Trust-Based Access Control in Storage Middleware Grids: A Reference Framework Proposal to Deploy in the Financial Sector

Francisco Nunes, Henrique O'neill

Trust-Based Access Control in Storage Middleware Grids: a Reference Framework Proposal to Deploy in the Financial Sector

Francisco Nunes[1], Henrique O'Neill[1]

[1] ISCTE/IUL, Avenida das Forças Armadas, 1649-026 Lisboa, Portugal
fjfnunes@gmail.com, henrique.oneill@iscte.pt

Abstract. Fostered by the development of the Web, the financial sector has been able to develop a broad set of shared IT services. Despite the high levels of maturity that have been achieved there are still improvement opportunities concerning the sharing of services by financial institutions. This research addresses the sharing of data storage resources among different financial organizations to fulfil the needs for unplanned peaks of data storage, or to help shortening the time needed to start projects requiring allocation of storage space when this is not available in the organization. To answer to these requirements it was proposed a data grid infrastructure (SRM), centrally managed by a versatile storage resource manager middleware. Senior IT infrastructure managers of representative financial organizations have been questioned to assess the proposed solution. Security has been identified as a key concern that prevents the dissemination of this type of solutions. These solutions may be fostered by the adoption of a security mechanism that would consider the behaviour of the distinct organizations in the use of the shared resources. To meet this requirement the research proposes an algorithm for controlling the access to the storage resources based on trust, where the level of trust in the joint organizations will vary dynamically according to the fulfilment of the rules concerning the use of the shared storage by its users.

Keywords: Data storage systems, TBAC, grid data storage, virtual organizations.

1 Introduction

This applied research project described in this paper has been sponsored by AdI under the "PhD in the Enterprise" initiative[1], a program that aims to contribute to the improvement of the Portuguese economy by addressing specific problems of the industry in topics that require further research. The project aims to improve the use of data storage resources by firms of the financial sector. It was developed in collaboration with two of the most important Portuguese banks. Like many other institutions in several sectors, banks have several ongoing IT projects of the most diverse nature. Sometimes these organizations have some difficulty in initiating some of these projects that rely on computational power in general and in particular depend

[1] AdI – Agência de Inovação – Doutoramento em Empresa

on the availability of space in data storage systems. These projects that need data space may begin immediately, if the disk space is available, or take up to three months or more if the disk space does not exist and involves an operation of procurement. To meet this need there are some institutions that aim to drastically reduce the average time of purchase and installation of new storage equipment by redesigning procurement processes.

After a thorough analysis of the problem [12] a framework was created to address the problem of availability of storage resources in order to deploy space in storage systems immediately or almost immediately, particularly for projects developed in the studied financial sector institutions. This framework will comprise the creation of a federated environment composed by different financial institutions with a centralized management. Each institution contributes with the storage resources that can provide at a given time, so it can help to fulfill immediate needs of any other institution belonging to this federated environment that does not have storage resources available at that time. The way to implement this framework implies that the shared storage resource management is done through the implementation of a common grid storage by using the same kind of middleware. The proposed middleware is based on the Storage Resource Manager (SRM) [1]. It meets the requirements of data operation of financial institutions and has been accepted by the architects and IT managers of these institutions. However the use of SRM for temporary data sharing lack security features (access control, acces and operations log) [4]. This is an issue also identified by the experts of the institutions that participated in the investigation. So, an element of security to control data access based on dynamic trust management systems was created and added to the framework. It enables to manage not only the access and use of resources by users of various institutions with access to the pool of shared resources, but also assesses the reputation and trust of the entities that provide the resources.

This work relies on a series of research results on models on Trusted Based Access Control, collaboration and sharing to generate an integrated framework. It also addresses issues related with the technical feasibility of the infrastructure and its implementation.

2 Contribution to Cloud-based Engineering Systems

Typically Cloud Computing refers to the hardware and software resources that are available via the Internet [2, 3]. The resources made available in this way are called IT services [4]. The features of these IT services are distinguished by being scalable, configurable, measurable and able to provide an easy access from the perspective of auto use.

The infrastructure that supports these services must be a structure with sufficient elasticity to satisfy the business services requirements. The infrastructure proposed in this research is based on a grid of data storage with clustering of resources dictated by the availability of each institution that belongs to the group that makes up the grid [4].

In the context of IT infrastructure and Cloud Computing the proposed grid data storage with centralized management, has precisely the main advantage of allowing of

inclusion of resources in the grid space to meet peak needs or to remove these resources when there if less need for space data [5]. This requires the ability to monitor the needs of the users and to adjust the elasticity of the Cloud supply.

