Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 8 (2013) pp. 270-278
© MIR Labs, www.mirlabs.net/jias/index.html

A Review of the Risk Factors in Computational Grid

Sara Abdelwahab[1] and Ajith Abraham[2]

[1]Faculty of Computer Science & Information Technology, Sudan University of Science Technology, Khartoum, Sudan
Saraabdelghani@gmail.com

[2]Machine Intelligence Research Labs (MIR Labs), Scientific Network for Innovation and Research Excellence, WA, USA
ajith.abraham@ieee.org

Abstract: **Grid computing is the ultimate solution believed to meet the ever expanding computational needs of organizations. Nevertheless, privacy and integrity is the essential need of a user who runs applications from a remote machine on the grid where resource sharing is the main concern. Local host machine also needs same assurance with respect to client data and the jobs that execute on the host. As a result, data and applications security with the associated risks are the main concerns of grid computing usage. However, analysis of the various possible risks in order to evaluate and develop solution to resolve the risks is needed. Therefore addressing security threats in grid is an issue. The purpose of this paper is to explore the security problems in grid computing and review the risk factors that are highlighted in literature. The paper concludes that; there is need for further taxonomy of risk factors that are associated with computational grid. It also classifies the security risks that affect the grid computing.**

Keywords: Grid computing, risk, security.

I. Introduction

Grid is a term devised in the mid 1990s by Foster [1] -[2], which represents an emerging computing paradigm. Currently, grid has been applied in many applications to solve large-scale scientific and e-commerce problems [3] - [7]. A Grid is a collection of diverse computers and resources spread across several administrative domains with the purpose of resource sharing. However, the rate at which grid and the applications running on the grid are changing have resulted in many complexities that are altering the norms causing insecurity of infrastructure and its applications [8].

Therefore, risk reduction is needed to avoid security breaches. For a grid, to efficiently provide a secure system, many critical security requirements must be provided such as authentication, access control, integrity and confidentiality. The rest of the paper is organized into nine sections as follows: Section 2 demonstrates the computational grid, followed by grid architecture in Section 3. Grid security issues are discussed in Section 4. Network Security Issues are reviewed in Section 5. Related works are highlighted in Section 6. Risk Factors are presented in Section 7. Security Risk Factors Analysis is provided in Section 8 and finally Conclusions are provided in Section 9.

II. Computational Grid

This computing paradigm was introduced in 1998. Its main concern is resource allocation, which includes processing power and storage capacity. This is carried out in a well coordinated manner by virtual organizations (VO) [9]. Grid computing has no formal definition [5], but many researchers [3]-[5], [10]-[12] provide various perspective that try to define grid. A definition by [11] states that "Grid technologies allow large-scale sharing of resources within formal or informal group of companies or individuals which is known as virtual organizations". Czajkowski et al. [12] defines grid system from a different point of view as stated below:

(1) Grid is a system that coordinates resources that are under decentralized control.

(2) Grid is a system that utilizes standard, open, general-purpose protocols and interfaces to address many essential issues such as authentication, authorization and resource access.

(3) Grid is the system that provides reasonable quality of services that relate to many factors such as throughput, security, availability, and response time.

Butt et al. [13] demonstrated how the resources sharing is controlled by the virtual organizations. Primarily, the sharing that concerns the users here is direct access to computers, software, data, and many other resources, that may be of interest to the organizations. The shared resources are highly controlled. The resource providers and consumers define clearly and carefully what is shared, how it is shared and who is authorize to share.

In a computational grid, the grid architecture controls all resource allocation to achieve the required computing power to handle complex tasks on high performance servers. Its aim is to boost resource utilization effectively by making use of underutilized resources [14]. Grid computing is a group of computers connected loosely to perform large computational task that are shared among the connected computers. These computers run jobs in parallel and at the end; they return results to the original computer. The connected computers are nodes in a network that may spread across multiple administrative domains that are geographically distant. Each of the nodes is a distinct system that can perform work and have access to a network. These connected computers are often more cost-effective compared to high-end servers of equal computing power. Computational Grid Offers a framework to exploit resource utilization by enabling a combination of regular and multiple distributed resources to run widespread applications in scientific and business fields [10], [15].

In general, the most important concern of the grid is coordination of resource allocation in dynamically and geographically dispersed organizations that constitute a Virtual Organization (VO). Virtual Organization makes grid applicable extensively in many fields [3]. Likewise, VOs facilitate various groups of individuals or organizations with distinct administrative realms, to share resources in a coordinated way, which helps members to cooperate in performing common jobs [3], [10], [15]. Trust must be established among members to facilitate the construction and operation of VOs. Reputation is one property by which trust can be measured and justified [16].

