GRID THEORY AND GRID SECURITY INFRASTRUCTURE (GSI)

Mr. Arabolu Chandra Sekhar[1], Dr. R. Praveen Sam[2].

[1] Research scholar, Bharathiar University, Tamilnadu, India.
[2] Professor, Dept. of CSE. Andhra Pradesh, India.

ABSRATCT - *In the current geography, grid Computing is scattered worldwide and allows their shared computing power. Grid computing resource enables to access information for world wide web(www)[9], so that these resource include sensors, data storage capacity, visualization tools, processing power and etc. grid combines the thousands of different computers to create a powerful massive computing resource, useful for multiple applications in the areas of science and business. For next generation applications like integrating large scale, heterogeneous and distributed resources[19], grid is the global cyber infrasture. In complex scientific experiments, distributed resources[5] such as applications, data, computational devices and scientific instruments need to be managed within the grid environments. Now, unprecedented interest and importance to a variety of communities are the grid technologies and the associated applications. They enable the exchange, sharing, aggregation and discovery of resources distributed across multiple administrative[4] organizations, domains and enterprises.*

Key Words: *www, storage, environment etc…*

1. INTRODUCTION

In 1998 Foster and Kesselman explained the grid concepts and technologies. In general the grid is a very new discipline, which focuses on and the core components that make up its infrastructure .The associated infrastructures and critical information[10] are not compromised or put at risk by external agents to ensure critical information for IT Securities. The grid is increasingly being taken up and used by all sectors of industry, business, academic and the government as the middleware infrastructure[1] of choice. This means, if it is to be used for critical infrastructures grid security[8] is a aspect of its overall architecture.

2. GRID CHARACTERIZATION

A computational grid is a software and hardware infrastructure that provides consistent, dependable, inexpensive and pervasive access to high-end computational capabilities. A grid is a software framework for layers of services to manage and access the distributed software's and hardware[17] resources or a widely distributed network of high-performance computers, instruments, stored data and collaboration environments shared across institutional boundaries".

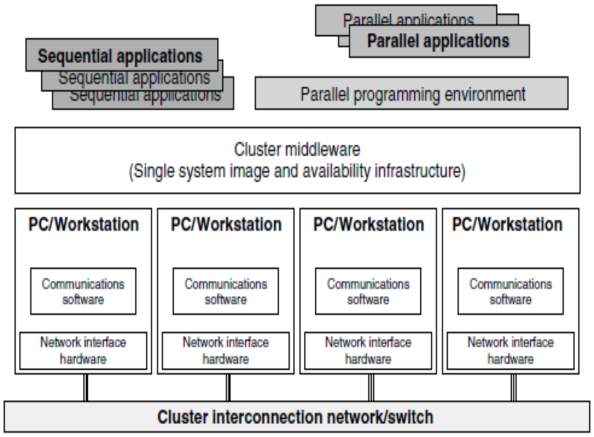

Fig -1: clustered software and hardware of Grid.

Foster suggested that the first part is that there is coordinated sharing resource with no centralized point of control that the reside users within different administrative domains. It is probably the case that, this is not a grid system, if this is not true. The second part is the use of open, standard, general purpose interfaces and protocols. System components will be able to interoperate or communicate, and it is likely that we are dealing with an application specific system, and not the grid, if this is not the case it is unlikely[11]. The final part is that of non trivial delivering qualities of service. Here we are considering, how the components that make up a grid, can be used in a coordinated way to deliver combined services, which are appreciably greater than the sum of the individual components

.

2.1 The Architecture of the Grid

Perhaps the most important standard that has emerged recently is the Open Grid Services Architecture (OGSA), which was developed by the GGF. OGSA is an Informational specification that aims to define a common, standard and open architecture for Grid based applications. The goal of OGSA is to standardize almost all the services that a grid application may use, for example job and resource management services, communications and security.

OGSA specifies a Service-Oriented Architecture (SOA) for the Grid that realizes a model of a computing system as a set of distributed computing patterns realized using web services as the underlying technology. Basically, the OGSA standard defines service interfaces and identifies the protocols for invoking these services.

There are many standards involved in building a service oriented Grid architecture, which form the basic building blocks that allow applications execute service requests.

As the aforementioned list indicates, developing a solid and concrete instantiation of OGSA is currently difficult as there is a moving target – as the choice of which standard or specification will emerge and/or become popular is unknown. This is causing the Grid community a dilemma[7] as to exactly what route to use to develop their middleware.

