International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2019/49572 Volume 6, Issue 1, January – February (2019)

SURVEY ARTICLE

Grid and Cloud Computing Security: A Comparative Survey

Sarra Namane
Networks and Systems Laboratory, Badji Mokhtar University, Annaba, Algeria
naamanesara2005@yahoo.fr

Nacira Ghoualmi
Networks and Systems Laboratory, Badji Mokhtar University, Annaba, Algeria
ghoualmi@yahoo.fr

Published online: 04 January 2019

Abstract – The major purpose of this article is to know the security requirements and their solutions in grid and cloud computing environments. We first focused generally on the security issue in grids as in cloud computing where we examined all the articles proposed in the literature. Then, we classify them according to the treated security issue (authentication, access control, integrity, confidentiality or multiple security issues). A comparative study was carried out between the different techniques presented in each class of each environment. The same classification is done with research articles concerning security issues in cloud computing environment. The study was followed by a comparison between the different proposed techniques for each class in grid computing with those proposed within the same class in cloud. As a result we found that the access control issue is the most considered research area in both grid and cloud computing environments.

Index Terms – Grid Security, Cloud Security, Security Issues, Access Control, Authentication, Integrity, Confidentiality.

1. INTRODUCTION

Despite the several definitions of grids, generally it can be defined as a dynamic and distributed environment which applies multiple resources at the same time in order to solve a single task. Furthermore, grids can be divided into three different types depending on the service they offer. The first type regroups computational grids which offer a great capacity of computing. The second type covers information grids, knowing that the most relevant example of this type is the web. The last type represents data grids. These later offer to users repositories where they can store their data [1].

The national institute of standards and technology defined the cloud computing paradigm as a model that permits access to a distributed network of configurable resources. These ones can be quickly provisioned and unfettered with a minimum management effort [2]. In the other hand, cloud computing can offer different types of services to users: the first service represents the rental of software hosted by the provider; the second one allows users to rent access to a programming platform. Finally, the last service gives users the opportunity to access an infrastructure which put several resources at his disposal such as networking, computing and storage [3]. Both grid and cloud are scalable and multitasking environments. The security of such systems stays one of the most crucial issues. To deal with this dilemma, several efficient mechanisms were proposed in the existing studies regarding grid and cloud computing. Namely, A comparison between the grid and the cloud was presented in [4] the authors first began their comparison with the cloud and grid's basic characteristics and interaction models with clients, resource consumers and providers. Then, they perform an examination of the similarities and dissimilarity in architectural layers and key usage patterns. Wholesale, authors' purpose was highlighting the best practices and technologies which are applicable in both grid and cloud. In [5] authors define the most important security issues that should be taken into consideration for grid and cloud computing. Additionally, they gave some proposals in order to resolve these cited issues. Moreover, they provide a solution for how to exploit a security method used for one technology, to use it in the other sub-adjacent technology.

In this paper, we will compare grid computing and cloud computing taking into account the security issues. Our main objective is to provide a comprehensive and structured overview of security requirements investigated in grid and cloud computing with the proposed solutions to deal with these requirements.

The rest of this paper is organized as the following: the second section gives an overview of grid computing security, the third section presents an overview of cloud computing security, and a comparison between the securities of both technologies is given in the fourth section. Finally, conclusions and future works are given in the last section.

2. GRID COMPUTING SECURITY OVERVIEW

In this section, we will discuss the grid computing security. We will explore different security challenges, classify them

SURVEY ARTICLE

according to security sub-areas (authentication, access control, integrity, confidentiality; …) and do a comparative study between them using the appropriate criteria.

2.1. Access Control

Access control is the security issue that encompasses (Figure 1): identification, authentication and authorization [6]. The last phase is generally called access control because it is at this level that access is really controlled. The identification phase represents the phase in which the user introduces his credentials. The next two phases will be explained in detail in the following.

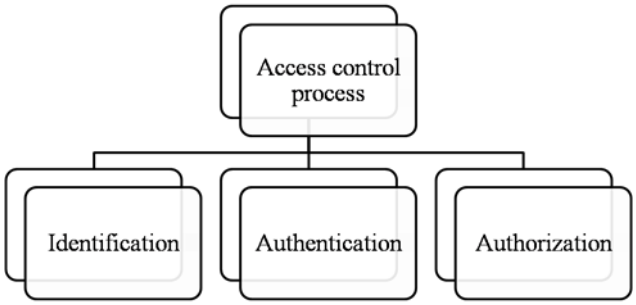

Figure 1 Access Control Process Phases

2.1.1. Authentication

The process of verifying the identity of a user and confirming that it is the one who claims to be. Some researches take into account the authentication issue, in Table 1 we will compare these articles.

An authentication mechanism can use one or more factors of different natures: something that the user cognizes (for example: a password or a PIN), something that the user possesses (for example: an ATM card, a smart card, certificates, tokens), something that represents the user (for example: a biometric feature, such as an eye retina or a fingerprint). Finally, the last factor represents something that the user knows how to do.