III. Grid Architecture

Many researchers have categorized the grid component into different classes. Schwiegelshohn et al. [5], classified grid component into three groups. These are hardware resources, domain independent software component, and application software. The domain independent software component is used to control access to resources and virtual organizations (VO). The application software component is dedicated to the needs of different VO within a virtual research environment. It is evident that the implementation of this classification can vary on account of the first and third layers. This is as a result of the large number of diverse resources in the grid coupled with many disciplines that can exploit the computational grid. Grid is a protocol based architecture that determine the fundamental approach employed by VO to control the relationship that exist among partners [3]. Built on top of these protocols are a set of standard protocols, middleware, toolkits, and services that are provided and defined by grids, to help in the construction of VO [6]. Essentially grid system components and procedures can be determined by the system architecture, as well as how these components communicate with each other [3]. The grid architecture can be viewed as five layers, where the components, which share common attributes, form a layer. The description of each of the five layers is provided below [17]. The architecture [3], [6] aims to recognize the requirements for general classes of components, instead of counting all needed protocols which leads to flexible and open architectural structure. Components are arranged in layers [3], [6] as illustrated in Figure 1. The higher layers were built based on capabilities and behaviors of lower layers.

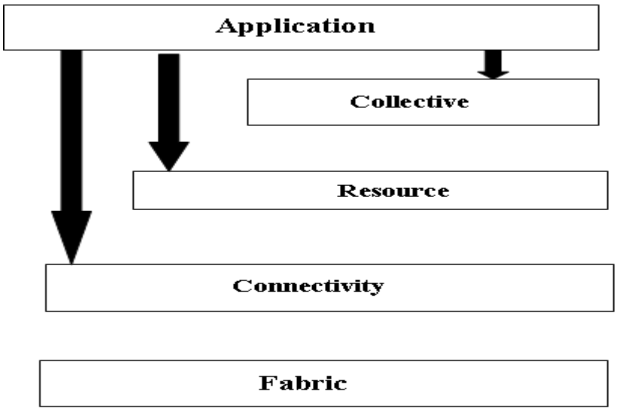

Figure 1. Grid Layered Architecture

Fabric Layer:

As shown in Figure 1, the Grid Fabric layer provides access to the resources that are shared, with the help of Grid protocols. Also, the resources are many and they include storage systems, computational resources, network resources, catalogs and so on. It can also be a logical entity, for instance a distributed file system, computer cluster or distributed computer pool [3], [6].

The connectivity layer:

The layer identifies a core communication and authentication protocols, for easy and secure network transactions [6].

The resource layer:

This layer is concerned mainly on individual resource management by defining protocols for the publication, discovery, negotiation, monitoring, accounting and payment of sharing operations. The Resource Management System (RMS) is used to manage all the resource processes such as allocation, monitoring, and utilization [1].

The collective layer:

The job of this layer is the organization of multiple resources. It is not directly associated with any particular resource. It also contains protocols as well as services that are global. It also captures interactions that exist across resource collections.

The application layer:

This is the layer that the user interacts with. It is the final layer at the top of the Grid architecture. It includes the user applications used within the VO environment. All the layers have well defined protocols that allow access to relevant services. Applications are designed with respect to services that are defined at any layer.

Grid Middleware

This is software that gives an integral part of the grid infrastructure. It is responsible for the formation of layers between programs or tasks that need to be executed on the grid and on the physical machines [5], [18], [19]. Grid Middleware also gives several functions like job scheduling, task parallelizing and even security. Essentially, good middleware is needed to run tasks, which helps to avoid miserable failure of the grid infrastructure.

Globus Toolkit

The Globus Toolkit (GT) was developed in the late 1990s to aid the development of service-oriented distributed computing applications and infrastructures. Core GT components address, basic issues. The issues are concerning security, resource management, resource access, resource discovery, and data movement. These GT components facilitate a wider “Globus ecosystem” of tools and components that interoperate with, core GT functions to give a varying degree of good application-level functionality. These tools have been applied in the development of wide range of both “Grid” infrastructures and distributed applications [20].

Globus Toolkit is a free middleware, and this makes it very popular [1]. Also, many of the defined standards for computational grids have been implemented in the middleware, such as Open Grid Services Architecture (OGSA) and Grid Security Infrastructure (GSI).

IV. Grid Security Issues

In grid environment, resources from many domains are connected together. The concern is to protect data and applications from both unauthorized users and the computer system that runs the applications. Strong authentication measures are required for genuine users and programs. In addition the users problems can be run on local system. Local execution should also be secured from remote systems. Interoperability between various security policies are needed since multiple administrative systems are involved in the grid [8].

