iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Increasing Reliability in Grid Computing By Layered Security Architecture

AdeshPatel[1], D.Sai Kumar[2]
[1,2]*Assistant Professor, Lords Institute of Engg.& Technology, Hyderabad*

Abstract- In this paper we described four layer architecture of Grid Computing System, analyzes security requirements and problems existing in Grid Computing System. This paper presents a new approach of five layer security architecture of Grid Computing System; Grid computing is believed to be ultimate solution for meeting the increasing computation needs of organizations. At present the major focus is on load balancing in Grid computing in order to improve the performance of grid. However, the user running an application on a remote machine in the grid-computing network requires assurance about privacy and integrity of his data. Similarly the local host requires a similar assurance regarding the client data and processes that run on the host. So the focus must be on the security of data and applications along with the high performance of the grid. The purpose of this paper is to explore the security problems in grid computing and the steps that can be taken to solve them.
Keywords: Grid computing, Resources, Security, Interoperability, Grid workflows.

I. INTRODUCTION

A Grid is a collection of heterogeneous computers and resources spread across multiple administrative domains with the intent of providing users easy access to these resources. In simple term, it is the pooling of computing resources. However, the inherent scale, heterogeneity, dynamism and non-determinism of grids and grid applications have resulted in complexities that are quickly breaking current paradigms, making both the infrastructure and the applications insecure. So there is a need for a fundamental change in how grids and grid applications are developed and managed [2]. Currently, grid-related research is focused mostly on delivering the best available performance, including questions of load balancing, on the questions of resource discovery, grid-enabling existing legacy software and the likes. At the same time the question of grid security, while recognized as an important issue, remains somewhat on the backburner. There is a reasonable explanation for this situation. Security matters only if the computational infrastructure of the grid works well and effectively. Until the desired work is correctly distributed to the appropriate resources on the grid and the problem is efficiently solved and the results returned to the originator, there is no real reason to worry if the whole process can be done in a secure fashion [4]. So there is a need to make a model of the grid that delivers high performance as well also concerns the security of data and applications. The user running an application on a remote machine in the grid-computing network requires assurance of the machine retaining its integrity, to ensure that proprietary application remains safe. The local host requires a similar assurance regarding the client data and processes that run on the host. In this paper we discuss the security requirements in grid environment and the steps to fulfill them.

II. GRID COMPUTING

A grid can be defined as a large-scale geographically distributed hardware and software infra-structure composed of heterogeneous networked resources owned and shared by multiple administrative organizations which are coordinated to provide transparent, dependable, pervasive and consistent computing support to a wide range of applications. These applications can perform distributed computing, high throughput computing, on-demand computing, data-intensive computing, collaborative computing or multimedia computing [1]. Ian Foster [5] made a three point checklist to define What a Grid is? According to him-

A Grid integrates and coordinates resources and users that live within different control domains and addresses the issues of security, policy, payment, membership.

A Grid is built from multi-purpose protocols and interfaces that address such fundamental issues as authentication, authorization, resource discovery, and resource access.

A Grid allows its constituent resources to be used in a coordinated fashion to deliver various qualities of service, relating for example to response time, throughput, availability, and security, and/or co-allocation of multiple resource types to meet complex

user demands, so that the utility of the combined system is significantly greater than that of the sum of its parts.

III. GRID SECURITY ISSUES

Security is one of the main issues that usually arise when considering a grid computing environment. While the safeguards of a traditional system aim at protecting the system and data from its users, the security orientation of grid systems need to go a step ahead and also protect applications and data from the system where the computation takes place. Therefore, some unique requirements and challenges are to be counted while adopting a security infrastructure in a grid computing system. In this section, we point out the Technical and Non-technical security requirements that should be in place in grid computing systems [3] [4].

A. Technical Issues

Logging information- There must be a proper record of log-in and log-out information of every event on grid.

Single sign-on- A user should be able to authenticate once and initiate computations without further authentication of the user.

Protection of credentials- User credentials such as passwords, private keys etc. must be protected.

Uniform credentials/certification infrastructure- There should be a standard such as X.509v3 for encoding credentials for security principals.

Delegation of access rights: Providing mechanisms to allow delegation of access rights from requesters to services while ensuring that the access rights delegated are restricted to the tasks intended to be performed within policy restrictions.

Message integrity: Ensuring that unauthorized changes made to message content or data can be detected at the recipient end.

Privacy: Allowing both a service requester and a service provider to define and enforce privacy policies.

Interoperability with local security solutions- Security policy for inter-domain access must be in accordance with security policy for local resources. There should not be any need to modify local security policy according to inter-domain security policy.

Support for secure group communication- A computation can comprise a number of processes that will need to coordinate their activities as a group. The composition of a process group can and will change during the lifetime of a computation. Therefore, support is needed for secure authenticated communication for dynamic groups.

Support for multiple implementations- The security policy should not dictate a specific implementation technology rather it should be possible to implement the security policy with a range of security technologies.