The application of this technology can support different types of offering Cloud Computing services [6]. An example is to use the platform as part of a shared services infrastructure, for example by deploying a Private Cloud serving various companies of the same economic group. An alternative approach will be to share resources between various financial enterprises despite the allocation of a resource to be assigned specifically to one of the group companies [9]. This sharing of resources will be partial and temporary in nature. It will be guaranteed not to harm the infrastructure, the resource will be temporarily allocated according to a set of rules and the recovery of the resource will be ensured. By using the Cloud with this collaborative network approach, those who provide resources for these effects will also benefit from them in times of unforeseen need. This versatility in the context of data storage can be materialized by a grid infrastructure for data storage with centralized management, able to integrate the storage devices capabilities of institutions that have joined this sharing group in the federate environment..

The uses of a data storage shared infrastructure can thus be a privileged resource in the context of Cloud systems, as the type of application described or other that will be implemented.

3 Related Work

For trust management, access policies and authorization different approaches have been explored in distributed environments with centralized management. However, no unified definition of trust exists in the current literature of computer science [8].

Most settings found in work related to the classification of trust tend to only use a number, a slight degree, a marker or a combination of all. In this context, there are several ways to define and establish a trustful relationship. The trust is paramount in a relationship and can be negotiated if the collaboration is established between actual organizations. In other scenarios, the trust agreement may be specified by one party (e.g. a service provider) and accepted by the other parties, without negotiation (e.g. a service consumer). Yet another example of establishing trust implies that the trust agreement may be declared by a supervisory authority and be applied by all parties involved (e.g., global policies declared by the supervisor of the federated environment).

In fact, one of the initial works that tried to provide a formal trust management, which could be used in computer science, was presented by Marsh (1994) [9]. Marsh's model is based on social trust properties and provides a motivation for the integration of some of the aspects of trust based on the concepts of sociology and psychology. But these sociological foundations proved that the model is quite complex and can hardly be implemented in electronic communities. Furthermore, the model places emphasis on the experiences of their own bodies, neglecting the views of others, a factor that prevents a network of trust to be built collectively. Later, 2009,

Boursas [8] developed a framework in order to manage federated environments that include a model of trust management that was accepted by the cientific community.

4 Shared Resources and Trusted Based Access Control

In this section we present the research developed around the middleware for grid storage control, its key features and capabilities. We will also present the Trusted Based Access Control algorithm inserted into the framework that allows varying levels of confidence of participants of the Sharing Group. Finally a prototype used to validate the developments carried out in the research model will be presented.

This work built a varying trust model that is the basis of a framework that allows trust based access control to shared resources by different institutions in the financial sector, in a federated environment of centralized management, which are themselves providers of resources storage (when resources are available) while customers of that environment.

4.1 Middleware Storage Resource Manager

The elected grid storage middleware management system was a modified version of the Storage Resource Manager (SRM) [10] implementation. The StoRM (Storage Resource Manager) works in a distributed fashion and with high availability across multiple systems ("Cluster", "GRID"). It allows to manage (share, transfer and access) data storage in an easy, fast and flexible way. The implementation can be distributed over several "datacenters" even when the geographical distance between them is very large. Its main characteristics are flexibility, scalability, high performance, able to run on various types of "filesystems" and independence of the storage manufacturer. It implements the mechanisms of SRM V2.2 interface standard (https://sdm.lbl.gov/srm-wg/). A StoRM application runs on Linux systems on "POSIX filesystems" (ext3, ext4, xfs, etc.), enabling the grid computing to simultaneously provide a direct of multiple systems to a common "filesystem" (e.g. GFS for Linux, HP-UX CFS and Veritas, IBM GPFS, etc.).

For sharing the storage resource data all suppliers and customers in the Sharing Group must have installed SRM in their infrastructure. SRM is used by various academic solutions from simple "grid map files" to Role Based Control Access (RBAC) systems, with Virtual Organizations Management Systems (VOMS) among other proposals [11], despite its breach in access control. This is not the case of the financial sector institutions which have tight security requirements. The implementation of TBAC in SRM and its application to financial sector was a major contribution of this research in order to solve the difficult problem of managing the storage resources in the day-to-day operation of the financial institutions. TBAC is one of the control access models that has large acceptance and works fine when we are dealing with IT communities. Because is a more interesting base to acess control by level of trust in an entity than by the role the person has in his own organization (like RBAC did). It is believed that virtualization can help to significantly improve the application of more stringent security policies and finer granularity with the SRM as a virtual machine that provides basic insulation through Virtual Organizations

(VOs) to share resources and policies to monitor application properties. VO's are the way how an organization is created in the storage grid.