As a ground-breaking technology, the Grid causes new security issues, in terms of the requirement for improved intensity and flexibility of security mechanisms. Also, Grid entities must have the capacity to negotiate their security policies. For security policy negotiation to be achieved, effective security policy reconciliation is needed. Even though the use of grid computing has become the best choice for scientific, engineering and commercial applications; there are many challenges computational grid is facing in terms of secure utilities [21]. Managing security in computational grid is a serious issue as a result of the various distributed resources and broad range of users, each with different requirements for the grid, [22], [23]. Therefore, security in the grid is a crucial aspect. Without satisfying it, the grid becomes susceptible to unauthorized users which leads to data tampering, and malicious activities that may likely make grid futile [22].

In grid computing, Virtual Organizations (VOs) enable different groups of organizations and/or individuals, with different administrative domains, to share resources in a controlled manner, which brings the challenge of some security issues. Therefore it is the responsibility of the resource management system [22] to ensure that various resources are handled properly while conforming to the various usage policies.

Due to the nature of the grid computing environments, they are easily targeted by intruders who are looking for potential vulnerabilities to exploit. The intruders impersonate legitimate users, to gain access to resources and act maliciously [24]. Risk is a function of threats exploiting vulnerabilities to cause damage or destroy assets. Thus, threats (actual, conceptual, or inherent) may exist, but if there are no vulnerabilities then there is little or no risk. Equally, you can have vulnerability, but if you have no threat, then you have little or no risk.

Risk is considered as the possibility that a valuated entity will be negatively affected by vulnerability while “vulnerability” is any unsafe situation with potential for harm. In addition, risk is defined as a measure under uncertainty of the severity of a vulnerability [25].

Vulnerability is a weakness or gap in our protection efforts, and risk is the intersection of assets, threats, and vulnerabilities [26]. While a threat is what we’re trying to protect against vulnerabilities. In order to prevent security breaches, grid uses controls such as authentication, single sign on, access control, security policy, and so on to protect resources from various types of threats. Even though with the use of controls the grid is still not fully protected.

Security in general is the degree of resistance to or protection from harm. It applies to any vulnerable and valuable asset. Also, security assurance is to guarantee the integrity and confidentiality of data [27] and authentication to ensure the identity of the user before granting permission to access resources [28].

Traditionally the definition of security is to protect a system from its users or to protect data from compromise. While security in grid computing is to ensure the protection of applications and data from misuse. Therefore, strong and reliable means of authentication is essential for both users and codes. Furthermore, security policies must be put in place to protect local execution from remote systems.

Computational Grid resources can be accessed in many ways, each way having its unique security requirements and implications for both the resource provider and the user. Their design objective is to provide easy and secure access to the diverse resources in the grid. Grid computing is not immune to all classical security vulnerabilities, which includes resources misuse, bypassing controls, data tampering and denial of service.

The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The threat is the possible breach of the Security [29]. The security threats have been classified into four broad categories namely disclosure (unauthorized access), deception (acceptance of false data), disruption (interruption or prevention of correct operation), and usurpation (unauthorized control of some part of a system).

Foster [30] mentioned that, managing transaction in grid have a number of interesting requirements, such as the following:

- *Single sign-on:* This is a situation in which a user should be able to authenticate once and initialize computations that get resources, use the resource and release it, as well as to communicate internally, without the need for re-authentication [30], [31].
- *Delegation:* Is a scenario in which another entity get the right to carry out some action on behalf of a user [7]. The proxy credential creation is a form of delegation; it is important operation in Grid environment. A computation that cut across many resources generates sub computations that may generate requests to other resources and services, and so on. The more these delegated credentials the greater the risk.
- *Authorization and policy:* In a large grid environment, the policies that control resources access cannot be based on individual identity and resources cannot keep track of VO membership and privileges. Instead, the resources and its users have to express policies in terms of other criteria, like group membership.

Authentication, authorization, and policy are among the most challenging issues in Grids. Authentication ensures the identity of the user is who he claims to be, before access to resources is granted [28]. The certificate is a central concept in Grid Security Infrastructure (GSI) authentication. Authorization ensures that authenticated user access only resources his credentials permit. The mandate of conventional security technologies is securing the communications between clients and servers. High-end technologies have been developed to perform these basic tasks of protecting and detecting various forms of attacks [30].

V. Network Security Issues

Threat to the information security poses a security issue by hacking into a computer system or a network. During the design of computer operating systems and application software, there are often some flaws or vulnerabilities. An attacker mostly searches for these flaws to invade the system. Once the attacker is able to locate the flaws, he/she try to gain control of the computer system, and cause damages. The attackers may steal passwords, intercept data, transmit viruses and sometimes destroy whole computer systems. Majority of the successful intrusions result from the internal network and currently most of the intrusion detection systems are difficult to detect attacks from the internal network [32].

As a discipline, network security is one of the most attractive areas of research, where specialist are always on demand especially in the context of the Internet. Attacks and vulnerability of Network and systems respectively form security threats to grid computing where numerous user jobs are processed [33]. A lot of security issues arise when we use networks. Some of the security issues in a network are addressed by [34] such as link attacks, router attacks and sensor network attacks which include Sybil attacks, wormhole, and sinkhole attacks and node hijacking [35]. Sybil attacks [36] is a small number of entities that are faked with multiple identities with the sole intention of compromising the system. In the wormhole attack [35] define it as: “An adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them." It is mentioned in [37] that all computer platforms are vulnerable and subject to network attacks. They provided some security loopholes that include OS blind spots, software bugs, privacy traps and hardware weakness.

VI. Related works

Grid Computing has made considerable attractions in high performance computing field. Although, there are still lots of challenges that have not been tackled. If these challenges are addressed, they may provide seamless computing environment [27]. One of these challenges is risk that arises when using computational grid. Over the past years, there are many researchers such as [7], [13], [22], [34], [28] that focus on security issues in grid computing.

Cody et al. [38] reported the most common vulnerabilities in the three different types of grid system. Each of the three identified grid systems has vulnerabilities common to them. The first type is computational grid, where the grid architecture is responsible for resource allocation to gain computing power to solve complex problems on high performance servers. The most popular vulnerability is node downfall that diminishes the functionality of the system. This could happen when the program contains infinite loops. In the second type of grid system called data grid, the main focus of grid architecture here is on storage and offering access to large amount of data across multiple organization. The possible risk that is associated with this type is overwrite or data corruption that occurs when user override their obtainable space. Denial of Service attack (DoS) is the most widespread attack that threatens the service grid that is considered as the third type of grid system.

Chakrabarti et al. [7] addressed the security issues associated with the grid by classifying the security issues into three levels. The first level according to their taxonomy is host level issue, which includes data protection issue and job starvation. In data protection issue, the main concern is protecting the pre-existing data of the host that is associated with the grid system. While job starvation happens when the resources used by local job are taken away by stranger job scheduled on the host. In the second level (architecture level), the following issues are addressed: policy mapping, denial of services (DoS), resource hacking, information security, authentication, Integrity and confidentiality. The third level is credential level that is categorized into: credential repositories which are responsible for user's credential storage, and the second is credential federation system that support managing credentials among multiple systems and regality.

Chakrabarti [34], investigated a taxonomy of grid security issues that is composed of three categories. The first class addressed the architectural issues, which include data confidentiality, integrity and authentication. While the second category is security issues coupled with infrastructure such as data protection, job starvation, and host availability. The most critical security threats found in the grid infrastructure is malicious service disruption. The third class addressed the security issues that are related to management which include credentials management, and trust management.

Butt et al. [13] mentioned that sharing of resource in grid environment involve execution of unreliable code from arbitrary users, which cause security risks such as securing access to shared resources. In addition, the authors addressed two possible situations that can occur in grid environment and has the power to affect both the program executing in shared resource and the integrity of the resource. In the first scenario, the resource may be malicious that can affect the programs using these resource, or the grid program may be malicious which affect the integrity of resource.

Other works [28], [39] analyzed the security threats in on-demand grid computing. Authors analysis is built on trust relationship between grid actors. They provided three different levels that address the security issues in on-demand computing and each level has possible forms of misuse. Level 1 addresses the threats that arise between users and solution producer. Whereas, level 2 provides the threats done by solution producer to use the resource provider in a bad manner, resulting in possible type of misuse. At the third level resource provider posed threats to users and solution producer caused different type of misuse. Smith et al. [39] addressed the security issues related to on demand grid computing by categorizing it to three types: internal versus external attacks, software attacks, and privilege threats and shared use threats, these threats threaten traditional grid as well.

Kar et al. [40] provided vulnerabilities of grid computing in context of Distributed Denial of Service (DDOS) attack. Using spoofed IP address by attackers make DoS attacks so hard to detect, especially in large distributed system like grid, where it becomes more complicated. He presented four types of grid intrusions: unauthorized access, misuse, grid exploit, and host or network specific attacks. Kussul [41] addressed the most significant security threats for a utility based reputation model in grid. Based on the resource behavior observed in the past, the reputation can be seen as quality and reliability expected from that resource. The authors mentioned nine types of attack according the reputation model: Individual malicious peers, Malicious collectives, Malicious collectives with camouflage, Malicious spies, Sybil attack, Man in the middle attack, Driving down the reputation of a reliable peer, Partially malicious collectives, and Malicious pre-trusted peers. Hassan et al. [42] proposed the problem of Cross Domain Attack (CDA). Authors viewed that when a grid node is compromised it is so difficult to determine it, due to the existence of different administrative domains collaborating with each other, each with multiple nodes. In this case, the attack is likely propagated to another organization's network that is part of the grid network, resulting in cross-domain attack. Services Level Agreements (SLAs) problem was addressed in the works of [43]. Authors mentioned that a resource provider [RP] in grid computing offers resources and services to other Grid users based on agreed service level agreements [SLAs]. The research problem that they have addressed is formulated as follows: the RP is running a risk of violating SLA if one or more of the resources offered to prospective customers will fail when carrying out the tasks.

