ISSN 2047-3338

Analysing Grid Security Issues and Some Preliminary Approaches for Secure Environment in Grid

Avijit Bhowmick[1] and C.T. Bhunia[2]
[1]Department of CSE/IT, Dr. B.C. Roy Engineering College, Jemua Road, Durgapur, West Bengal, India
[2]National Institute of Technology, Yupia, Papum Pare Arunachal Pradesh, India
er.avijit.bhowmick@gmail.com, ctbhunia@vsnl.com

***Abstract*— Grid computing is a wide area parallel distributed computing environment where idle processor cycles and underutilized storages of geographically dispersed resources are utilized optimum way which act as a supercomputer. In this paper we identify and explain the problematic key security issues and propose briefly some novel approaches for solving those existing security related problems lie in Grid computing environment.**

***Index Terms*— Grid Computing, Globus Toolkit, VO and GSI**

I. INTRODUCTION

THE conception of Grid states a potent wide area distributed parallel computing architecture with advanced services which is first presented by Ian Foster et al. [1], [7]. The key characteristic of this architecture is virtual organization (VO) [2], where geographically distributed resources like CPU cycles, storage, software etc. are shared and accessed across the multi administrative domains.

Accessibility of these resources depends on mutual trust and policies among the service providers and users [3].One real life instance of virtual organizations is the Large Hadron Collider (LHC) Computing Grid at CERN [4].

In Grid environment different heterogeneous resources and users are incorporated together without affecting the system.

To access any resource over any network, authentication process is essential at first. Since, Grid is network based architecture, so there must be a strong authentication procedure for the sake of security of resources. Accordingly, the Grid provides open and standard protocols and application interfaces to build up all the measures for resource sharing [3].

Thus the most important feature of the Grid is allowing development of Virtual Organization combining different sites of different administrative domains. Reliability is maintained in Grid network which is another important aspect of data transfer.

In case of failure of allocated task to any specific resource, then automatically resource replacement takes place for carrying out that specific job in Grid environment [1].

Another specific trait of Grid is creating parallel computing environment where large jobs are divided into multiple jobs to the different nodes of Grid [16].

Different types of scheduling algorithm provide precedence of tasks which are submitted by different nodes of Grid.

The indispensable conception behind Grid is: data security, resource administration, data administration and information discovery and controlling [1]. In this paper we will identify the key characteristics of security in Grid computing environment and propose novel approaches for solving those issues.

II. REQUIREMENTS FOR SECURE GRID ENVIRONMENT

In Grid computing environment mainly three types of security issues are faced: integration with present existing systems and technologies, interoperability with dissimilar service providers like J2EE technology based systems, .NET based systems, Linux based systems and trust establishment among service providers and users of Grid environments. These three security challenges are shown in Fig. 2.

To face the above security issues mainly five main areas of security are taken account:

A. Authentication

Authentication is to ensure that the communication is established from that entity which it claims to be (Fig. 3).

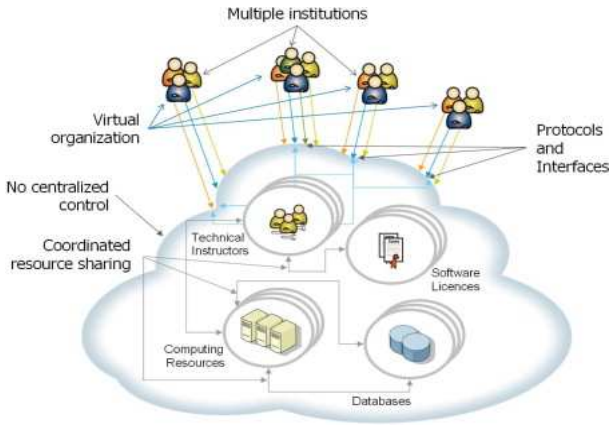

Fig. 1. Ian Fosters model of Grid Computing [6], [7]

