International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 1, Issue 12, December 2013.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

Contemporary Security Outcomes in Grid Computing Using Globus Toolkit

S. Selvakumar, S. Nandhakumar
Department of Electronics and Communications Engineering
Dhanalakshmi Srinivasan Engineering College, Tamil Nadu, India

ABSTRACT

Grid computing coalesce computer sources from more than a few administrative domains to attain the important objective. In grid computing, the computer systems in the community can work collectively to resolve a large-scale computational problem, therefore functioning as a supercomputer. Grid computing is used to whole tricky or tedious mathematical or scientific calculations. Some research areas were recognized in the lessons of the literature survey where greater finds out about is necessary. The avenues for future research are also mentioned in this paper. Some sorts of grid structures exist presently and the safety wants and options to tackle these wishes for every kind vary. This paper describes an overview of different sorts of the safety troubles in grid computing and additionally presents an effort to define, analyze and grid security troubles for extraordinary kinds of grid setups and protection situation that are confronted by means of grid computing.
Keywords: Grid, Grid Computing, Security outcomes, Globus Toolkit.

1. INTRODUCTION

A computational grid is a hardware and software shape that gives reliable, responsible, power and low-cost get entry to to high-end computational capabilities. Though grid computing has come to be the buzzword in each enterprise and the academic community it is now not a technology which has been developed from scrape. To a sure extent, it is a conglomeration of specific present applied sciences like cluster computing, peer-to-peer (p2p), quit web carrier technologies [1].

Grid computing is a powerful and efficient computational technology which is represented as an superior step for the preceding distributing computing. Alongside with the high network conversation velocity and excessive technical specific machines that are shared nonetheless suffers from some obstacles because of the way and the proportion of the usage of these resources. Grid computing as a new computing era uses the assets of many divided computer systems linked with the aid of a community for fixing such high-quality computation problems by using making use of the underutilized sources or grid shared resources.

Grid computing is rising as a promising science for three reasons: (i) its capability to make extra low-budget utilization of a given amount of computing resources, (ii) as a way to clear up large-scale problems that cannot be solved barring an big quantity of computing power, and (iii) because it proposes that the assets of many computers can be managed and managed closer to a common goal [2]. During the closing decade, extraordinary technology elements like cluster computing and peer-to-peer computing (p2p) have developed from the dispensed and high-performance computing. In cluster computing, exclusive computing resources like machines, server, etc. are linked collectively by using high-speed inter-connects like communications, Gigabit Ethernet, etc. to furnish high performance. Grid computing is a huge region parallel disbursed computing environment the place idle processor cycles and underutilized storage of geographically dispersed sources are utilized in an foremost way which acts as a supercomputer [1].

Security is defined in the resource layer of grid architecture. The aid being used may be precious and the troubles being solved or assignment being attempted sensitive. The protection issues in a grid environment are complex because assets are located in unique administrative domains with each aid achievable having its personal insurance policies and procedures. The security carrier is a processing or communication service furnished via a gadget to supply a precise variety of safety to machine resources. Security offerings implement security plans and are applied by means of the security mechanism. Security issues are difficult by means of the truth that there are exclusive requirements by means of users, aid owners, designers who are growing or adapting their modern-day products and equipment to take proof the grid technological know-how [3].

The relaxation of the paper is equipped as follows: Section 2 describes the problems in grid computing and their concerns. Section three describes a number of authorization structures in grid computing. Section four describes the taxonomy of grid security issues. Section 5 describes the safety authentication schemes in grid computing and Section 6 describes the safety in Globus toolkit. Finally, Section 7 offers the conclusion.

2. GRID COMPUTING ISSUES AND CONCERNS

In Grid computing surroundings in the main three kinds of security problems are challenged: integration with their present systems and technologies, interoperability with diverse service providers like J2EE technology-based systems, .NET primarily based systems, and Linux based structures and trust formation among provider companies and users of Grid environments. There are a large number of technology providers, users, and academicians who are working at exclusive ranges of grid computing stack to make the science usable omnipresent [4].

Application and Data Engineering

Though grid computing is extra than nowadays a technological know-how to abet high presentation computing, most of the early adopters of the grid are customers in the areas where there are massive amounts of statistics and computation concerned like life sciences, finance, automotive and aerospace strength [5].