Three types of failures were addressed by [44]. The process failure, which is expanded into two types that are Process stop failure and a starvation of process failure. Processor failure is the second type of failure which is further categories into a processor crash (Processor stop failure) and a decrease of processor throughput due to burst job (Processor QoS failure) while the third type of failure is Network failure that is classified into a network disconnection and partition (Network disconnection failure) and a decrease of network bandwidth due to communication traffic (Network QoS failure).

VII. Risk Factors

Many risk factors were reported in the literature by [7, 13, 18, 28, 31, 34, 38, 40-42] , [36, 45], [43]. Some of the factors are:

1. Service Level Agreement (SLAs) Violation: SLAs are contracts between service providers and users, specifying acceptable QoS levels. An important challenge in grid environment is how to monitor and enforce SLAs when many users share the same resources, especially because a key part of a grid environment's definition is that it provide nontrivial QoS [46].
2. Node downfall: Running applications on the Grid environment poses significant challenges due to the diverse failures encountered during execution. This could happen when the program executing in grid environment contains infinite loops, which result in diminishing the functionality of the grid.
3. Data overwrite or corruption: This occurs when the user of a data grid system override their obtainable space.
4. Denial of Service attack (DoS): This involves sending large number of packets to a destination or a victim, which is flooded with traffic that is difficult to handle or manage, to prevent legitimate users from accessing information or services. In a Distributed Denial of Service (DDoS) attack the computing power of thousands of compromised machines known as "zombies" are used to a target a victim. Zombies are gathered to send useless service requests, packets at the same time.
5. Quality of Services (QoS) Violation: Where access to certain services is denied, this can be as a result of congestion, delaying or dropping packets or resource hacking.
6. Cross-Domain Attack (CDA): In a single administrative domain networks there is only one security policy, which can be evaluated by the IT security manager. Grid networks are often composed of different administrative domains owned by different organizations dispersed globally. Such networks are referred to as multi-administrative domain networks. Each domain might have its own security policy and may not want to share its security data with less-protected networks, making it more complex to ensure the security of such networks and protecting them from cross-domain attacks.
7. Data protection: The data protection issue is concerned about protecting the pre-existing data of the host that is associated with grid system.
8. Job starvation: Job starvation happens when the resources used by local job are taken away by stranger job scheduled on the host.
9. Policy mapping: Due to the spread of VO across multiple administrative domains with multiple policies, users might be concerned with how to map different policies across the grid. As a result of the grid's heterogeneous nature and its promise of virtualization at the user level, such mapping policies are a very important issue.
10. Resource Failure or Allocation failure: It is a failure if and only if one of the following two conditions is satisfied. 1. Resource stops due to resource crash 2. Availability of resource does not meet the minimum levels of QoS [44].
11. The malicious resource: The resource may be malicious that affect the programs using these resource.
12. The integrity of resource: When a program executed in grid environment is malicious the integrity of resource is affected.
13. Securing access to shared resource: These issues are caused due to incompatibility between the attributes of grid users and conventional users of the computing resources that form the basis of the grid.
14. Exploit the leased nodes to send junk mail and host illegal content for others.
15. Data attacks: Illegal access to or modification of data.
16. Meta data attacks: A malicious program can use operating system commands to acquire information about competitor's work.
17. Compromising the passwords and security system, by exploiting the large computation power that grid provides.
18. Malicious acts such as faking of accounting, billing and malicious service disruption.
19. Store illegal software and data; by utilizing the big store that grid offer [40], [47]
20. Download or steal account information from the resource provider.
21. Hijack other nodes in the system.
22. Stealing the software or the information contained in the database.
23. Altering the software or the information in the database allowing access to unauthorized parties.
24. Stealing the input and output data
25. Modifying the results.
26. Resource attacks or resource hacking: Illegal use of software or physical resources such as CPU cycles and network bandwidth.
27. Credential level issues: Credentials are tickets or tokens used to identify, authorize, or authenticate a user.
28. Man in the middle attack: When a message between other peers is intercepted and modified either by rewriting or changing reputation values, by a malicious peer.