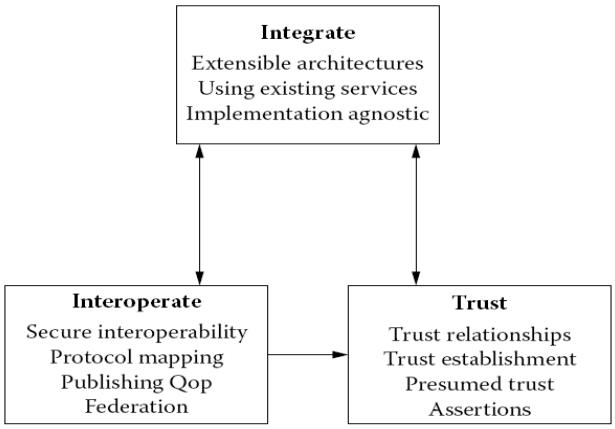

Fig. 2. Security challenges of Grid computing environment

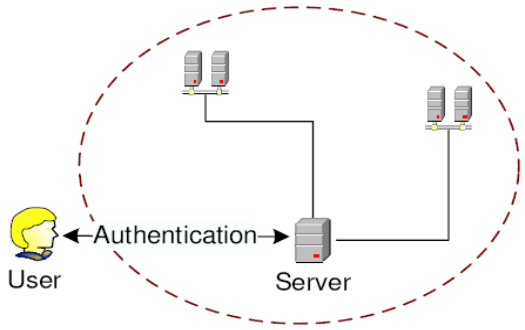

Fig. 3. Simple user Authentication

1) Mutual Authentication: Mutual authentication is the key concept of Grid computing model. A user is allowed to access certain resource of Grid environment provided the user is authorized entity. On the basis of the trust relationship mutual authentication takes place to avoid duplicate source to interfere.

2) Third party certification authority: Certificates are created by some trusted third party certificate authority (CA) and provides to the users which are used for mutual authentication in Grid environment.

3) User Proxies: A user proxy is a session manager process provides consent to proceed on behalf of a user for a limited phase of time. User proxy works as a substitute for the user. It has got the unique feature to prevent repetitive password typing by the user for offering its service.

B. Authorization

Authorization is the process of verification of a user that whether he has got the enough credential to perform the job what he wants to do.

1) Controlling access to the resources: Limited permission is granted to access the resources of Grid so that unauthorized users cannot access those resources.

2) User participation: Only recognised and trusted users are permitted to participate for sharing their valuable specified resource.

C. Confidentiality

Data is protected from unauthorized users otherwise there would be loss of data integrity.

1) Data communication: Data transmission among the participants of Grid should be secured enough to protect data from attack. Since, there is a concept called VO(Virtual Organisation) in Grid environment which consists multiple administrative domain, so proper data communication is vital issue.

2) Security of data: In Grid data crosses the geographical boundary through the formation of VO, so data protection act of different domains should be maintained.

D. Data Integrity

Data should not be changed or altered at any cost without the permitted processes.To enhances the integrity there are used the hash algorithms.

1) Procedure for authentication and authorization: Passwords, keys, certificate credentials etc. are to be changed session to session within the Grid framework.

2) Data and Information backup: In Grid environment distributed storages are utilized for storing valuable data. So, data backup is the important issue for data integrity.

3) DDoS attack: DDoS attack is distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users.

E. Data and information Recovery and Management

Data and information recovery system should be robust enough because data shared among loosely coupled connected resources.

III. GLOBUS TOOLKIT

The Globus Toolkit (GT) [15] is an open source middleware developed as a collection of loosely coupled components and it has become de facto pioneer of grid development. These components compose of services, programming libraries and development tools designed for building Grid-based applications.GT components fall into five wide domain parts: Security (GSI-Grid Security Infrastructure), Data management, Execution Management, Data and Information Services, and regular runtime, fault detection, portability. A simplified view of the main components for the Globus toolkit is shown in Fig 4 [8], [9].