The analysis of the proposed mechanisms detailed in table 1, shows that the authors use a single-factor authentication in grid computing environments [11]. Thus, they used a One Time Password which is generally a dual operator factor. The first operator is a fixed user identification code (e.g., user's private key) and the second consists of variable factors (e.g., time, random number, counter value, etc.). In this case, even if an attacker intercepts the password, he won't be able to deploy that password to fake the identity of legitimate users. Hence, it is obvious that the One Time Password can resist password guessing attack. We can also say that the traditional authentication using a static password is not used in grid computing environment because it is no longer considered secure in such environments. Two-factor authentication is also used in [10], authors combined the knowledge factor (password) with the possession factor (CS card) to ensure a strong authentication. In [12] authors proposed a shared key to ensure a mutual authentication in grid computing environment. Besides, authors used a mathematical technique in key sharing which allowed them to propose a new method of encryption and decryption. In [7], authors developed a single sign on infrastructure using identity federation standard. This proposal eliminated the management burden of X.509 certificates by allowing users to deploy only their usual authentication information. Authors used a knowledge factor (password) but the possession factor (X.509 certificate) was replaced by identity federation. In [8], authors proposed an authenticated key agreement protocol based on a signature without certificate. The proposed protocol has the intention of avoiding the issues related to the theft of an encryption key inherited from schemas based on user's identity. In addition, it permits removing one of the negative points of cryptosystems based on PKI in grid (certificate management). In [9], authors considered the key exchange issue; they presented protocols using a secret public key based on the user's identity. These protocols manage the key exchange process between two participants or three and that to ensure a mutual authentication in grid computing environment.

2.1.2. Authorization (Access Control)

It ensures access to resources and services only by legitimate users [13]. Some researches articles have taken into account the access control issue; in Table 2 a brief comparison is done.

The access control mechanisms proposed in grid computing are based on RBAC model [14, 15, 16], ABAC model [17] or others [18]. The RBAC model used the user's roles instead of using user's identity. The ABAC model is based on user's attributes (role, name, email,…), it is a dynamic model and more suitable for dynamic and multi domains environments such us grid computing. Researches about access control models encompasses two types, the first one take into account the access control mechanism on itself, the second one is about how to store security policies efficiently [15,16]. In order to represent and verify security policies, authors in [15] used the Brute Force Approach (BFA). One of the side effects of this approach is the huge repetition caused by the assessment of the entire security policy in order to find the users authorized resources group (UARG). Moreover, the Primitive Clustering Mechanism (PCM) was also proposed in this study. The main idea of this mechanism is to reduce the redundancy by gathering resources sharing the same security policies. However PCM is not able to completely discard the redundancy; despite that it removes the redundancy caused by checking identical security policies, it cannot remove the one caused by the identical security rules checking. To remove this redundancy, authors proposed the Hierarchical Clustering

SURVEY ARTICLE

Mechanism (HCM). This last considers the PCM's parent node's information as a data to generate a hierarchical clustering of the parent nodes themselves depending on their shared security rules. The XACML standard which is a tool for RBAC and ABAC implementations is also a security policy specification language. XACML is used in several researches [16, 17] because it is generic, standard, distributed and powerful. The proposed model in [18] used neither the RBAC model nor the ABAC model. It is a model based on multi agent grid architecture where each element of the grid (user or resource provider) has its own agent. This last receives a set of requirements from user. Then, a set of trustworthy resource providers is selected using the experience of user's agent trust worthy's peers with various resource providers.

Articles	Year	Authentication technique	Advantages	Validation
Qiang and Konstantinov [7]	2010	• Login/Password • SSO • Federated identity • Web service	• Scalability • User don't have to maintain certificates	☒
Chen et Al [8]	2010	• Certificate less-Signature-Based authenticated key agreement protocol	• Secure and efficient	☒
Hedayati et Al [9]	2010	• Identity-based secret public keys	• Resistant to several attacks (password guessing)	☒
Bhowmick et Al [10]	2012	• Login/Password • CS card • RSA signature	• Simple and easy to deploy	☒
Kazemi [11]	2014	• One Time Password (OTP)	• Each user can have its own software model	●
Nandakumar [12]	2014	• Shared Key	• A 128-bit key is difficult to trace • Its three-part formation made it impossible to break	●

☒ Satisfied ● Not Satisfied

Table 1: Comparison of Various Authentication Methods in Grid Computing Environment

Classification Model	Researchers	year	Approaches	Security policy storing	Validation
RBAC	Zhu X.J et Al [14]	2010	• Trust • Task • Condition	●	☒
	Kaiiali et Al. [15]	2010	• BFA • PCM • HCM	☒	☒
	Kaiiali et Al [16]	2013	• GAG • XACML	☒	☒
ABAC	Zhao T. and Shoubin D. [17]	2010	• Trust factor • XACML	●	☒
Others	Gupta V. et Al [18]	2011	• Multi agent architecture • Trust	●	☒

☒ Satisfied ● Not Satisfied

Table 2: Comparison of Various Access Control Methods in Grid Computing Environment

SURVEY ARTICLE

2.2. Integrity

Generally, integrity concerns the protection of content from unauthorized and intentional changes. It can be divided into three groups: data integrity, hardware integrity, and software integrity. The mechanisms used to ensure integrity can be divided into two categories; the first represents preventive mechanisms such as access control. These mechanisms avoid unauthorized changes. The second category concerns defective mechanisms, which consist of detecting changes after the failure of the first type of mechanism. When considering the context of the grid, the data may refer to data resulting from experiments or simulations. This data is usually organized in databases accessible to grid users. In addition, this data may belong to known or anonymous grid users. In both cases, these users want to be assured that the data accessed has not been tampered with by unauthorized hands. So, the integrity of the data in an environment such as grids is the most considered type. Partitioning schemes with dynamic replication are used in [19] in order to guarantee data integrity. Hence, the article's purpose is the development of positioning algorithms to allocate shared replicas. In this way, the communication costs and access latency will be minimized. According to their approach, the authors first introduced a heuristic algorithm to determine the clusters that should host the data parts. Then, they proposed another heuristic algorithm for the allocation of shares in a cluster.