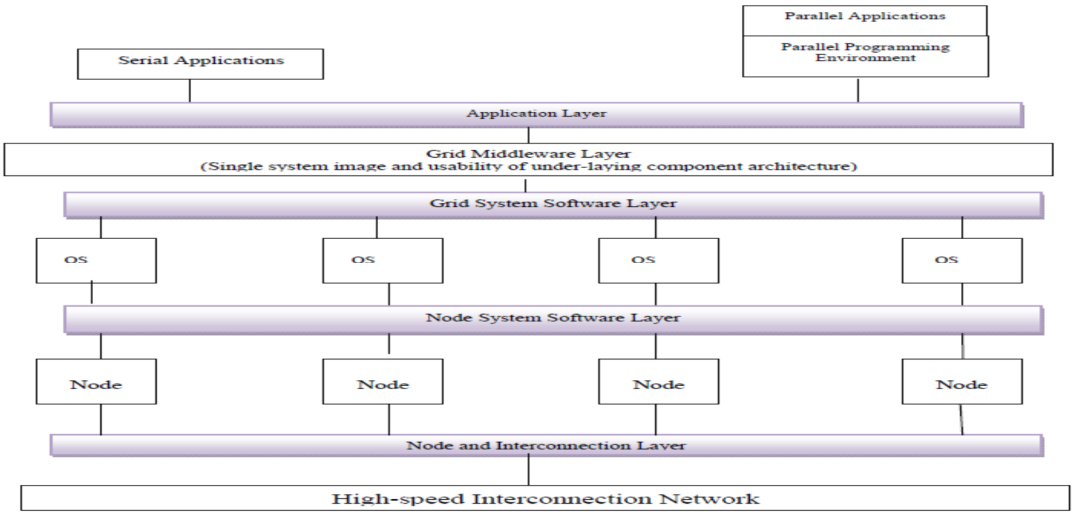


Fig.1 Four layer architecture of Grid Computing System

IV. FIVE LAYER SECURITY ARCHITECTURE OF GRID COMPUTING SYSTEM

Considering security requirement, security management of Grid Computing System and four layer architecture. We present new five

layer security architecture from bottom to up these five layers are-

A. Node and Interconnection Layer

This layer provides physical security to hardware resources.

B. System and Network Security Layer

This layer includes virtual privet network layer, secure socket layer, secure shell, firewalls, and integrity checks.

C. Security Abstract Layer

This layer encapsulates security technologies and provides uniform interface for Grid security protocol layer.

D. Grid Security Protocol Layer

This layer provides Grid Security protocols like user proxy creation, resource allocation from process & mapping registration protocol.

E. Security Application Layer

This layer provides applications based on security protocols. The layers of the five layer security architecture and the layers of the four layer security architecture Grid Computing System corresponding relationships. We place node and interconnection layer and system and network security technology layer in different layer and place all system and network security technology in is same layer. Security abstract layer and security application layer are implemented

In Grid system software layer of four layer architecture of Grid Computing System. The five layer security architecture layer supports services for higher layer and higher layer utilizes the services supported by lower layer.
Foster and other people [3] have been studying Grid
Security protocols these are given below-
User proxy creation protocol
Resource allocation protocol
Resource allocation from process protocol
Mapping registration protocol

V. NEW SET OF SECURITY POLICY FOR FIVE LAYER SECURITY ARCHITECTURE

Considering the five layer security architecture of Grid Computing System now we will define a new set of security policy.

A. Policy about Object

An object is a resource or process that is being protected by security policy. There are two kind of object in Grid Computing System: Global Object &Local Object
A Global Object is the abstraction of one or more local objects. Global Object and Local Object exist in Grid Computing System at the same time.

B. Policy about Subject

A subject is a participant in a security operation. In grid system, a subject is generally a user, a process operating on behalf of a user, a resource, or process acting on behalf of a resource. There are two kind of subject in Grid Computing System: Global Subject & Local Subject
A Global Subject is the abstraction of one or more Local Subject. Global Subject and Local Subject exist in Grid Computing System at the same time.

C. Policy about Security

There are two kinds of Security Policy in Grid Computing System:Global Security Policy & Local Security Policy
Global Security Policy is the abstraction of all Local Security Policy. Global Security Policy & Local Security Policy exit in Grid Computing System at the same time.