29. Sybil attack: When a large number of malicious peers in the system is launched by an enemy, the peers in the system exchange the role of a resource provider and at each time one of them is scheduled, and then provides malicious service before it is replaced by another peer and be disconnected. In grids, such an attack is scarcely carried out in complete manner because the certificate authority should provide appropriate certificate to merge a resource into the grid system.
30. Privilege threats: Solution producer need more privilege to administer their system and to perform a security audit on all code submitted into the system.
31. Confidentiality: Indicates that all data sent by users should be accessible to only legitimate users.

VIII. Security Risk Factors Analysis

The Grid computing architecture and its platform provide solutions to most of the security threats that are found in grid environment. Access control in grids is concerned with evaluating every request submitted by a VO entity to access a VO resource, in order to determine whether the request should be allowed or denied on the basis of a set of rules stating “who can do what and to whom” which is known as the VO’s security policy [48]. There are many security threats that affect the proper functioning of the grid. They are briefly discussed below.

Threats to Availability indicates the percentage of time, usually on a monthly basis, in which the Grid service supplied by the provider will be available [49]. Distributed denial of service (DDoS) severely threatened the availability of grid resources. Any delay or denial of access to the services in time-critical applications causes heavy losses. This is the reason why the availability of computing resources is important, even if there is no application running. Failure of computing resources as well as power interruption threatens the availability of resource.

Threats to Integrity:

Integrity gives the assurance that the data received are not altered [27]. The physical infrastructure threats are directly related to the as the integrity of the replica files and other stored data is dependent on the integrity of the grid hardware.

Threats to Confidentiality:

Viruses threats, worms, and Trojan horses have serious implications for the grid resources. The extent of their malicious damage has made them more attractive to virus and malicious codes developers. Unauthorized information disclosure without changes in the working state of the system is a serious confidentiality threat this is because it is hard to detect.

Threats to Access Control:

The overall security of the grid is at stake if the authentication and authorization mechanisms are not strong enough to handle the access control properly. This will result in an unauthorized access to the resources.

Threats to Communications:

The threats to data that is being transported across the grid network. The security of the communication mediums exacerbated by the presence of security gaps. These security gaps are introduced in any secure path that passes through one or more points that need to carry out some processing in order to forward data packets. These points include Network Address Translation (NAT) gateways, firewalls, and Wireless Application Protocol (WAP) gateways and many more. Security gaps may surface, mostly in cases where there is nodes and grid resources existing in a local network behind a firewall. Also, the use of passive wire tapping in communication to observe information that is being transmitted is another threat [50].

IX. Conclusions

In order to prevent security breaches, grid use various control measures to protect resources from various type of threats, even though the grid is not still fully protected.

Grid computing presents a number of security challenges that are met by the Globus Toolkit’s Grid Security Infrastructure (GSI). This paper summarized the security challenges and risks inherent in the grid computing environment and we attempted to formulate all the security factors that were reported in the literature.

Many associated risk factors were extracted from those factors. Based on the analysis, a taxonomy of extracted risk factors associated with grid is also provided. Computational grid risks and security issues cannot be ignored. As such, to make customers have confidence in the service provided by the grid, the security of the grid must be highly secured in such a way that usage is not jeopardized. Otherwise, the customers will be worried about the compromise of their valued information. This will make the grid computing service providers to lose a lot of its customers and users.

Table 1: The risk factors and the security threats they influence

Reference	**Risk Factors**	**Security Threats**				
		Availability	**Integrity**	**Confidentiality**	**Access control**	**Communication**
[38]	Node downfall	√				
[7], [28], [34], [38]-[40], [47]	Denial of Service attack (DoS) or Distributed Denial of Service (DDOS) attack	√				
[7], [34]	Job starvation	√				
[34], [44]	QoS Violation or Failure	√	√	√		
[42]	Cross Domain Attack (CDA)	√				
[13], [34], [41]	Malicious acts		√	√		√
[44]	Resource Failure or Allocation failure	√	√			
[7], [28], [34]	Resource attacks or resource hacking	√				
[7],[34]	Credential level issues				√	
[43]	Violation in Service Level Agreement	√	√	√	√	√
[39]	Privilege threats		√	√		
[40]	Unauthorized access,			√		
[28], [40]	Misuse	√	√	√	√	√
[49]	Power interruption	√				
[40]	Network specific attacks					√
[50], [38]	Alteration of grid data		√			

References

[1] I. K. Foster, Carl, "The grid in a nutshell," in *Grid resource management*, ed: Springer, 2004, pp. 3-13.

[2] I. K. Foster, Carl Tuecke, Steven, "The anatomy of the grid: Enabling scalable virtual organizations," *International journal of high performance computing applications,* vol. 15, pp. 200-222, 2001.

