA, January 2005.

[48] S. Javanmardi, M. Shojafar, S. Shariatmadari, and S. S. Ahrabi, "FR trust: a fuzzy reputation-based model for trust management in semantic P2P grids," *International Journal of Grid and Utility Computing*, vol. 6, no. 1, pp. 57–66, 2015.

[49] B. Yu, M. P. Singh, and K. Sycara, "Developing trust in large-scale peer-to-peer systems," in *Proceedings of the 2004 IEEE 1st Symposium on Multi-Agent Security and Survivability*, pp. 1–10, USA, August 2004.

[50] Z. Su, L. Liu, M. Li, X. Fan, and Y. Zhou, "Reliable and resilient trust management in distributed service provision networks," *ACM Transactions on the Web (TWEB)*, vol. 9, no. 3, pp. 1–37, 2015.

[51] B. Shafiee Sarjaz and M. Abbaspour, "Securing BitTorrent using a new reputation-based trust management system," *Peer-to-Peer Networking and Applications*, vol. 6, no. 1, pp. 86–100, 2013.

[52] H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 12, no. 12, pp. 1091–1103, 2012.

[53] J. Moteff et and P. Parfomak, "Critical infrastructure and key assets: definition and identification," 2004.

[54] I. Wakeman, E. Gudes, C. D. Jensen, and J. Crampton, "From Access Control to Trust Management, and Back – A Petition," in *Proceedings of the 5th International Conference on Trust Management (TM)*, pp. 1–8, 2011.

[55] N. A. Aali, A. Baina, and L. Echabbi, "Evaluation of interaction messages in trust model within collaborative system," in *Proceedings of the International Conference on Information Technology for Organizations Development, IT4OD 2016*, Morocco, April 2016.