2.3. Confidentiality

Is defined as the process to which unauthorized parties are prevented from obtaining sensitive information [6]. Regarding grid computing, authors in [20] present their strategy reinforced by experimental results. Authors aims in this work, is to emphasize performance improvements. Hence they carried on the implementation of several well-known cryptographic algorithms to the grid infrastructure, such as: symmetric key ciphers, asymmetric key ciphers, hash functions, random number generators, and statistical tests for random number generators.

2.4. Multiples security areas

It encompasses articles which we found hard to fit in one of the above sub-areas of security requirements. In grid computing we found a lot of articles concerning several issues. We will compare them in Table 3.

An access control process starts by an identification phase where user introduces his credentials. The next phase represents the authentication which verifies that user is really who he claims to be. The last phase represents the authorization that permits to know the rights granted to the user.

According to Table 3, we can see that some articles have taken into account the entire access control process (authentication + authorization) [21, 23, 25, 26, 27]. In [21], authors presented an access control mechanism ensuring two security metrics: integrity (hashing) and confidentiality (encryption). In [22], authors have taken into consideration only the authentication phase ensuring confidentiality. Finally, after this analysis, we can notice that access control represents the most targeted security issue by recent researches in grid computing environment.

Researches	Year	Techniques	Security areas	Validation
Sudalai Muthu et Al [21]	2010	• Symmetric Cryptography • Hashing • Information Dispersal algorithm • PKI	• Integrity • Confidentiality • Access control • Authentication	☒
Razieh et Al . [22]	2010	• Mutual authentication • Identity-Based Key Exchange Protocol	• Authentication • Confidentiality	☒
Rajesh et Al [23]	2010	• Secure group communication • SSO • SSL/ TLS • PKI • Group key management	• Authentication • Access control	☒
Ashrafijoo et Al. [24]	2010	• Probability theory • Random process	• Trust • Reputation	☒
Khider H. et Al. [25]	2010	• AA proxy • XACML	• Authentication • Access control	☒

SURVEY ARTICLE

		• SAML		
G. Jaspher Willsie et Al. [26]	2011	• SAML/ XACML • RBAC • Secret string • Biometric data	• Authentication • Access control	●
Anitha Kumari et Al.[27]	2011	• Secure group communication • Key distribution • Vo-Vo communication	• Authentication • Access control	☒

☒ Satisfied ● Not Satisfied

Table 3: Multiple Security Areas Related Works Comparison in Grid Computing Environment

3. CLOUD COMPUTING SECURITY

In this section, we will compare the different works that have been presented to resolve security issue in cloud computing environment. This comparison will be made between contributions of each group of the following classes: authentication, access control (authorization), integrity, confidentiality, and multiple issues. For each class, we will use the same comparison criteria used for the comparison of the articles of this same class in grid computing environment.

3.1. Access control

We have seen in section 2.1 that this issue encompasses three key phases: identification, authentication and authorization.

3.1.1. Authentication

In a cloud environment, authentication is important just as in grids, cloud service users would like to have to deal with authenticated service providers. On the other hand, these providers want to provide their services to authenticated users. Several publications were presented to face the authentication dilemma. In Table 4, we will compare them using the same criteria presented in Table 1.

According to table 4, we can say that actual researches proposed several authentication techniques in cloud computing environment. They were limited to the second phase of the access control process. In [28], authors presented a multi-level authentication using a knowledge factor (password). The levels used are: user level, team level and organization level. In [29], authors proposed a one factor authentication which is a biometric factor (the voice). This last was combined with cryptography and encryption to ensure a strong authentication. In [30], authors presented two factors authentication where the first one is a knowledge factor (password) and the second one represents a possession factor (smartcard). Besides, authors combined these factors with steganography and encryption to have a solid authentication. In [31], authors proposed an authentication mechanism based on two factors where they combined the user password with a know-how factor (predetermined activity on a virtual screen).

In [33], authors also used two-factor authentication. The first is also a password (knowledge factor) but the second is a USB token (possession factor). The authors used a hash function for the password to ensure its security. In addition, they deployed the Diffie-Helleman key exchange algorithm to provide mutual authentication. In [32], authors proposed a three-factor authentication. The first one represents a knowledge factor (password), the second is a possession factor (token) and the third is a biometric factor. One of the positive points of this proposal is that the last biometric factor is multimodal, that is, the authors used several types of biometrics and merged them. Finally, in [34], authors presented an authentication with the Kerberos 5 protocol, which is considered as a third-party authentication. In addition, they used the user's fingerprint (biometric factor) as well as the Diffie-Helleman key exchange protocol associated with the DSA signature (digital signature algorithm) to ensure a strong mutual authentication.