[3] I. K. Foster, Carl Nick, Jeffrey M Tuecke, Steven, "The anatomy of the grid," *Berman et al.[2]*, pp. 171-197, 2003b.

[4] I. K. Foster, Carl Nick, Jeffrey M Tuecke, Steven, "The physiology of the grid," *Grid computing: making the global infrastructure a reality*, pp. 217-249, 2003a.

[5] U. B. Schwiegelshohn, Rosa M Bubak, Marian Danelutto, Marco Dustdar, Schahram Gagliardi, Fabrizio Geiger, Alfred Hluchy, Ladislav and D. L. Kranzlmüller, Erwin, "Perspectives on grid computing," *Future Generation Computer Systems,* vol. 26, pp. 1104-1115, 2010.

[6] I. Z. Foster, Yong Raicu, Ioan Lu, Shiyong, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE'08*, 2008, pp. 1-10.

[7] A. D. Chakrabarti, Anish Sengupta, Shubhashis, "Grid computing security: A taxonomy," *Security & Privacy, IEEE,* vol. 6, pp. 44-51, 2008.

[8] M. G. Gupta, Garima, "Security Requirements For Increasing Reliability In Grid Computing," *Journal of Engineering Computers & Applied Sciences,* vol. 2, pp. 5-10, 2013.

[9] H. V. Rosmanith, Jens, "Interactive techniques in grid computing: A survey," *Computing and Informatics*, vol. 27, pp. 199-211, 2012.

[10] H. A. AlHakami, Hamza Alwada'n, Tariq, "COMPARISON BETWEEN CLOUD AND GRID COMPUTING: REVIEW PAPER," 2012.

[11] K. F. Czajkowski, Steven Foster, Ian Kesselman, Carl, "Grid information services for distributed resource sharing," in *High Performance Distributed Computing, 2001. Proceedings. 10th IEEE International Symposium on*, 2001, pp. 181-194.

[12] I. Foster, "What is the grid?-a three point checklist," *GRIDtoday,* vol. 1, 2002.

[13] A. R. A. Butt, Sumalatha Kapadia, Nirav H Figueiredo, Renato J Fortes, José AB, "Grid-computing portals and security issues," *Journal of Parallel and Distributed Computing,* vol. 63, pp. 1006-1014, 2003.

[14] B. B. Jacob, Michael Fukui, Kentaro Trivedi, Nihar, *Introduction to grid computing*, first ed. vol. chapter 2: IBM, International Technical Support Organization, 2005.

[15] I. K. Foster, Carl Nick, Jeffrey M Tuecke, Steven, "Grid services for distributed system integration," *Computer,* vol. 35, pp. 37-46, 2002.

[16] A. E. A. Arenas, Benjamin Silaghi, Gheorghe Cosmin, "Reputation management in collaborative computing systems," *Security and Communication Networks,* vol. 3, pp. 546-564, 2010.

[17] R. A. Alsoghayer, *Risk assessment models for resource failure in grid computing*: University of Leeds, 2011.

[18] R. Bhatia, "Grid Computing and Security Isses," *International Journal of Scientific and Research Publication,* vol. 3, 2013.

[19] *http://www.brighthub.com/environment/green-computing/articles/67604.aspx (assessed on Dec. 2013).*

[20] I. Foster, "Globus toolkit version 4: Software for service-oriented systems," *Journal of computer science and technology,* vol. 21, pp. 513-520, 2006.

[21] Y. G. Demchenko, Leon de Laat, Cees Oudenaarde, Bas, "Web services and grid security vulnerabilities and threats analysis and model," in *Proceedings of the 6th IEEE/ACM international workshop on grid computing*, 2005, pp. 262-267.

[22] K. B. Krauter, Rajkumar Maheswaran, Muthucumaru, "A taxonomy and survey of grid resource management systems for distributed computing," *Software: Practice and Experience,* vol. 32, pp. 135-164, 2002.

[23] V. S. Welch, Frank Foster, Ian Bresnahan, John Czajkowski, Karl Gawor, Jarek Kesselman, Carl Meder, Sam Pearlman, Laura Tuecke, Steven, "Security for grid services," in *High Performance Distributed Computing, 2003. Proceedings. 12th IEEE International Symposium on*, 2003, pp. 48-57.

[24] K. S. Vieira, Alexandre Westphall, Carlos Becker Westphall, Carla Merkle, "Intrusion detection for grid and cloud computing," *It Professional,* vol. 12, pp. 38-43, 2010.

[25] P. K. Marhavilas, D Gemeni, V, "Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009," *Journal of Loss Prevention in the Process Industries,* vol. 24, pp. 477-523, 2011.