2.2 Grid Securities

The goals of security are, prevent attackers from violating security policy, detect attackers' violation of security policy and recovery – stop an attack, repair damage and assess , and continue to function correctly

even if the attack succeeds. If someone violates the security policy, then detection occurs. Reported swiftly, when a violation has occurred or is underway and the system must be respond appropriately. The system continues to function correctly, possibly after a period of degraded operation called recovery, such systems are said to be intrusion tolerant. There are three classic security concerns of information deals with data.

1. *Confidentiality*: Data is available to those who only are authorized.
2. *Integrity*: Data is not changed except by controlled processes.
3. *Availability*: Data is available when required.

To be secure, the content of a packet during a communication to prevent malicious users from stealing the data. In order to prevent retrieving secret information from unauthorized users, a common approach is to encrypt data from the sender before sending to the receiver. On the end of receiving, the receiver can extract the original information by decrypting the encrypted text. Hence, confidentiality of data transmission is closely related to application of different encryption algorithms. From modification, integrity is the protection of data by unauthorized users and is not the same as data confidentiality[1]. Data integrity requires that no unauthorized users can change or modify the data concerned.

Other security concerns relate to:

- *Trust*: Computer based systems, people can justify to perform critical functions securely, and on systems to process, communicate and store the sensitive information securely;
- *Reliability*: The system does when and what you want it to;
- *Privacy*: Within certain limits, no one should know who or what you do.

2.3 GSI(Grid Security Infrastructure)

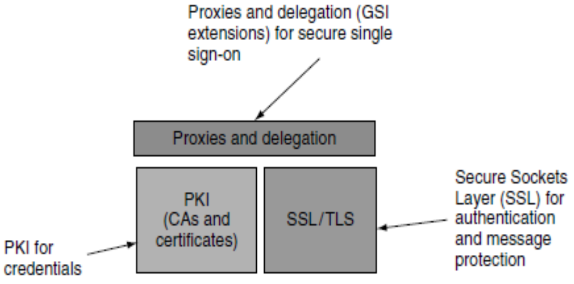
Proxies and delegation (GSI extensions) for secure single sign-on
Proxies and delegation
PKI (CAs and certificates)
SSL/TLS
PKI for credentials
Secure Sockets Layer (SSL) for authentication and message protection

Fig - 1: the Security of grid Infrastructure

Grid Security Infrastructure is a based on a Public Key Infrastructure, with certificate authorities and X.509 certificates. GSI provides:

- A public-key system;
- Mutual authentication through digital certificates;
- Credential delegation and single sign-on.

GSI is a collection of trusted and well known technologies. To provide integrity, privacy and authentication, it can be configured and in addition to that strong authentication is provided with the help of certificates but not all of these features are always needed during communication. A GSI based secure conversation must be at least authenticated and integrity is desirable, but encryption can be disabled and can also be activated, when needed, to ensure privacy. GSI uses X.509 certificates to guarantee[15] strong authentication for mutual authentication through digital certificates. Mutual authentication means that both parties in a secure conversation authenticate the others. When an originator wants to communicate with a remote party, must establish the originator to trust in the remote party and vice versa. Trust means that the each party must trust the certificate of the CA that signed the other's certificate. Otherwise, no trust can exist between the parties.

3. GSI AUTHORISATION MODES

GSI supports few authorization modes on both the client and server.

1. Server-side authorization : The server will decide if it accepts or declines an incoming security request, depending on the authorization mode chosen(i.e. None, Self, Grid map).
2. Client-side authorization: Based on it having the appropriate security credentials, a GSI client, can chose(i.e. None, Self, Host) to use a remote service or not.
3. Mutual authentication: For mutual authentication protocol, the GSI uses the Secure Sockets Layer (SSL). The entities involved must first trust the CAs that signed each other's certificates. Each entity will have a copy of the other CA's certificate, which contains its public keys.