3.1.2. Authorization

In cloud computing environment, several studies have taken the access control issue into consideration; we will compare them in Table 5. According to this comparative study we can say that access control models proposed in cloud computing environment are based on the RBAC model, ABAC model, ARBAC model, or others. Those which are based on the RBAC model [35, 36, 37] use security policies that focus on the role of the user instead of his identity. Those based on the ABAC model [38, 39, 40, 41], use security policies that focus on user attributes and their values (name, email address, role). In a Cloud environment, we notice the use of the new ARBAC model [42, 43, 44], which is the combination of the RBAC and ABAC models, where the role of the user is considered as an attribute but the security policies are based only on it. There is also another type of models named "other" such as [45], which are neither role-based nor attribute-based; they have used other approaches to provide access control. We also note that the use of the RBAC model has always been combined with a new approach. In [35], authors used structured vocabularies and ontologies. In [36], authors used a quantified role, a permission value, and a behavioral value. In

SURVEY ARTICLE

[37], authors deployed a reputation value and a task-based access control model. Access control models based on ABAC used a risk policy or Attribute Based Encryption (ABE). Besides, attribute management can be done by a single authority or by several ones as in [41]. ARBAC-based access control models combined the two models (RBAC and ABAC) to take advantages of the role hierarchy and role conversion function of the RBAC model, as well as the flexibility and dynamicity of the ABAC model at the same time and that in a dynamic environment such as cloud computing. The XACML tool was used for the implementation of access control models based on ABAC [38] or ARBAC [44]. Finally, none of the works listed in Table 5 have taken into consideration the issue of storage and security policies management in a cloud environment.

Articles	Year	Authentication technique	advantages	validation
Dinesha and Agrawal [28]	2012	• Multilevel password	• User has to know the password of all the levels	●
Velciu et Al. [29]	2014	• Voice-based authentication mechanism	• overcomes vulnerabilities of the conventional biometric systems	☒
Sarvabhatla et Al.[30]	2014	• Shared key • Steganography • Password • Smart card	• faster response to users • resistant to all major cryptographic attacks	☒
Singh A. and Chatterjee [31]	2015	• Password • Preset activity on a touch screen	• Does not necessitate additional hardware or software	☒
Mansour A. et Al. [32]	2015	• Password • Token • Multimodal biometrics	• Avoid the disadvantages of one modal biometrics (noise in sensed data, intra-class variations)	●
Al-Attab and Fadewar [33]	2016	• ID/Password • USB Token • Hach function • Mutual authentication • Diffie Helleman key exchange	• Choosing and updating the password freely • USB token blockage freely in case of lost using backup identifier	☒
Talkhaby and Parsamehr [34]	2016	• Kerberos 5 protocol • Diffi-Hellman-DSA key exchange algorithm • User's fingerprint samples • Mutual authentication	• Password guessing attack is solved • Non repudiation ensured using biometrics	☒

☒ Satisfied ● Not Satisfied

Table 4: Comparison of Various Authentication Methods in Cloud Computing Environment

Classification Model	Researchers	year	Approaches	Validation	Security policy storing
RBAC	Sun et Al. [35]	2012	• Semantic access control model • Ontologies • Highly heterogeneous and structured vocabularies	●	●
	Chunlei et Al. [36]	2012	• Quantified role • Permission value • Behavior value	☒	●

SURVEY ARTICLE

	Yue-qin and Yong-sheng [37]	2015	• Task based access control model • Reputation value	☒	●
ABAC	Dos Santos et Al. [38]	2013	• Risk policy • ABAC policy • XACML	☒	●
	Aluvalu and Muddana [39]	2016	• Risk aware access control model • Attribute based encryption (ABE)	☒	●
	Chen et Al. [40]	2016	• Risk policy • ABAC policy	☒	●
	Khan F. et Al. [41]	2016	• Access control based on attribute encryption (ABE) • Multiples attribute authorities	☒	●
ARBAC	Mon and Naing [42]	2011	• Users security levels • Data security levels	●	●
	Varadharaj an et Al.[43]	2015	• Attribute centric • Role centric • Access tree	●	●
	Ayache et Al. [44]	2015	• A middleware • XACML • Acl • Multiple providers • OpenStack	☒	●
Others	Auxilia M. and Raja K.[45]	2014	• Dynamic access control • Semantic context aware access control architecture • Ontologies	☒	●

☒ Satisfied ● Not Satisfied

Table 5: Access Control Related Works Comparison in Cloud Computing Environment

3.2. Integrity

In cloud computing environment, we have not found a lot of recent articles that deal only with the integrity issue. The only work we found was that of [46], where the author proposed a technique guaranteeing the integrity of the hosted data. The author used a read protocol algorithm deployed on the user side to measure the data to be hosted. Once this data is outsourced to the cloud, this same algorithm is used to measure it again. Another algorithm for comparing data at multiple cloud servers was used for each outsourced data. This algorithm manages the data recovery. In the case of cloud server failure, entire data may be affected. In addition, the user cannot predict the integrity of its data as this depends on the service provider, who can hide the loss of some data. To answer this problem, the authors proposed a data management algorithm at the server level and an automatic protocol that allows knowing the entire exchange of data before and after its insertion in multiple cloud servers. This algorithm allows the user to know if changes or deletions have occurred.

3.3. Confidentiality

In cloud computing environment, recent researches were not focused on the confidentiality issue. We found only one article that takes this issue into consideration. In [47], authors proposed a data classification approach based on K-Nearest Neighbours (KNN) to ensure data confidentiality within the cloud. The classification is based on data security needs (two data classes: sensitive and non-sensitive). The sensitive ones are encrypted using the RSA algorithm.

3.4. Multiples security areas

In cloud computing environment, we found several articles that treated multiples security issues at the same time, we attributed them the multiple security areas. As shown in Table 6, the access control issue represents the most targeted security issue for researchers in cloud computing environment. This issue has been treated in different ways,

SURVEY ARTICLE

some works have taken into consideration only its second phase, which is authentication as in [48; 55, 56]. In the first article, authors provided authentication using the RSA signature. In addition, they used a hash function to ensure the integrity and symmetric encryption to guarantee data privacy. In the second article, authors proposed a single-factor authentication technique (identifier/password) in a multi-cloud architecture. Besides, they used data partitioning to ensure their integrity and RSA encryption to ensure confidentiality. In [56], authors proposed a group authentication technique that supports the generation and refresh of keys. In plus, they used double encryption to guarantee data confidentiality. Some articles have taken into account the third phase of access control which is the authorization as in [51], where authors tried to protect sensitive information ensuring their confidentiality by their encryption. Finally, the access control process has also been fully considered (authentication + authorization) in [49; 50; 52; 57]. Integrity and confidentiality in a cloud environment have been addressed together in [53; 54] and this using an encryption algorithm with data partitioning or a third party auditor. In [57], authors addressed all the security issues presented previously. They provided authentication using a One-Time Password (OTP). Besides, the RBAC model has been used to provide access control. Then, they used the MD5 (Message Digest 5) algorithm to ensure data integrity. Finally, the RSA algorithm has been used to ensure data confidentiality.

Researches	Year	Techniques	Security area	Validation
Luo W. and Bai G. [48]	2011	• RSA signature • Hashing function • Symmetric encryption	• Authentication • Integrity • Confidentiality	●
Chugh and Peddoju [49]	2012	• Password • Data encryption • Users and group relationship • Users permission table	• Access control • Confidentiality • Authentication	●
Gonzalez et Al. [50]	2013	• Multi-purpose credential management architecture	• Authentication • Access control	●
Sun et Al. [51]	2013	• Encryption • Sensitive data protection • RBAC	• Access control • Confidentiality	●
Liu et Al. [52]	2013	• CP-ABE • Attribute-based signature (ABS) • XACML	• Authentication • Access control	☒
Abbdal S.H. [53]	2014	• New TPA model • Progressive encryption	• Integrity • Confidentiality	●
Khedar S.V. and Gawande A.D. [54]	2014	• Data partitioning • MD5 • RSA algorithm	• Integrity • Confidentiality	●
Sulochana and Dubey [55]	2015	• RSA encryption • Data partitioning • Multi cloud system	• Authentication • Integrity • Confidentiality	●
Nair N.K. and Navin [56]	2015	• Group authentication mechanism • Generation of key • Dual encryption	• Authentication • Confidentiality	☒

SURVEY ARTICLE

		• Refreshment of key		
Pawar and Sheikh [57]	2016	• OTP • RBAC • MD5 • RSA algorithm	• Authentication • Access control • Integrity • Confidentiality	☒

☒ Satisfied ● Not Satisfied

Table 6: Multiple Security Areas Related Works Comparison in Cloud Computing Environment

4. COMPARISON BETWEEN GRID AND CLOUD COMPUTING SECURITY

In this section, we will compare the different techniques proposed to ensure grid computing security with those proposed in cloud computing environment and that for each of the following security issues: authentication, access control (authorization), integrity, confidentiality, and multiple issues.

4.1. Authentication

According to Table 1 and Table 4, we can notice that the solutions proposed to resolve the authentication issue did not use traditional authentication based on a static password and that in both environments: grid and cloud computing. Single-factor authentication has been used in grids as in the cloud. On the other hand, in a grid environment, authentication was limited to two factors (type: knowledge and possession). But in a Cloud environment, a two-factor authentication was deployed with a know-how factor, and authors proposed a three-factor authentication where they used a knowledge factor, a possession factor, and a biometric factor. Authentication using biometrics has been widely used in a cloud computing environment, unlike work that has been presented in a grid environment. This type of authentication deployed a single type of biometrics (voice, fingerprints) or several types at the same time (multimodal) that will be merged using specific algorithms. In plus, multi-level authentication has been used in a cloud environment but not in a grid environment. We also notice that most methods used for authentication in cloud have always been combined with an additional mechanism such as encryption, hashing, key exchange, ... Finally, we can say that the proposed solutions to resolve the authentication issue in a cloud environment are more sophisticated than those proposed to resolve the same issue in a grid environment. The term "more sophisticated" refers to the additional effort of the user, a greater complexity or the need for more expensive equipment (fusion of biometrics).