[26] D. P. López, Oscar Villalba, Luis Javier García, "DYNAMIC RISK ASSESSMENT IN INFORMATION SYSTEMS: STATE-OF-THE-ART," 2013.

[27] R. K. Selvi and V. Kavitha, "Authentication in Grid Security Infrastructure-Survey," *Procedia Engineering,* vol. 38, pp. 4030-4036, 2012.

[28] M. F. Smith, Thomas Engel, Michael Freisleben, Bernd, "Countering security threats in service-oriented on-demand grid computing using sandboxing and trusted computing techniques," *Journal of Parallel and Distributed Computing,* vol. 66, pp. 1189-1204, 2006a.

[29] ucdavis. (2013, *http://nob.cs.ucdavis.edu/book/book-intro/intro01.pdf*
(accessed on Dec 2013).

[30] I. Foster, "The grid: a new infrastructure for 21st century science," *Phys. Today,* vol. 55, 2002.

[31] I. K. Foster, Carl Nick, Jeffrey M Tuecke, Steven, "A security architecture for computational grids," in *Proceedings of the 5th ACM conference on Computer and communications security*, 1998, pp. 83-92.

[32] M. Z. Xia Hu, Qing Xia, "Research on the Information Security Problems in Cloud Calculation's Environment " *IAES Journal,* vol. 11, p. 7316~7323, December 2013.

[33] S. H. Song, Kai Kwok, Yu-Kwong, "Risk-resilient heuristics and genetic algorithms for security-assured grid job scheduling," *Computers, IEEE Transactions on,* vol. 55, pp. 703-719, 2006.

[34] A. Chakrabarti, "Taxonomy of Grid Security Issues," in *Grid Computing Security*, ed: Springer, 2007, pp. 33-47.

[35] C. W. Karlof, David, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks,* vol. 1, pp. 293-315, 2003.

[36] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*, ed: Springer, 2002, pp. 251-260.

[37] K. T. Hwang, Sapon, "Trust Models and NetShield Architecture for Securing Grid Computing," *Journal of Grid Computing*, 2003.

[38] E. S. Cody, Raj Rao, Raghav H Upadhyaya, Shambhu, "Security in grid computing: A review and synthesis," *Decision Support Systems,* vol. 44, pp. 749-764, 2008.

[39] M. E. Smith, Michael Friese, Thomas Freisleben, Bernd, "Security issues in on-demand grid and cluster computing," in *Cluster Computing and the Grid, 2006. CCGRID 06. Sixth IEEE International Symposium on*, 2006b, pp. 14 pp.-24.

[40] S. S. Kar, Bibhudatta, "An Anamaly Detection System for DDOS attack in Grid Computing," *International Journal of Computer Applications in,* 2009.

[41] O. K. Kussul, Nataliia Skakun, Sergii, "Assessing security threat scenarios for utility-based reputation model in grids," *Computers & Security,* 2013.

[42] S. R. S. Hassan, Maxime Bourgeois, Julien, "Protecting grids from cross-domain attacks using security alert sharing mechanisms," *Future Generation Computer Systems,* 2012.

[43] C. F. Carlsson, Robert, "Risk Assessment in Grid Computing," in *Possibility for Decision,* ed: Springer, 2011, pp. 145-165.

[44] H. M. C. Lee, Kwang Sik Jin, Sung Ho Lee, Dae-Won Lee, Won Gyu Jung, Soon Young Yu, Heon Chang, "A fault tolerance service for QoS in grid computing," in *Computational Science—ICCS 2003,* ed: Springer, 2003, pp. 286-296.

[45] V. V. Mukhin, Artem, "Integrated Safety Mechanisms Based on Security Risks Minimization for the Distributed Computer Systems," 2013.

[46] D. A. Menasce and E. Casalicchio, "QoS in grid computing," *Internet Computing, IEEE,* vol. 8, pp. 85-87, 2004.

[47] M. S. Smith, Matthias Fallenbeck, Niels Dörnemann, Tim Schridde, Christian Freisleben, Bernd, "Secure on-demand grid computing," *Future Generation Computer Systems,* vol. 25, pp. 315-325, 2009.

[48] B. A. Aziz, A. Johnson, Ian Artac, Matej Cernivec, Ales Robinson, P., "Management of security policies in virtual organisations," in *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*, 2010, pp. 1-11.

[49] D. Parrilli, "Legal Issues in Grid and Cloud Computing," in *Grid and Cloud Computing,* K. W. Stanoevska-Slabeva, Thomas Ristol, Santi, Ed., ed: Springer Berlin Heidelberg, 2010, pp. 97-118.

[50] S. Naqvi and M. Riguidel, "Threat model for grid security services," in *Advances in Grid Computing-EGC 2005,* ed: Springer, 2005, pp. 1048-1055.