Grid manageability

The systems have been besotted with issues planning, management, security, and different challenges. To resolve these problems, massive work has been universal out at specific levels. For example, in the shape of shape management systems, job schedulers, methods for implementing security, and so forth [5].

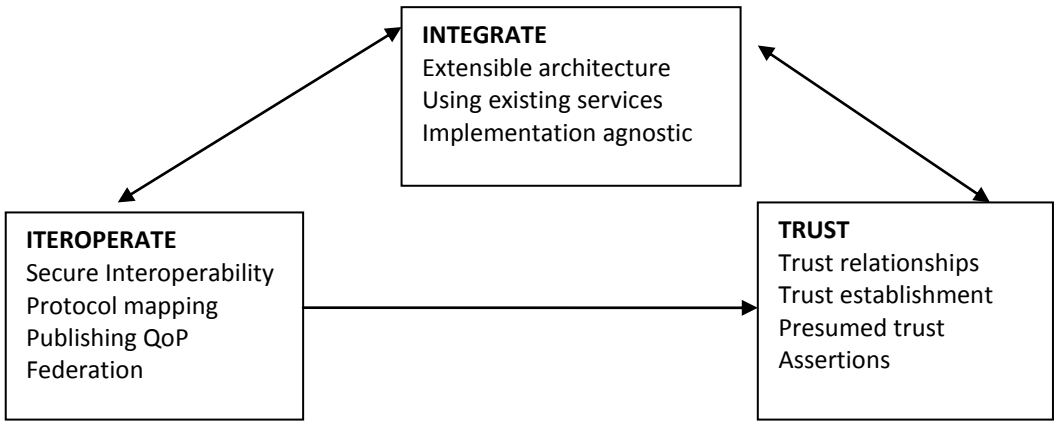

Fig 1: Security challenges in Grid Computing [4]

Grid Licensing Large degree records technological know-how structures are present process transformation modifications in the wake of technological trends and their adoption in scientific and business applications [7]. Grid Security In addition to the ordinary security challenges like authentication, confidentiality, and truth, the grid provides several other single safety challenges [7]. three

3. DIFFERENT AUTHORIZATION SYSTEMS IN GRID COMPUTING

Scalability Push based totally system are normally greater scalable than their pull based totally counterparts. Also, for administrators, it is greater scalable to have the coverage in a centralized device alternatively than in each and each node of the Grid system. In both these counts, each Community Authorization Service (CAS) and Virtual Organization Membership Service (VOMS) score extraordinarily [5]. Security Most of the structures mentioned in these is immune to masquerade assault as they support authentication of several types. Certificates are the most well-known potential of authentication whilst Enterprise Authorization and Licensing System (EALS) supports passwords, certificate, or other sorts of credentials like bio matrices. However, most of the push-based machine is susceptible to DOS assaults as most of them depend on a centralized database for storing insurance policies [6].

Revocation Community Authorization Service and Virtual Organization Membership Service do not have explicit revocation mechanisms. Therefore once adversary positive aspects access to the device then it can access all the sources primarily based on the got credentials [8]. Inter-Operability Another characteristic which is necessary to the Grid authorization structures is how inter-operable the structures are. CAS and privilege and position administration infrastructure standards (PERMIS) have been made to inter-operate the usage of the Security Assistance Management Manual (SAMM) standards. However, if they are to be used extensively in the enterprise's policies want to be exposed as Extensible Access Control Markup Language (XACML) standards and exchanged the use of Security Assertions Markup Language (SAML) [15]. 4

4. TAXONOMY OF GRID SECURITY ISSUES

Architecture Related Issues

These issues tackle the affairs pertaining to the structure of the grid. The customers of the grid are involved about the records powdered by means of the grid and subsequently there is a need to guard