4.2. Authorization

The access control models presented in a grid environment were divided according to the model used in three classes, namely: those that use as a basis the RBAC model, those found on the ABAC model and the last class that encompasses models that were based on neither RBAC nor ABAC. On the other hand, in a cloud environment, in addition to the classes mentioned above, there is a new class named ARBAC that combines the two RBAC and ABAC models. This class allows, keeping the importance of the user's role in relation to its identity with the principle of the hierarchy of roles. On the other hand, it allows taking advantage of the ABAC model flexibility in a dynamic and distributed environment such as cloud computing. The access control (authorization) process has two phases: the first one supports the manner in which security policies are stored and managed. The second phase takes into consideration the access control itself, in other words: what are the access rights for a particular user? According to table 2 and table 5, we can say that the works presented in a grid environment to resolve access control issue have taken into account both phases, whereas those presented in a cloud environment did not considered the security policies storage and management issue. There is no work that mentioned the storage mechanisms of security policies, how are they stored? How are they verified? Security policies storing and management represents a very important issue because a cloud environment usually has a great number of users and a significant number of services; if its policies are stored and verified effectively, it will improve the whole process (response time and false positives). According to comparison tables, we can also notice that the XACML tool was used for access control models implementation in grids as in cloud computing and that in the case of RBAC, ABAC or ARBAC models. All RBAC-based models in a cloud environment have combined a new principle (permission value, behavior value, reputation value, encryption, ontologies) with the notion of role, which makes the validation of these models a little more complicated. Furthermore, all ABAC-based models in a cloud environment added a risk policy or attribute encryption to the ABAC policy. Finally, all access control models presented in a grid environment were validated unlike those presented in a cloud environment, this is due to the complexity of the access control techniques proposed in a cloud environment compared to those proposed in a grid environment, and this may have hindered their validation.

4.3. Integrity

The integrity issue was not widely considered in recent work in both grid and cloud environments. We found only one article that dealt with this issue in the grids and only one in cloud computing environment.

SURVEY ARTICLE

4.4. Confidentiality

This security issue has not attracted the attention of researchers and that in both grid and cloud environments. We found only one article that dealt with this issue in the grids and only one in cloud computing environment.

4.5. Multiples security areas

According to Table 3 and Table 6, we can say that access control is the most treated security issue by researchers in both grid and cloud computing environments. Apart from the identification step where the user introduces his credentials, the access control issue can be divided into two important steps, namely: the authentication that verifies that user is the one he claims to be and the second step represents the access control itself (authorization), that is, the process which verifies that the user can access only authorized services. Some grid and cloud articles were limited to the first step (Table 1 and Table 4), others were limited to the second step (Table 2 and Table 5), and finally, there are those considered the entire process. The access control issue is the most important one because if an attacker can gain access to unauthorized services or resources, he can compromise the confidentiality and the integrity of the system.

5. CONCLUSIONS AND FUTURE WORKS

In this article, we made a detailed state of the art on all that has been presented to resolve the security issue in both grid and cloud computing environments. For each environment, we assigned the articles that we found to one of the following classes, depending on the security issue being addressed: authentication, access control (authorization), integrity, and confidentiality. We attributed the articles that dealt with several security issues at the same time to the "multiple issues" class. After this classification, we made a comparison between the proposed articles to solve the same issue in a grid environment using as a basis some important criteria. The same thing was done for articles of each issue in a cloud environment. Finally, a comparison between articles of each issue of grid environment was made with those of the same issue in cloud computing. As a conclusion, we can say that the most important security issue for both environments is access control. This last can be separated into two steps which are authentication and access control itself (authorization). For this last step, it can also be divided into two parts, the first one that takes into account the security policies storage, and management but the second one tries to ensure a fast and efficient access control process. The first phase was widely considered in a grid environment, but in cloud computing, none of the found articles managed this sub problem. In our future work, we will want to center our efforts on the access control issue; first, we want to know if the mechanisms proposed in grids for security policies storing and management can have improvements. Furthermore, we want to explore how security policies are stored in a cloud environment. For the second phase, we will try to propose an efficient access control model.

REFERENCES

[1] Daniel Minoli, a networking approach to grid computing, published by John Wiley & Sons, Inc., Hoboken, New Jersey (2005).

[2] Peter Mell and Tim Grance , The NIST Definition of Cloud Computing, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 (2011).

[3] Harmeet Kaur ,comparison of data security in grid and cloud computing, ijret: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308 (2013).

[4] David Villegas, Ivan Rodero, Liana Fong, Norman Bobroff, Yanbin Liu, Manish Parashar and S. Masoud Sadjadi ,The Role of Grid Computing Technologies in Cloud Computing, Handbook of Cloud Computing pp 183-218 (2010).

[5] David Munoz Sanchez , Comparison between security solutions in Cloud and Grid Computing, Aalto University, T-110.5290 Seminar on Network Security (2010).

[6] Firesmith D., Specifying Reusable Security Requirements, ETH Zurich, Chair of Software Engineering, Vol. 3, No. 1, January-February –(2004).

[7] Weizhong Qiang and Aleksandr Konstantinov; The design and implementation of standards-based Grid single sign-on using federated identity, 2010 12th IEEE International Conference on High Performance Computing and Communications, (2010).

[8] Ming Chen ; Kaigui Wu ; Changze Wu and Zhongfu Wu , Certificateless-Signature-Based Authenticated Key Agreement Protocol for Grid, 2010 Fifth Annual ChinaGrid Conference, DOI: 10.1109/ChinaGrid.2010.52 (2010).

[9] Hedayati M., Kamali S.H. and Shakerian R.,. Using Identity-Based Secret Public Keys Cryptography for Heuristic Security Analyses in Grid Computing, 2010 5th International Symposium on Telecommunication (IST'2010), DOI: 10.1109/ISTEL.2010.5734028

[10] Avijit Bhowmick , Chandan Koner , C T Bhunia "A Novel Time based Authentication Technique for Enhancing Grid Computing Security "; National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC (2012).

[11] A. Kazemi ; "Review of Grid Computing Security and Present a New Authentication Method for Improving Security " , International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 4 ISSN2348 – 4853 (2014).