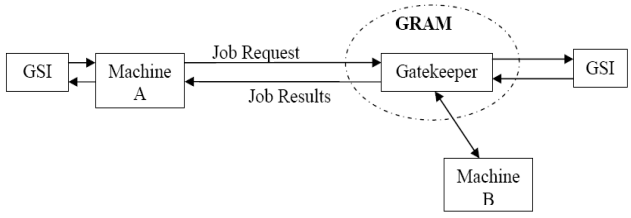

Fig. 4. Components of Globus Toolkit

IV. GRID SECURITY INFRASTRUCTURE(GSI)

The Grid Security Infrastructure is that component of the Globus Toolkit middleware that provides security mechanisms for Grid. GSI conforms to the Generic Security Service Application Programming Interface (GSS-API, RFC 2078/2743) standard. GSI provides libraries and tools for authentication and data protection that use standard X.509 public key certificates [10], public key infrastructure (PKI), the SSL/TLS protocol [11] and X.509 proxy certificates. Grid Security Infrastructure (GSI) is now a Global Grid Forum (GGF) standard. GSI is mainly based on PKI (Public Key Infrastructure) with third party certificate authorities. GSI provides [14]:

- A system based on public key
- Using DC for mutual authentication
- SSO(Single Sign-On)

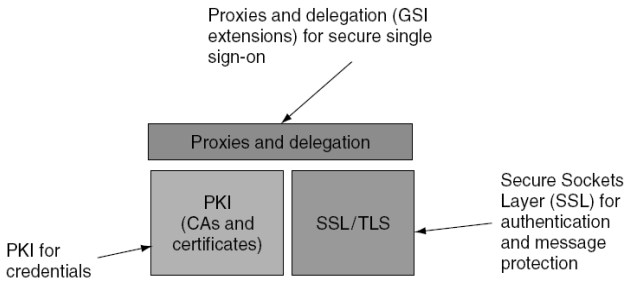

Fig. 5. Grid Security Infrastructure [14]

A. X.509 certificates

For the purpose of authentication GSI uses public keys X.509 certificates and SSL. These Certificates allotted to Grid entities unequivocal names and are signed by Certification Authority [12].

The layout of the certificate used in the Internet is described in RFC-3280 [13].

The certificate is composed of the following essential parts:

- Serial number and the Version of the certificates
- Name of the Issuer
- Validity time period of the certificate
- Public key
- Digital Signature
- Extensions of the certificate
- Subject name and ID

B. X.509 proxy certificates

The proxy certificate is created on the basis of X.509 certificate. This certificate is used for accessing remote resources by the authorised user. Proxy certificates are created dynamically in Grid environment for running abundant processes which is better known as proxy. Different tasks running in Grid of one user use these proxy certificates for authenticating themselves devoid of the interaction of user. Either user or user proxy signs the certificate. At the time of remote proxy creation a completely new public key is generated along with the certificate which is signed by the user X.509 certificate.

C. Single Sign-On (SSO)

Single sign-on (SSO) is a significant aspect as it makes simpler the dexterity of multiple resources of multiple administrative domains; once the user is authenticated, then he can carry out multiple works without further authentication; processes are allowed to proceed on behalf of that authenticated user without any further authentication.

V. ANALYSIS OF SECURITY PROBLEMS IN GRID WITH PROPOSED NOVEL APPROACHES

For the sake of security in Grid computing environment two different types of services are provided: firstly is to assurance the security inside the Grid environment; secondly is to provide warranty the security outside the Grid computing environment.

A. Password Usage

Passwords are used to user's authentication in Grid computing environment. It is generally used to initial Login to the Grid infrastructure i.e. to access private keys in files or My proxy certificates, obtain a Kerberos tickets etc.

Password plays vital role for providing enough security by using robust encryption algorithm for keeping it secured in confidential file. Session based dynamic password is ideal for Grid if it is generated correctly.

B. Confidentiality

By default, data shared among the mutual entities in Grid is not encrypted by GSI. Once the mutual authentication has been established among user and service provider of Grid, no data will be encrypted.So, during data transfer among the Grid nodes are prone to attack.

A robust key exchange algorithm should be imposed for data confidentiality.

C. DDoS Attack

DDoS attack prevention mechanism is not clearly identified in the Globus based system.