the records confidentiality and integrity as well as the user validation [7]. Architecture level issues may additionally include troubles like facts security, authorization and service degree security which destabilize the entire machine and for this reason an architectural level answer is wished to prevent these [16]. Information security offers with the data change between one of a kind hosts and users. The options to these issues are communication in a invulnerable way, authentication, single sign-on, and delegation. Grid systems require resource particular and gadget unique authorizations. It is important normally for systems where the sources are shared between more than one departments or organizations. The authorization systems are of two types: Virtual corporation degree structures and useful resource degree systems. Virtual organisation degree systems have a centralized authorization system which offers credentials for the customers to get entry to the resources and useful resource level structures allow the customers to get entry to the resources based totally on the credentials introduced by using the users. The grid service level security problems are of two types: QoS Violation Issues and DOS (Denial-of-Service) related issues. The QoS violation issue is about the forced QoS violation with the aid of the adversary through congestion, slowing or losing packets or thru resource hacking. The Denial-of-Service is more unsafe the place the get entry to to a certain carrier is denied. Infrastructure-Related Issues These troubles are associated to the community and host which are observed in the grid infrastructure. Host degree safety problems are individual's troubles that make a host frightened about affiliating itself to the grid system. The problems that are related to the infrastructure may also include records protection, job starvation, and host accessibility [5]. Grid computing infrastructure must address several potentially tricky areas in many tiers of the implementation. These complications arise in the areas of security, aid management, and facts offerings and facts management. The infrastructure-related issues are of two types: host protection troubles and network safety issues. The host level security issues are those problems that make a host complete about affiliating itself into the grid system. The primary sub-issues encompass statistics safety troubles and job starvation [16]. The network safety issues arise in the main due to the heterogeneity and high-speed requirements of many grid applications. Many of the grid community issues are lively areas of lookup and are most developed in labs and not yet commercialized.

Management Related Issues

The third set of problems associated to the management of the grid. Managing pass is without a doubt essential in grid structures due to the fact of the combined nature of the grid frame and applications. Like any disbursed system, managing faith is additionally serious and falls below the purview of management related issues. The one-of-a-kind management issues are credential management, believe administration and monitoring associated problems [16]. Management of credentials is very necessary in grid context as there are multiple one-of-a-kind structures which various credentials to access them. Management of have faith is very difficult in a dynamic grid situation where grid nodes and users join and depart the system. Monitoring of assets consists of one-of-a-kind levels such as collection, processing, transmission, storage and presentation of the facts

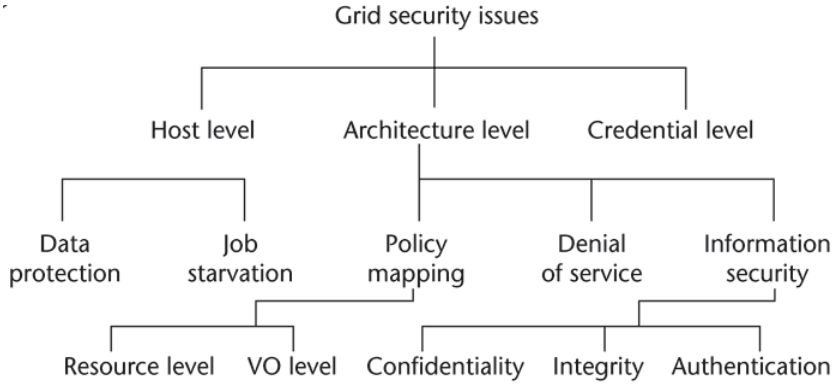

Fig 2: Taxonomy of grid security issues [16]

5. SECURITY AUTHENTICATION SCHEMES IN GRID COMPUTING

The goal of grid computing is to furnish invulnerable grid carrier assets to felony users and consequently the security difficulty will become an vital situation of grid computing. To avoid the illegal users from traveling the grid resources, it must be positive that robust mutual authentication wanted for users and server. To get admission to any aid over any network, the authentication method is imperative at first. Since Grid is network-based architecture, there have to be a robust authentication technique for the sake of protection of resources. Accordingly, the Grid presents open and preferred protocols and utility interfaces to build up all the measures for aid sharing [4]. Authentication is to make certain that the verbal exchange is installed from that entity.

Mutual Authentication Mutual authentication is the key idea of Grid computing model. A person is allowed to access a sure useful resource of Grid environment providing the person is approved entity. On the foundation of the dependence relationship, mutual authentication takes vicinity to keep away from a substitute source to avert [14]. User Proxies A consumer proxy is a convention supervisor system that affords consent to proceed on behalf of a user for a constrained segment of time. User proxy mechanism is a alternative for the user. It has acquired the unique characteristic to forestall repetitive password typing through the consumer for offering its provider [1].