[12] V. Nandakumar , A novel shared key for security in grid computing, 2014 International Conference on Smart Structures and Systems (ICSSS), DOI: 10.1109/ICSSS.2014.7006190, (2014).

[13] Ivan Stojmenovic, Access Control in Distributed Systems, 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, (2011).

[14] Xiao-jun Zhu; Shi-qin Lv; Xue-li Yu and Guang-Ping Zuo, Dynamic Authorization of Grid Based on Trust Mechanism, 2010 International Symposium on Intelligence Information Processing and Trusted Computing, DOI: 10.1109/IPTC.2010.113 (2010).

[15] Mustafa Kaiiali; Rajeev Wankar; C. R. Rao and Arun Agarwal, New Efficient Tree-Building Algorithms for Creating HCM Decision Tree in a Grid Authorization System, 2010 Second International Conference on Network Applications, Protocols and Services, DOI: 10.1109/NETAPPS.2010.8, (2010).

[16] Kaiiali, M., Wankara, R., Rao, C.R., Agarwal, A., & Buyya R. Grid Authorization Graph. Future Generation Computer Systems 29 1909–1918,(2013).

[17] Tiezhu Zhao and Shoubin Dong, A Trust Aware Grid Access Control Architecture Based on ABAC, 2010 IEEE Fifth International Conference on Networking, Architecture, and Storage, DOI: 10.1109/NAS.2010.18, (2010).

SURVEY ARTICLE

[18] Bhavna Gupta; Harmeet Kaur; Namita and Punam Bedi, Trust Based Access Control for Grid Resources, 2011 International Conference on Communication Systems and Network Technologies, DOI: 10.1109/CSNT.2011.146, (2011)
[19] Tu M., Li P., Yen I.L,. Secure Data Objects Replication in Data Grid; IEEE transactions on dependable and secure computing, vol. 7, no. 1, january-march (2010).
[20] E. Cebuc; A. Suciu; K. Marton; S. Dolha and L. Muresan , Implementation of cryptographic algorithms on a Grid infrastructure, 2010 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR) Year: 2010, Volume: 2 Pages: 1 - 6, DOI: 10.1109/AQTR.2010.5520814, (2010).
[21] T Sudalai Muthu; R. Vadivel; A. Ramesh and G. Vasanth , A novel protocol for secure data storage in Data Grid environment, Trendz in Information Sciences & Computing(TISC2010) Year: 2010 Pages: 125 - 130, DOI: 10.1109/TISC.2010.5714622. (2010).
[22] Razieh Mokhtarnameh; Ho Sin Ban and Nithiapidary Muthuvelu , An empirical study on secure communication for grid information service, 2010 International Conference on Computer Applications and Industrial Electronics Year: 2010, DOI: 10.1109/ICCAIE.2010.5771166.(2010).
[23] Rajesh Ingle and G. Sivakumar , EGSI: TGKA Based Security Architecture for Group Communication in Grid, 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, DOI: 10.1109/CCGRID.2010.28. .(2010).
[24] Ashrafijoo B., Navin A.H., Nia M.M., Abedini S., Azari N., Trust Management in Grid Computing Systems Based on Probability Theory, 201O 2nd International Conference on Education Technology and Computer (ICETC) (2010).
[25] Khider H.; Osman T. and Sherkat N., Attribute-Based Authorization for Grid Computing, 2010 International Conference on Intelligent Systems, Modelling and Simulation, DOI: 10.1109/ISMS.2010.24 (2010).
[26] G. Jaspher Willsie Kathrine; Benson Edwin Raj and E. Kirubakaran , A novel security framework for computational grid, 2011 3rd International Conference on Electronics Computer Technology Year: 2011, Volume: 1 Pages: 103 - 107, DOI: 10.1109/ICECTECH.2011.5941569. (2011).
[27] Anitha Kumari K, Sudha Sadasivam G , Senthil Prabha R, Saranya G, Grid Based Security Framework for Online Trading, 2011 International Conference on Process Automation, Control and Computing (2011)
[28] H. A. Dinesha and V. K. Agrawal , Multi-level authentication technique for accessing cloud services, 2012 International Conference on Computing, Communication and Applications, DOI: 10.1109/ICCCA.2012.6179130, (2012).
[29] Velciu M.A., Patrascu A. and Patriciu V.V.,. Bio-cryptographic authentication in cloud storage sharing; 9th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 15-17, 2014 Timişoara, Romania (2014).
[30] Chandra Sekhar Vorugunti , M. Giri and Mrudula Sarvabhatla (2014), a robust ticket-based mutual authentication scheme for data security in cloud computing, 2014 International Conference on Data Science & Engineering (ICDSE), DOI: 10.1109/ICDSE.2014.6974613, (2014)
[31] Ashish Singh and Kakali Chatterjee, A secure multi-tier authentication scheme in cloud computing environment, 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], DOI: 10.1109/ICCPCT.2015.7159276 (2015).
[32] Mansour A., Sadik M. and Essaid Sabir; Multi-factor Authentication based on Multimodal Biometrics (MFA-MB) for Cloud Computing; 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA) (2015).
[33] Al-Attab B.S.; Fadewar H.S., Authentication Scheme for Insecure Networks in Cloud Computing, 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (2016).
[34] Hamid Roomi Talkhaby and Reza Parsamehr , Cloud computing authentication using biometric-Kerberos scheme based on strong Diffi-Hellman-DSA key exchange, 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), DOI: 10.1109/ICCICCT.2016.7987926, (2016).
[35] Sun L., Wang R., Yong J. and Wu G. (2012), Semantic access control for cloud computing based on e-Healthcare, Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design.
[36] Chunlei W., Zhongwei L. and Xuerong C. (2012), An Access Control Method of Cloud Computing Resources Based on Quantified-Role, 14th International Conference on Communication Technology, IEEE.
[37] Yue-qin F. ET Yong-sheng Z. (2012), Trusted Access Control Model Based on Role and Task in Cloud Computing, 7th International Conference on Information Technology in Medicine and Education .
[38] Dos Santos D. , Westphall C. Et Westphall C. (2013), Risk-based Dynamic Access Control for a Highly Scalable Cloud Federation, SECURWARE 2013: The Seventh International Conference on Emerging Security Information, Systems and Technologies.
[39] Rajani Kanth Aluvalu and Lakshmi Muddana , A dynamic attribute-based risk aware access control model (DA- RAAC) for cloud computing, 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), DOI: 10.1109/ICCIC.2016.7919618, (2016).
[40] Chen A., Xing H. , She K. and Duan G., A Dynamic Risk-based Access Control Model for Cloud Computing, IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (2016).
[41] Khan F., Li H. and Zhang L. (2016), Owner Specified Excessive Access Control for Attribute Based Encryption, DOI 10.1109/ACCESS.2016.2632132, IEEE Access.
[42] Mon E. and Naing T., The privacy-aware access control system using attribute-and role-based access control in private cloud, proceedings of IEEE IC-BNMT (2011).
[43] Vijayaraghavan Varadharajan, Alon Amid, Sudhanshu Rai, Policy Based Role Centric Attribute Based Access Control Model; 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India (2015).
[44] Meryeme Ayache, Mohammed Erradi and Bernd Freisleben, Access Control Policies Enforcement in a Cloud Environment: Openstack; 2015 11th International Conference on Information Assurance and Security (IAS) (2015).
[45] Auxilia M and K. Raja , Dynamic Access Control Model for Cloud Computing, 2014 Sixth International Conference on Advanced Computing (ICoAC), DOI: 10.1109/ICoAC.2014.7229744. (2014).
[46] Dinesh C, (2018). Data Integrity and Dynamic Storage Way in Cloud Computing, https://arxiv.org/abs/1111.2418 (Consulté en 2018)
[47] Munwar Ali Zardari, Low Tang Jung, Nordin Zakaria, K-NN Classifier for Data Confidentiality in Cloud Computing , 2014 International Conference on Computer and Information Sciences (ICCOINS) (2014).
[48] Luo W. and Bai G., (2011). Ensuring The Data Integrity In Cloud Data Storage, 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (2011).
[49] Sonam Chugh, Sateesh Kumar Peddoju, Access Control Based Data Security in Cloud Computing, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2589-2593 (2012).
[50] Nelson Mimura Gonzalez, Marco Antônio Torrez Rojas and Marcos Vinícius Maciel da Silva, A framework for authentication and authorization credentials in cloud computing, 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (2013).
[51] Lili Sun, Hua Wang and Elisa Betino, Role based access control to outsourced data in cloud computing; Proceedings of the Twenty-Fourth