4.2 Algorithm for Trust Variation

The approach presented in this paper sought a quick and cost effective way to supplement the static nature of the federated environments, with a set of new mechanisms for dynamic reliability assessment, without affecting others or compromising the integrity of the federated environment [11]. A notable advantage of the presented solution is to reduce the effect of the arbitrariness of classical evaluation methods of confidence that are usually solely based on the classification of individuals. The proposed approach is based on the evaluation, updating and aggregation of trust by reputation and from past experiences. Three functions were used one to enhance, another to decrement and other neutral for the confidence levels and are used as follows:

$$f(x) = 1 - \frac{1}{2}e^{-\alpha^2(\sum interaction(x))}, \text{ x} \in \{0, 0.5, 1\}, \alpha \in \text{N}. \quad \textbf{(1)}$$

- The function (1) depends on the number of interactions, performs the incremental curve of confidence values that represent reliable behavior (above the axis of 0.5). The asymptotic values increases, but never touch the axis of one (indicating the absolute confidence) such that the confidence value is closer shaft requiring a large set of interactions. This function, on one hand, facilitates the rapid increase of the level of trust from the neutral level of trust for a higher level, but on the other hand, ensures that sufficient positive interactions must be made to achieve Absolute Trust Level.

$$\text{g(x)} = \frac{1}{2}e^{-\alpha^2(\sum interaction(x))}, \text{ x} \in \{0, 0.5, 1\}, \alpha \in \text{N}. \quad \textbf{(2)}$$

- The second function is the inverse function of the previous one. The same principle is defined for all values of trust representing an unreliability. Similarly, the curve rises rapidly to confidence values below 0.5, while rises more slowly when approaching the axis of 0 which represents the Absolute No Trust Level.

$$h(x) = 0, \text{ x} \in \{0, 0.5, 1\}. \quad \textbf{(3)}$$

- The function (3) is a static function, zero, representing that no modifications are required by Neutral Trust Level, which of course can improve or degrade under the other two above functions
- (x) is a set of interactions with a rating level represented by discrete values: x ∈ {0, 0.5, 1}
- The parameter α represents the convergence factor of the curve of the exponential function.

4.3 Implementation of the Prototype

A prototype was implemented on virtual machines (Figure 1) where each machine implements a service and adopts the following authorization flow:

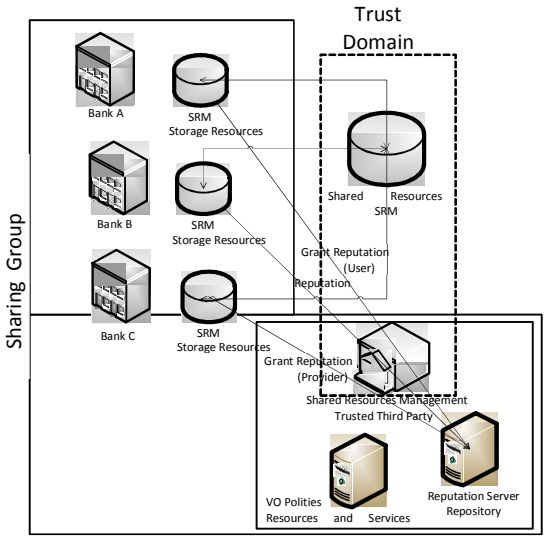

Fig. 1. Auth Flow

1. All the entities are made known to the system. Each one has to send an id and the role (user or provider) for the Services server that recognizes and keeps the records of the entities. If the entity that manages the shared resources confirms which entities are forwarded in accordance with the policies of the VO, and no reputation problems arises, then writes the data and the role of the user.

2. The Bank B, which aims to provide resources, creates and sends the VO, VO-id, the VO policy and public key pair for the server managers of the shared resources, which are stored on the server resource services (SSR).

3. The assets manager notifies the different participants, with user role, which has resources available.

4. The Bank C, needs resources and questions whether the SSR VOs are available in accordance with their technological needs and if the supplier complies with the desired level of trust. If so the SSR registers the request and analyzes the reputation of the Bank C, the requestor.

5. After the validations the SSR delivers the public key of B VO customer to Bank C. Thus the Bank C can enter the VO.

6. If the Bank C complies with the contractual agreement, the index will increment its trust in a reliable server, if some of the clauses violate the agreement its trust will be decremented. In the future, if there are many institutions competing for the same resource, it will be privileged the entity that holds the higher levels of trust.

5 Discussion of Results, their Validation, and Critical View

Given the nature of the research carried out, its assessment should be taken into account in its different dimensions. We considered two dimensions, one Formal and another Functional. Formal assessment was necessary to evaluate the coherence of the research where, in this case, comprised the validation by an expert panel of the acceptance in the sector and by other hand base the mathematical model that was proposed in other derivative models. Concerning the functional assessment we have

to demonstrate that things really work and this was done by testing a prototype implementation and by validating that the grid storage solution may be applied to the financial sector, if the context meets certain requirements that enable the solution acceptance.