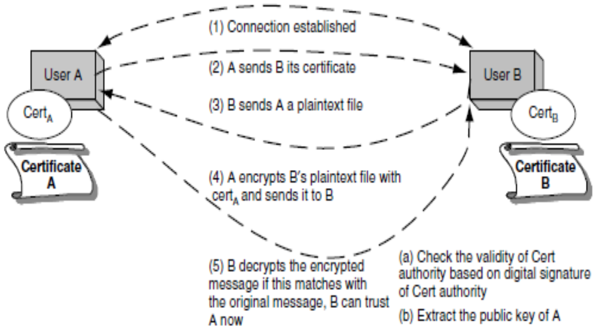
(1) Connection established
(2) A sends B its certificate
(3) B sends A a plaintext file
(4) A encrypts B's plaintext file with $cert_A$ and sends it to B
(5) B decrypts the encrypted message if this matches with the original message, B can trust A now
(a) Check the validity of Cert authority based on digital signature of Cert authority
(b) Extract the public key of A
User A
User B
$Cert_A$
$Cert_B$
Certificate A
Certificate B

Fig -2 : mutual authentication GSI

4. Confidential communication: To establish encrypted communication between entities, GSI is not the default behavior. In GSI, once mutual authentication has occurred, communications occur without the overhead of encryption. When it is needed, confidential communication can be established[20] again.GSI provides communication integrity by default.

5. Securing private keys: In a safe location on a computer's file system, GSI software expects a user's private key to be stored in a file, which is encrypted via a password (also known as a pass phrase). To decrypt the file containing the private key, the user needs to enter the required pass phrase.

6. Delegation and single sign-on: To reduce the number of times, a user must enter the pass phrase for the GSI delegation. Each requiring mutual authentication and a proxy can be created to avoids the need to enter the pass phrase[13] repeatedly, if an activity requires that several resources be used, or a broker or agent is acting upon a user's behalf.

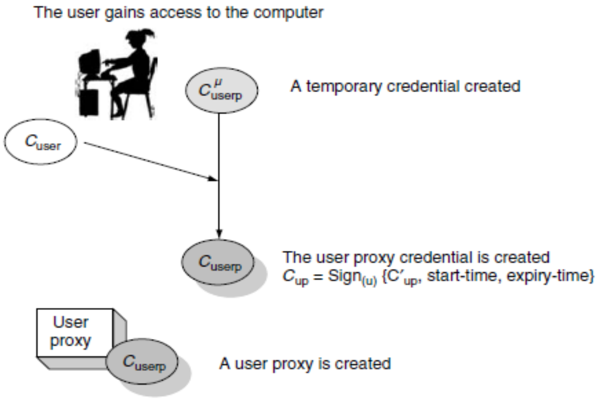
The user gains access to the computer
C^{μ}_{userp}
A temporary credential created
C_{user}
C_{userp}
The user proxy credential is created
$C_{up} = Sign_{(u)} \{C'_{up}$, start-time, expiry-time$\}$
User proxy
C_{userp}
A user proxy is created

Fig -3: User proxy creation

4. CONCLUSION

In the security, Grid can be seen as both technical and sociological in nature, and to address, there are many challenges to ensure that resources and users are secure. To trust, there are many technical challenges are being meet which are being considered and which have still to be addressed. It is crucial[19] that Grid security is watertight and Grid is increasingly used by all sectors and being taken up all sectors of business, academic, industry and the government as the middleware infrastructures of choice.

REFERENCES

[1] Ian Foster and Carl Kesselman (eds), The Grid: Blueprint for a New Computing Infrastructure, 1st edition, Morgan Kaufmann Publishers, San Francisco, USA (1 November 1998), ISBN: 1558604758.
[2] Smarr, L. and Catlett, C., Metacomputing, Communication of the ACM, 35, 1992, pp. 44–52, ISSN: 0001-0782.
[3] De Roure, D., Baker, M.A., Jennings, N. and Shadbolt, N., The Evolution of the Grid, in Grid Computing: Making the Global Infrastructure a Reality, Fran Berman, Anthony J.G. Hey and Geoffrey Fox (eds), pp. 65–100, John Wiley & Sons, Chichester, England (8 April 2003), ISBN: 0470853190.
[4] CCA, http://www.extreme.indiana .edu/ccat/glossary.html.
[5] IPG, http://www.ipg.nasa.gov /ipgflat/aboutipg/glossary.html.
[6] Foster, I., Kesselman, C. and Tuecke, S., The Anatomy of the Grid: Enabling Scalable Virtual Organizations, International Journal of Supercomputer Applications, 15(3), 2001.
[7] Grid Checklist, http://www.gridtoday.com /02/0722/100136.html.
[8] Critical Infrastructure Information Security Act, Bob, Bennett, http://bennett.senate.gov /bennettinthesenate/speeches/2001Sep25_Crit_Infrast_ Inf_Sec.htm.
[9] eLiza Project, http://www.ibm.com/servers /autonomic/.
[10] Bosworth, S. and Kabay, M.E. (eds), Computer Security Handbook, Wiley, US, 4th edition (5 April 2002), ISBN: 0471412589.
[11] Hash Function, http://www.nist.gov/dads/HTML /hash.html.
[12] ITU-T, http://www.itu.int/rec/recommendation.asp? type=folders&lang=e&parent=T-REC-X.509.
[13] GSI Working Group, http://forge.gridforum.org /projects/gsi-wg.
[14] Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S., A Security Architecture for Computational Grids. Proceedings of 5th ACM Conference on Computer and Communications Security Conference, 1998, pp. 83–92.
[15]SSL,http://docs.sun.com/source/816-6156-10/contents.htm.