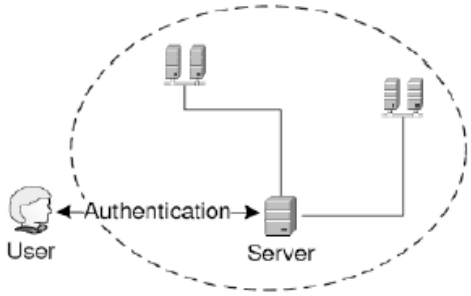

Fig 3: Simple user authentication [13]

Shared secret based authentication

The first mechanism is via sharing a secret. Most of the digital structures additionally work by using the principle of shared secret [14]. One way to implement such a person device would share a password between the authenticator and the user. In this form of the system, the authenticator asks the person for a password which when disclosed will permit the person completely [4].

Public Key Based Authentication

Public-key cryptography is a cryptographic device that desires two-part keys one of which is secret and one of which is public. One key lock or encrypts the plaintext, and the different unlocks or decrypts the ciphertext. Neither key can perform each features [7].
The visibly available encrypting-key is commonly distributed, while the personal decrypting-key is recognised only to the recipient. Messages are encrypted with the receiver's public key and can be decrypted solely with the equivalent non-public key. The keys are related mathematically, however the parameters are chosen so that figuring out the private key from the public key is either not possible or prohibitively high priced [1].

Third Party Authentication Schemes

When a man or woman tries to enter a new country, the immigration branch of the US mandates that the man or woman possesses valid passport and visa to enter the nation. In this case, the

immigration branch does not comprehend the person coming into the country. However, the branch believes some third celebration like the person's personal United States of America issuing the passport and the consulate issuing the visa. This is a traditional case of third-party verification the place the authenticator does now not discover the user, however, makes use of a 0.33 party credential (in this case passport/visa) for authentication purposes. In digital machine also this type of authentication is very famous [10].

6. SECURITY IN GLOBUS TOOLKIT 4 (GT4)

The Globus Toolkit (GT) [8] is an open source middleware developed as a collection of loosely coupled factors and it has end up a facto pioneer of grid development. These aspects composed of services, programming libraries and development equipment designed for building the Grid-based application.GT components fall into 5 extensive domain parts: Security (GSI-Grid Security Infrastructure), Data management, Execution Management, Data and Information Services, and ordinary runtime, fault detection, portability [15]. A simplified view of the most important factors for the Globus toolkit is proven in figure3 [7].

The protection implementations of the Globus Toolkit 4 are discussed below:

Message safety in GT4

GT4 uses two mechanisms to guard the SOAP message being transferred between the exclusive components, viz. Transport-level security and message stage security. Transport-level safety protects the files transferred at the transport layer the use of requirements like Transport Layer Security (TLS). Message stage security, on the other hand, works at a excessive layer and makes use of web offerings primarily based standers like WS-security, WS-secure conversation by protecting the SOAP messages that are being transferred over the transport channel [8].