SURVEY ARTICLE

Australasian Database Conference (ADC 2013), Adelaide, Australia (2013).

[52] Xuejiao Liu, Yingjie Xia, Shasha Jiang, Fubiao Xia and Yanbo Wang, Hierarchical Attribute-based Access Control with Authentication for Outsourced Data in Cloud Computing, 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (2013).

[53] Salah H. Abbdal, Hai Jin, Deqing Zou, Ali. A. Yassen, Secure Third Party Auditor for Ensuring Data Integrity in Cloud Storage; IEEE International Conference on Ubiquitous Intelligence and Computing/International Conference on Autonomic and Trusted Computing/International Conference on Scalable Computing and Communications and Its Associated Workshops (2014).

[54] Khedkar S.V. and Gawande A.D.,.Data Partitioning Technique to Improve Cloud Data Storage Security, Swapnil V.Khedkar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3347-3350 (2014).

[55] M Sulochana ,Ojaswani Dubey, Preserving Data Confidentiality using Multi-Cloud Architecture, 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15) (2015).

[56] Nikhitha K. Nair and Navin K. S , An efficient group authentication mechanism supporting key confidentiality, key freshness and key authentication in cloud computing, 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), DOI: 10.1109/ICCPEIC.2015.7259477. (2015).

[57] Prativesh Pawar and Rashid Sheikh, Implementation of Secure Authentication Scheme and Access Control in Cloud Computing; 2016 International Conference on ICT in Business Industry & Government (ICTBIG) (2016).

Authors

Sarra Namane: obtained her Ph.D from Badji Mokhtar University, Annaba, Algeria. She is a member of Computer Networks and Systems Laboratory. Her research interests include networks security, grid computing security and cloud computing security.

Nacira Ghoualmi: is a Professor in Computer Sciences and has been a lecturer in the Department of Computer Science at Badji Mokhtar University, Annaba, Algeria since 1985. She is the Head of the Master and Doctoral option entitled Network and Computer Security, and Head of a Laboratory of Computer Networks and Systems. Her research includes cryptography, networks security, intrusion detection system, wireless networks, distributed multimedia applications, quality of service and optimization in networks, grid computing security, cloud computing security.