[16] OpenSSL, http://www.openssl.org/.
[17] Key Conversion, http://www.grid-support.ac.uk/ca/user-documentation/Globus.html.
[18] Novotny, J., Tuecke, S. and Welch, V., An Online Credential Repository for
the Grid: MyProxy, High Performance Distributed Computing, Proceedings of 10th IEEE International Symposium on, Los Alamitos, CA, USA, IEEE Computer Society Press, 2001, pp. 104–111,
http://csdl.computer.org/comp/proceedings/hpdc/2001/1296 /00/12960104abs.htm.
[19]Surridge,M.A Rough Guide to Grid Security, http://www.nesc.ac.uk/technicalpapers, e-Science Technical Report 2002.
[20]gridmapdir patch for Globus, http://www.gridpp.ac.uk/gridmapdir/.

BIOGRAPHIES

ARABOLU CHANDRA SEKHAR was born in Nandyal Town, India, in 1973. He received the M.Sc. degree in Information Technology (IT) from the Kuvempu University, Shimoga, India in 2008, MBA degree in Marketing from Alagappa University, Karaikudi, India in 2008, M.Sc. degree in Psychology from Karnataka State Open University, Chennai, India in 2013 and PG Diploma in Telecommunication from Periyar University, Salem. Now he is pursuing PhD Degree in Computer Science (Cloud Computing) from the Bharathiar University, Coimbatore, India.

He is having total 15 + years of experience in Software Development in Telecommunication and Application Development domain with Microsoft Technologies. Presently working in Tech Mahindra Ltd, Bangalore as Technical Architect. He worked on IVR (Dialogic API) technologies, VOIP, Mobile technologies and Image Processing Tools. He is expertise and having good experience in C, C++, VC++ and COM, C#.Net, ASP.Net, WCF, WPF, Silverlight, AJAX, jQuery, Cloud Computing Technologies such as MS Azure, Amazon Web Services, and Hadoop for Big Data, as well as expertise in OOAD, Design Patterns and UML with Rational Rose. He certified in PRISNCE2 Practitioner (Management) from APMG, UK, TOGAF Certified from Open Group and Microsoft Certified in WPF, WCF, ASP.Net, and VC++.

RACHAPUDI PRAVEEN SAM was born in Kurnool City in 1975. He received the B.Tech degree in Computer Science and Engineering with First Class in 1999 from Sri Krishna Devaraya University, Ananthapur, A.P., India; M.Tech degree Computer Science and Engineering with First Class in 2001 from Madras University, Chennai, T.N., India and was awarded Ph.D. degree in Computer Science and Engineering in 2010 from JNTU University, Ananthapur, A.P., India. His Ph.D. specialization is mobile and Ad Hoc Networks(MANETS). He expertise in Computer Networks and Network Security.

He is having 13 years of teaching experience, presently he is working as a professor of Computer Science and Engineering department for G.Pulla Reddy Engineering College (Autonomous), Kurnool City, India. He has a total of 25 publications out of which 13 papers in International and National Journals and 12 papers in National and International Conferences. He is a member of various professional bodies like ISTE, IE, CSI, IAENG, CSTA, and IACSIT.

He received Minor Research Project titled "Developing Disaster Management Applications using Mobile Ad Hoc Network Tested" sanctioned by UGC for a period of 2 years in March 2014.