Probabilistic approach where previous history and statistics of IP addresses of computer nodes may be used to defend this attack.

D. Trust establishment among different sites of Grid

Developing Virtual Organisation (VO) among the different sites of Grid for the purpose of resource sharing is very significant task.

A server can be established where trustworthy service provider's list should be maintained and before creating any VO, it would be checked first with this server.

VI. CONCLUSIONS

The presented security mechanisms are the essential part of Grid computing system and these security related issues are very important in Grid because of complexity nature of Grid computing environment. In this work we have briefly pointed out the security related challenges of Grid. Among all other issues, authentication is the first step every user performs to access resources and for this process we have presented the concept of dynamic password which is our future direction of work.

REFERENCES

[1] F. Magoules, 1. Pan, Kiat-An Tan and A. Kumar, Introduction to Grid Computing, CRC Press Taylor & Francis Group, ISBN 978-1-4200-7406-2, 2009

[2] I. Foster, C. Kesselman, and S. Teucke, "The anatomy of the Grid: enabling scalable virtual organizations," International Journal of High Performance Computing Applications, vol. 15, no. 3, pp. 200-222, 2001.

[3] I. Foster, What is the Grid? A Three Point Checklist, Argonne National Laboratory & University of Chicago, 2002

[4] What is the Worldwide LHC Computing Grid?, CERN, January 2011, http://lcg.web.cern.ch/lcg/public/overview.htm, retrieved 2012-01-11

[5] C. Ellison: SPKI Requirements, IETF RFC 2692 (1999).

[6] Uwe Schwiegelshohn, Rosa M. Badia, Marian Bubak, Marco Danelutto, SchahramDustdar, Fabrizio Gagliardi, Alfred Geiger, Ladislav Hluchy, Dieter Kranzlmüller, Erwin Laure, Thierry Priol, Alexander Reinefeld, Michael Resch, Andreas Reuter, Otto Rienhoff, Thomas Rüter, Peter Sloot, Domenico Talia, Klaus Ullmann, Ramin Yahyapour, Gabriele von Voigt, Generation Computer Systems, Volume 26, Issue 8, October 2010, Pages 1104-1115

[7] I. Foster, C Kesselman (eds.). The Grid: Blueprint for a Future Computing Infrastructure. Morgan Kaufmann: San Francisco, CA, 1999.

[8] Borja Sotomayor and Lisa Childers,Globus® Toolkit 4: Programming Java Services, Morgan Kaufmann Publishers

[9] Ian Foster. A Globus Toolkit Primer. (Draft). April 26, 2005. http://www.globus.org/toolkit/docs/4.0/key/GT4_Primer_0.6.pdf.

[10] R. Hously, W. Polk, W. Ford and D. Solo, Internet X.509 public key infrastructure certificate and certificate revocation list(CRL) profile, RFC 3280, IETF, April 2003

[11] T. Dierks and C. Allen, The TLS protocol version 1.0, RFC 2246, IETF, 1999.

[12] Welch, V., Siebenlist, F., Foster, I. et al.: Security for Grid Services. In: 12th IEEE Int. Symposium on High Performance Distributed Computing (HPDC'03), IEEE (2003)

[13] Community Authorization Service. http://www-unix.globus.org/toolkit/docs/3.2/cas/index.html

[14] GSI Working Group, http://forge.gridforum.org/projects/gsi-wg.

[15] P. Asadzadeh, R. Buyya, C.Ling Kei, D. Nayar and S.Venugopal, "Global Grids Software Toolkits: A Study of Four Grid Middleware Technologies". High Performance Computing: Paradigm and Infrastructure, Laurence Yang and Minyi Guo(editors).Wiley Press, New Jersey, USA,June 2005.

[16] S. Venugopal. R. Buyya and L. Winton, " A grid Service Broker for Scheduling e-Science Applications on Global Data Grids", Concurrency and Computation: Practice and Experience, Vol. 18 No. 6,pp. 685-699,Wiley Press, New York, USA, May 2006.