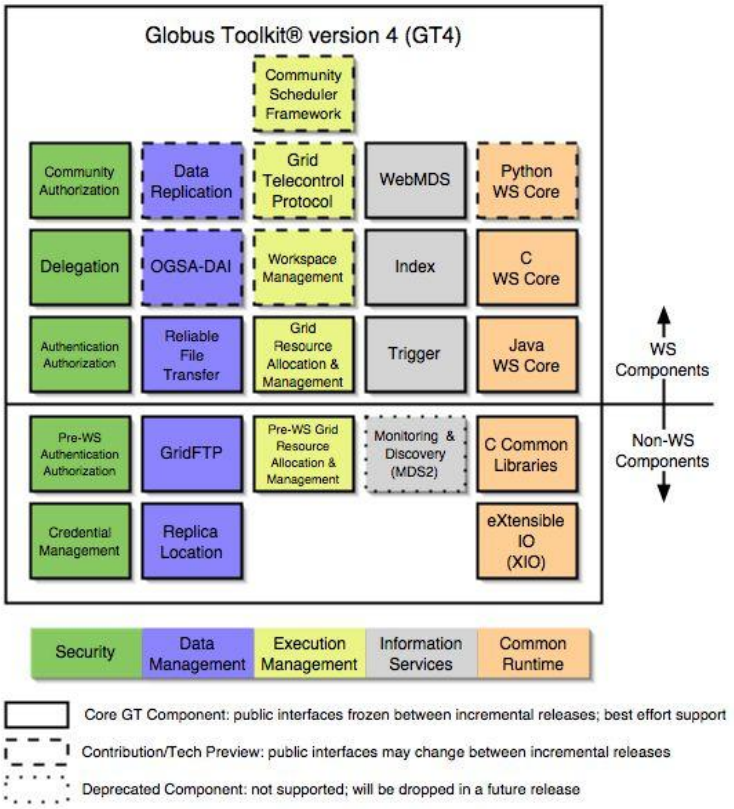

Fig 4: Globus Toolkit version 4.0 [18]

Transport-level protection

Transport stage safety in GT4 is carried out the usage of the transport layer security (TLS) standards. GT4 implements the transport security the use of a secure socket implementation which is able to provide the protection houses [4]. The transport degree safety in GT4 is the default security mechanism used in GT4. The predominant cause for that is the performance overhead delivered by using message-level safety mechanisms [7].

Message-level protection

GT4 additionally makes use of message degree protection (MLS) as an choice to transporting level defense, where encryption, authentication and integrity mechanisms are employed at the message layer, instead than at the transport layer with the aid of means of web service standards like WS-Security and WS-Secure conversation. WS-Security preferred offers mechanisms to provide privacy, authentication, and integrity to the SOAP messages [1].

Message-level and transport level safety processes

When the two mechanisms message stage and transport level safety are compared, two foremost points are wished to be considered. They are end-to-end protection and performance.

End-to-end security

The transport stage security works as a point-to-point mechanism and does not work across a multi-hop link. This is one of the benefits of message stage security. It works across hops and is a whole end-to-end answer [9].

Performance

The overall performance overhead associated with the net services primarily based protection mechanisms is quite significant. The stream-based pipelining is used at every period in order to enhance the overall performance [14].

Delegation in GT4

GT4 helps delegation thru the use of X.509 based totally proxy certificate. Proxy certificates permit the bearers of X.509 certificates to delegate their privileges briefly to every other entity. GT4 supports the delegation to technique through the components: a delegation manufacturing facility service (DFS) and a delegation provider (DS) [8].

GT4 COMPONENTS

The GT4 factors include

- Common runtime
- Security
- Data Management
- Information Services
- Execution Management

Common Runtime

The frequent runtime factors supply a set of integral and equipment libraries which are needed to build all WS and non-WS services [17].

Security

Using the Security components, mounted on the grid safety infrastructure (GSI), it is guaranteed that the communications are securing [6].

Data administration

These components allow getting access to the giant set of facts in a virtual organization.

Information offerings

The Information Services consists of a set of aspects to find out and screen resources in a digital organization. GT4 also consist of a non-WS model for legacy purposes. This factor is deployed and will truly dissolve in future releases of the toolkit.

Execution administration

Execution management materials deal with the initiation, monitoring, management, planning, and coordination of executable programs, generally known as jobs, in a grid.

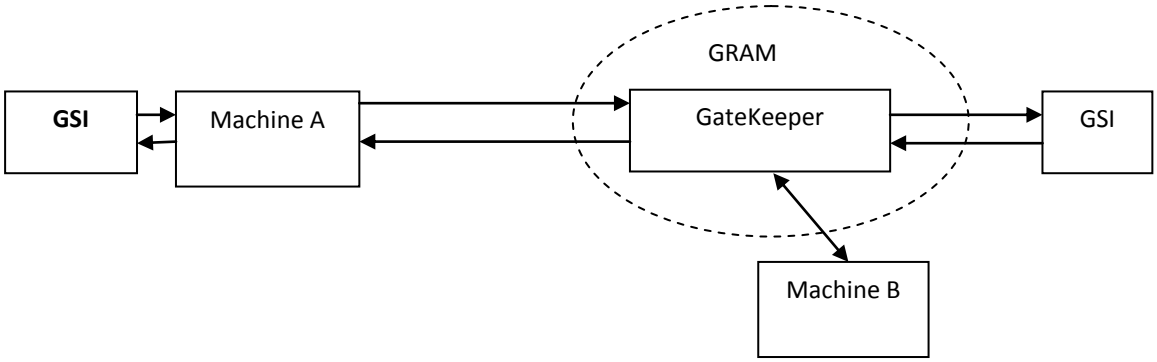

Fig 5.Components of Globus Toolkit [19]

7. CONCLUSION

Grid computing has become a hopeful way for distributed supercomputing from its very beginning and attracts many attentions worldwide. There are numerous ways to entrée the resources of a computational grid and each method is associated with a unique security requirement and it also has implications for both the resource user and the resource provider. Although this computing technology has been accepted worldwide, still it has got a lot of problems mainly regarding with different security issues. The security in grid environment is achieved through the implementation of various security measures such as authentication, authorization and data integrity. This study provides an overview of security issues concerned mainly with authentication and presented various schemes in authentication. Further strong authentication procedures must be developed in future for the sake of security of resources in the grid environment.

REFERENCES

[1] Foster, Ian, Carl Kesselman, and Steven Tuecke. "The anatomy of the grid: Enabling scalable virtual organizations." The International Journal of High Performance Computing Applications 15.3 (2001): 200-222.
[2] Al-Khannak, R., and B. Bitzer. "Modifying modern power systems quality by integrating grid computing technology." (2008).
[3] Selvi, R. Kalai, and V. Kavitha. "Authentication in grid security infrastructure-survey." Procedia engineering 38 (2012): 4030-4036.
[4] Bhowmick, Avijit, and C. T. Bhunia. "Analysing grid security issues and some preliminaryapproaches for secure environment in grid." International Journal of Computer Science and Telecommunications 3.5 (2012).
[5] Geetha, R., and D. Ramyachitra. "Security issues in grid computing." International Conference on Research Trends in Computer Technologies (ICRTCT–2013). 2013.
[6] Chakrabarti, Anirban, Anish Damodaran, and Shubhashis Sengupta. "Grid computing security: A taxonomy." IEEE Security & Privacy 6.1 (2008).
[7] Pérez, José M., et al. "Branch replication scheme: A new model for data replication in large scale data grids." Future Generation Computer Systems 26.1 (2010): 12-20.
[8] Welch, V. "Globus toolkit version 4 grid security infrastructure: A standards perspective." http://www. globus. org/toolkit/docs/4.0/security/GT4-GSI-Overview. pdf (2005).
[9] Saltzer, Jerome H., David P. Reed, and David D. Clark. "End-to-end arguments in system design." ACM Transactions on Computer Systems (TOCS) 2.4 (1984): 277-288.
[10] Atkinson, B. "Web Services Security (WS-Security), Version 1.0 05." http://www-106. ibm. com/developerworks/webservices/library/ws-secure/ (2002).
[11] Buyya, Rajkumar. "Grid computing info centre: frequently asked questions (FAQ)." (2005).
[12] Humphrey, Marty, Mary R. Thompson, and Keith R. Jackson. "Security for grids." Proceedings of the IEEE 93.3 (2005): 644-652.
[13] Lu, Rongxing, et al. "A Simple User Authentication Scheme for Grid Computing." IJ Network Security 7.2 (2008): 202-206.
[14] Hemandezl, V., M. Robles, and M. Talon. "Blast2GO goes grid: developing a grid-enabled prototype for functional genomics analysis." Challenges and Opportunities of Healthgrids: Proceedings of Healthgrid. Vol. 2006. 2006.
[15] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28.3 (2012): 583-592.
[16] Li, Xu, et al. "Securing smart grid: cyber attacks, countermeasures, and challenges." IEEE Communications Magazine 50.8 (2012).
[17] Hashemi, Seyyed Mohsen, and Amid Khatibi Bardsiri. "Cloud computing vs. grid computing." ARPN journal of systems and software 2.5 (2012): 188-194.
[18] Foster, Ian. "Globus toolkit version 4: Software for service-oriented systems." IFIP international conference on network and parallel computing. Springer, Berlin, Heidelberg, 2005.
[19] Foster, Ian. "A globus toolkit primer." 2009-03-01]. http://www. globus. org/toolkit/docs/4.0/key/GT4_ Primer_0. 6. pdf (2005).