5.1 Formal Assessment

With respect to the adequacy of the Middleware Data Storage System Oriented for a Grid implementation to the financial sector, an expert panel was created and it was explained to the panel members the middleware that was developed to become a proof of concept. Unanimously the panel members agreed that the use of virtualization technology would be the way forward for the financial industry and even suggestions were given that provided good contributions to the prototype that was developed.

Regarding the adequacy of the dynamic variation of the trust model used, it was formally presented in the doctoral thesis of Marsh (1994) [9], which has profoundly demonstrated its validity as well as the mathematical representation of the belief model considered. Later, mentioned above, Boursas (2009) [8] with a variation introduced, applied this representation in the framework presented in her doctoral thesis. We proceeded to work in this setting, maintaining and ensuring semantic issues in the Body of Real Numbers, keeping unchanged its initial algorithmic essence.

5.2 Functional Assessment

In order to validate the acceptance by the financial industry an expert panel that studied the issue was created and agreed that the proposal made in this research was a good idea. The expert panel also contributed with suggestions that helped to improve the results of the research, namely in the security middleware component used in.

With respect to the prototype it has to be evaluated according to all the expected benefits that will be learned from its implementation. The performance has no significant impact in the operations. Conversely, the impact of their gaps must also be assessed to foster future improvements and extensions.

6 Conclusions and Further Work

The proposed trust model was developed just to solve an issue of lack of security found in the middleware that was adopted in the framework. The middleware was chosen as a solution to the needs of disk space available for start-up projects in the financial sector. The middleware was the option to provide central management of the Sharing Group. It was found to be suitable for the purpose since no prior knowledge of each element that needs to use the resources available in the group becomes necessary.

The adaptation of the framework applied to address the problem, assessing the suitability of the dynamic trust management model, as well as the formal evaluation of the developed mathematical model, are key components of the research developed. The suitability of the framework presented in this research was also sustained by

leveraging the knowledge base of frameworks previously investigated, developed and applied in doctoral thesis such as Boursas [8], which enabled to justify its application in this context the financial sector.

The mathematical model that was created followed the standards of mathematical inference of parametric models based on the Marsh's theory of belief (2004), thus justifying the application of the framework to the financial sector. The approach presented in this research complements the nature of more traditional systems with a new trust mechanism for evaluating trust dynamics. The proposal for a broader concept of trust, allowing dynamic trust values contributed to the body of knowledge of the specific area Trusted Based Access Control. This approach sought an efficient cooperation between members of the Sharing Group and any external organization without compromising the integrity inside the Sharing Group or affecting any third-party. Basically it allows a trade-off between flexibility, speed and degree of automation in the configuration of cooperation agreements and the level of security and privacy hit. As future work, certain points that can enable to evolve and enrich this research are:

- The research of inter-organizational trust and Service Level – there is a need to investigate this point since inter organizational trust agreements may conflict with organizational security policies, SLAs and restrictions
- Research of other dimensions of trust, aimed at identifying the behavior of other elements of trust. For instance the research of belief in case of an organization is absolute unknown of the group and the new contribution to the model once itself is very flexible.

References

1. Sim, A., Berkeley, L.: Grid, Storage and SRM. (2008)
2. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. Commun. ACM 53, 50-58 (2010)
3. Erdogmus, H.: Cloud Computing: Does Nirvana Hide behind the Nebula? Software, IEEE 26, 4-6 (2009)
4. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud Computing and Grid Computing 360-Degree Compared. 2008 Grid Computing Environments Workshop 1-10 (2008)
5. IBM Cloud Computing und Green IT - Ausbildung 2010. 49, 4887246-4887246 (2010)
6. Andreozzi, S., Forti, A., Magnoni, L., Zappi, R., Pichat, V.B.: Cloud Storage as a new Storage Class : QoS Characterization and Cost Analysis (S3) *. 40127-40127 (2008)
7. Erlenmeyer, M.: Grid and Cloud Computing. (2009)
8. Boursas, L.: Trust-Based Access Control in Federated Environments. vol. 10, (2009)
9. Marsh, S.: Formalising Trust as a Computational Concept. (1994)
10. Alfieri, R., Cecchini, R., Ciaschini, V., dell'Agnello, L., Frohner, Á., Lőrentey, K., Spataro, F.: From gridmap-file to VOMS: managing authorization in a Grid environment. Future Generation Computer Systems 21, 549-558 (2005)
11. Boursas, L., Hegering, H.-G., Hommel, W.: Standards and New Technology for Systems and Virtualization Management: A Report on Svm'08. J. Netw. Syst. Manag. 17, 99-104 (2009)
12. Zissis, Dimitrios; Lekkas, Dimitrios. Addressing cloud computing security issues. Future Generation Computer Systems, 2012, 28.3: 583-592.