D. Policy about Trust Domain

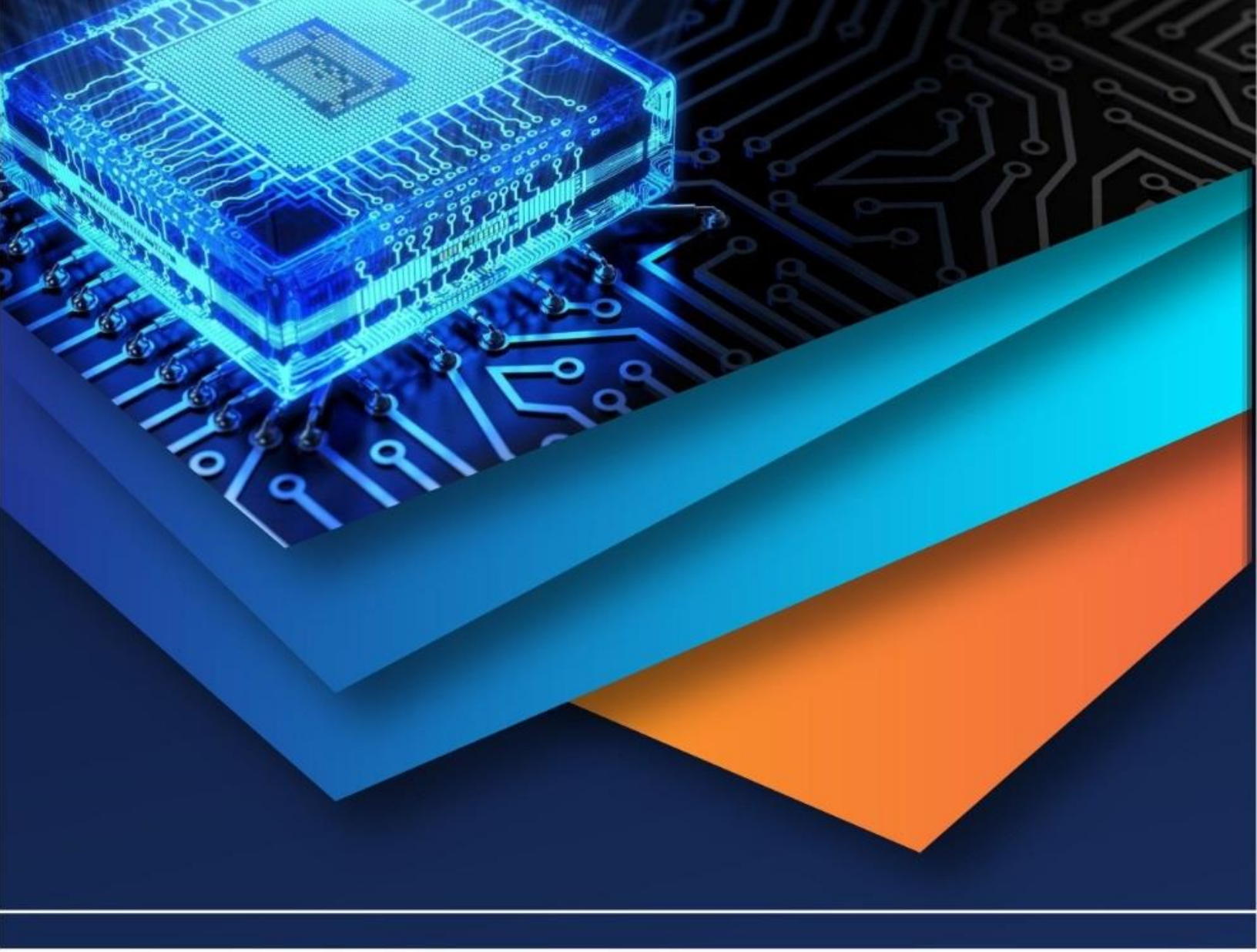
A Trust domain is a logical, administrative structure within which a single, consistent local security policy holds. In other words a trust domain is a collection of both subjects and objects governed by single administration and single security policy. There are two types of trust domain – Global trust domain and Local trust domain. Global trust domain is the abstraction of all local trust domains. Global trust domain and Local trust domain exists in Grid Computing System at the same time.

VI. CONCLUSION

Security problems in Grid Computing System are crucial because Grid Computing System works between Virtual Organizations (Heterogeneous Environment). Research on security is burning topic in Grid Computing System. We present five layer security architecture of Grid Computing System. Considering the Five layer security architecture based on Security Policy, we define a new set of Security Policy & present the representaion.Considering the existing Grid Security Policy, we will extend authentication & authorization model of distributed System & define Grid Security Policy layer to solve the problems of authentication & authorization in multiple domain.

REFERENCES

[1] I. Foster, C. Kesselman, editors. Computational Grids: The Future of High Performance Distributed computing,1998.
[2] I. Foster, C. Kesselman, S. Tuecke, The Anatomy of the Grid, International J. Supercomputer Applications, 2001.
[3] I. Foster, C. Kesselman, S. Tuecke, G. Tsudik, A Security Architecture for Computational Grids, the 5th ACM Conference on Computer and Communication Security.
[4] M. K. Singh, S. Pal, Requirements for Developing Open Grid Services Architecture, Varahmihir Journal of Computer & Information Sciences,2008.
[5] M. K. Singh, S. Pal, Security Issues in Grid Computing, Pragyaan; Journal of Information Technology, 2010.
[6] I. Foster, C. Kesselman. The Globus Project: A progress report. In Heterogeneous Computing Workshop,1998.M.K. Singh et al, / (IJCSIT) International Journal of Computer Science and Information Technology



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY