International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Security in Grid Computing Using Globus and Legion

Prof. Sarita Khedikar[1], Krushna Jadhav[2], K Govind Kumar[3], Atul Rajanale [4]

[1]*Professor Sarita Khedikar, Dept. of Computer Engineering, smt Indira Gandhi college, Maharashtra, India*
[2]*Student Krushna Jadhav, Dept. of Computer Engineering, smt Indira Gandhi college, Maharashtra, India*
[3]*Student K Govind Kumar, Dept. of Computer Engineering, smt Indira Gandhi college, Maharashtra, India*
[4]*Student Atul Rajanale, Dept. of Computer Engineering, smt Indira Gandhi college, Maharashtra, India*

Abstract—*Grid computing is a type of distributed computing that share their resources between individual computers such as coordinating and sharing computational power, data storage and network resources across dynamic and geographically dispersed organizations. Till now we are having many scheduling algorithm but in all such scheduling algorithm there are some advantage and disadvantage. So we cannot perfectly say that this scheduling algorithm is best of all.*

So a research on that is mandatory but by using any one scheduling algorithm we can fulfill our needs so before doing research on that we have to see on other fields also which is more important than that from all of this can make our work. The other field is security. Resources which we are shared between server and clients should be secure and the third party cannot use it without any proper authorization. As resources are transferred between client and server using network so there may be chance of any misuse of these resources. So our main goal is to provide such a security which will prevent the misuse of these transferring resources.

Motivation of the survey is to encourage the future researcher to research in this field of grid computing, so that they can understand easily the concept of security in grid computing and can provide other security to this system. This will benefit interested researchers to carry out further work in this thrust area of research. We are providing this security combining the best security features present in different architectures into a single architecture to overcome the disadvantages of different architectures.

Keywords---**Grid computing, Resources utilization, Security mechanisms.**

1. INTRODUCTION

Grid computing is a term in distributed computing systems which allow the management of heterogeneous, geographically distributed and dynamically available resources in an efficient way, extending the boundaries of what we perceive as distributed computing. For running applications, resource management, providing security and job scheduling are the most crucial problems in grid computing systems. In recent years, the researchers have proposed several efficient security algorithms that are used in grid computing to provide security in grid computing. With further development of grid technology, it is very likely that corporations, universities and public institutions will exploit grids to enhance their computing infrastructure. This survey paper is organized as follows: In which we deal with the definition of different models of grid computing and how to combine this different models to get a hybrid architecture which provide maximum security to the shared resources.

2. BASIC GRID MODEL

The grid model actually consists of a number of clients and a server, each composed of several computational resources, which may be homogeneous or heterogeneous. The server is used to provide computational resources and security to these resources while sharing between different clients. The four basic building blocks of grid model are user, resource broker or sever, grid information service (GIS) and lastly resources. When user requires high speed execution, the job is submitted to the server in grid. Server splits the job as needed by the clients into various small tasks and distributes it to several resources according to user's requirements and availability of resources. GIS keeps the status information of all resources which helps the Broker for scheduling.

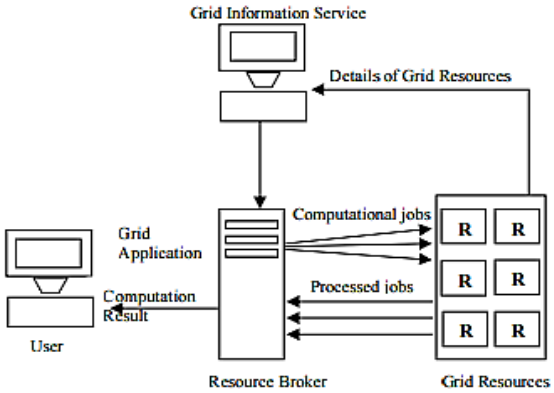


Fig. 1 Basic Grid Model

3. Grid Security Overview

Security is one of the important issues that usually arise when considering a grid environment. Since the goal of grid computing is sharing of resources, computer resources can be accessed by a lot of different virtual organizations (VOs) depend upon there need. The security requirements are fundamental to the Grid security design. The high level grid security requirements include following aspects:

1. Authentication: The process of identifying the users usually based on a username and password. Authentication ensures that the user who he or she claims to be, but nothing says about the rights of these users.
2. Authorization: Specific user can do specific things so these rights are checked at authorization.
3. Delegation: In this there is a software mechanism in which it check automatically that what are the rights which a user is having and if he/she want to access something else then provide it depend upon some security levels.
4. Message integrity: The messages received by the client or user should be same as send by the sender. If any changes was done in the message then that should be indicated.
5. Single Sign in: In this the user or admin should enter there username and password. After having match of this username and password with the one present at the database. It will send the OTP to the email ID. Once you enter this OTP then only you can enter inside your system,
6. Confidentiality: Protecting confidentiality of underlying transport and message content and between OGSA-compliant components in either point-to-point or store and forward mechanisms Privacy: Allowing both a service requester and a service provider to define and enforce privacy policies.
7. Policy exchange: Allowing security context negotiation mechanism between service providers and service requesters based on security policy information
8. Credential life span and renewal: Every user should provide a life span till which only he can access the system. After that the user should again login.
9. Secure logging: Providing a foundation for non-repudiation and auditing that enables all services to time-stamp and log various types of information without interruption or information alteration by adverse agents.
10. Assurance: User should have knowledge about all the security which we are providing to our system. This information is useful in deciding whether to deploy a service in the environment.
11. Manageability: This requirement mainly deals with various security service management issues such as identity management, policy management, and so on.
12. Firewall traversal: Ability to traverse firewalls without compromising local control of firewall policy to enable cross-domain grid computing environment

Securing the OGSA infrastructure:
This refers to securing core OGSA components. The security challenges faced in a Grid environment can be grouped into three categories

Integration with existing systems and technologies:

Interoperability with different "hosting environments"
Trust relationships among interacting hosting environments.
Because of the dynamic and multi-institutional nature of the grid environments, we need new technical approaches to solve security problem.

4. Grid Security Infrastructure (GSI)

In order to overcome the security challenges, Globus proposes the Grid Security Infrastructure (GSI). GSI is composed of a set of command-line tools to manage certificates, and a set of GSS-API to easily integrate security into other web services. GSI offers the following functions;

- Transport-level Security
- Message-level security (WS-Security and WS-Secure Conversation)

Authentication through X.509 digital certificates several authorization schemes
Credential delegation and single sign-on Different levels of security: container, service, and resource

GSI has satisfied basic Grid security requirements, such as authorization, delegation, authentication and message protection's provides two levels security: Message-level Security and Transport-level Security. Our research survey will focus on message-level interoperability. For both levels, we have server and client side security.

LEGION

Legion is a Grid computing platform which combines a large scale of independently administered machine. The processors, resources, database, user objects and other objects, are all distributed over a wide area network; each client and server machine have its own administrative level. The main advantage of Legion is that it combines the component together with the help of single, object-based met computer which primary goals, flexibility and site autonomy. One of the designs based on this single object-based is Security.

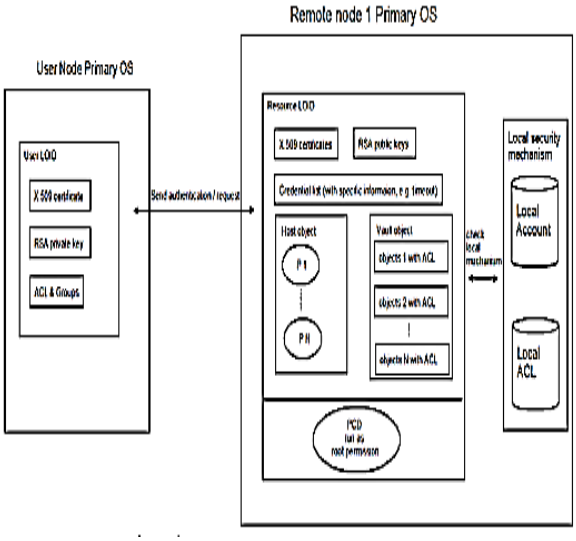


FIG.4.1 LEGION ARCHITECTURE

GLOBUS

According to Globus architecture it assumes that the Grid computing is large and dynamic. Due to which it think that the number of user who are going to use it is also in a large amount. So by considering this in mind this architecture provide all type of security measure which includes integrity, access control,

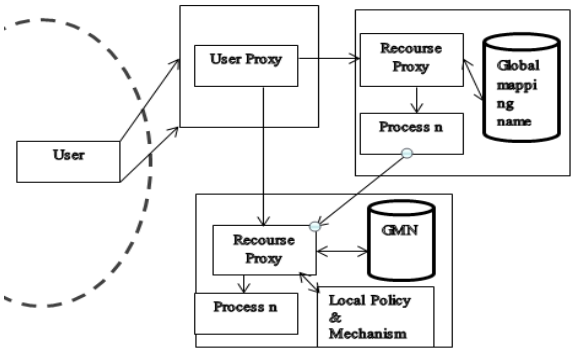


FIG 4.2 GLOBUS ARCHITECTURE

privacy, authentication, and non-repudiation. In security it gives more preference to authentication and access control. As stated earlier that Globus is also a system that includes numerous trust domains. User, resource, process is a participant called subject (both global and local with a different name), whereas a resource that is being protected by security policy is called object.

The process in which subject makes another subject to prove its identity with its credential is called authentication. One a user get authenticated by the server, after that user can use/access an object on the local machine by authorization. All the access control, Decision of an object is made locally by the administrator or server.

CRISIS

The main aim of this architecture is to make the grid computing system act as a component within WebOS. WebOS is a wide area application which provides support to network application and a basic function as a common OS services. As security is using WebOS so the resources are present at the different end. Hence due the which the security issues in crisis architecture include Redundancy, Least Privilege, Accountability, and Local Autonomy (Access control). Although it covers a lot of security problems, the main security issues are authentication, authorization and least privilege. Hence we should have to focus on it. There is some Process Managers (PM) and a Security Manager (SM), the PM listens to a certain request, e.g. login and resource request; depend upon the request the SM will provide the credentials of a user/resource and validates the certificate transmitted by others. These PMs identify the administrative domain within a request, and then ask the Security Manager whether they have the privilege to access remote resource.

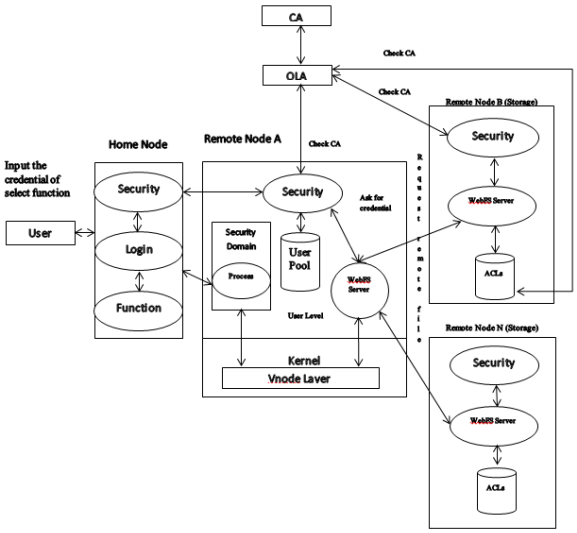


FIG.4.3 CRISIS ARCHITECTURE

5. DIFFERENCE BETWEEN THE ARCHITECTURES OF GLOBUS, CRISIS AND LEGION

The differences between these three architectures are shown in Table, as mentioned in previous section, these three systems are really similar to others. However, as shown in Table, we could see that Globus is the one that serve with the fewest security features. The reason might due to this is a first version of this security architecture, and this version focuses on the single sign-on mechanism. In addition, CRISIS likely pro-vides a completed

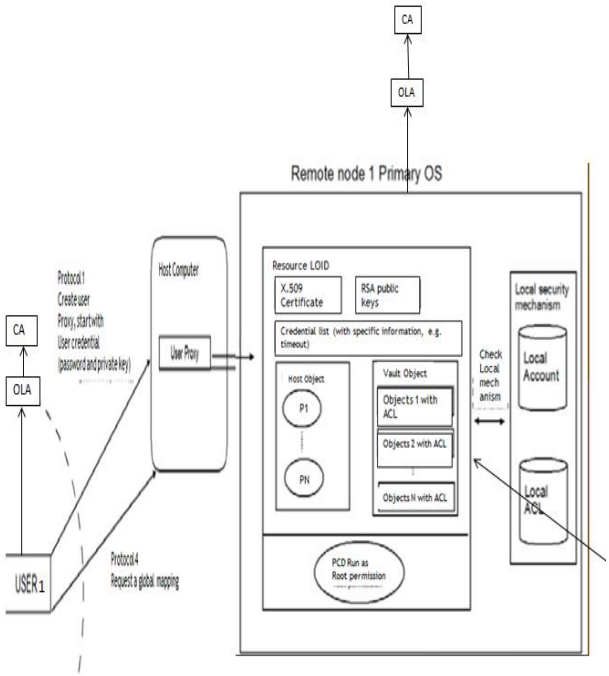
implementation for all security issue. Meanwhile, Legion seems to support all the security features.

	Legion	Globus	CRISIS
Architecture	Flexible	Extendable	Fixed
Authentication	LOID	User and Resource proxy ,single sign-on mechanism	Service Process and security manager, single sign-on mechanism
Authorization	LOID	User and Resource proxy	Service process and security manager
ACL	Object-based ACL	Use local machine ACL which checks with local Resource Proxy	Using local machine ACL which check with local Security man-ager
Authentication session	Maintain by user /developer	Long term session by Resource Proxy or short term by User Proxy	Public key with session timeout
Isolation	Host and Vault Objects use their own dedicated Local accounts to ensure isolation from other user objects.	N/A	CA/OLA redundancy
Least privilege	Using PCD to act as different level of account privilege	N/A	Using user-level and kernel level system call to reduce the privilege of a user/remote process.
Accountability	N/A	N/A	Yes

Table 5.1 Difference between the three architectures

6. HYBRID ARCHITECTURES

After comparing the differences, and skip ahead to nowadays, we get to know that whether know this architecture is existing or disappeared. First of all, single sign-on is a good mechanism to tell that the user is authenticated or not. Due to which there should be no doubt about to whom we are sending the resources. Second, If we are keeping ACLs control to a local administrative then the Grid system being more flexible and is more suitable for realistic requirement. Third, for every user we should provide a session time once he/she logged in. If that amount of session time is finished then the user should again login. By this we can enhance the security of our ports and nodes. Meanwhile, this feature sometimes helps a Grid system achieve Isolation. Fourth, the CA/OLA hierarchal trust mechanism is a high-level skill that avoid attacker taking control of a Grid node. However, this might increase network traffic as each node must check the CA/OLA before running a task. Last but not least, the least privilege is really important issue in today's security, even though Legion and CRISIS seems to achieve this goal. For instance, PCD runs as root permission, once if



attacker handle this PCD process, the system will break. So we are entering the data in PCD in such a manner which cannot be understood by the attacker. This mechanism provides the better security in PCD. The PCD gain the root permission such as "sudo" command in Ubuntu Linux cannot help attacker to gain full access.

7. FUTURE WORK

- We do experiment in reducing the size of the encrypted data.
- We produce a way to make double encryption of public and private key and also to change the random key whenever the user is going to send a message.
- We encrypt our database in such a manner that an external person cannot see it even though he can come to our database.
- We make a program in such a way that automatically the OTP value will be entered if you login to your email-ID because it is sometime become difficult to write a complex OTP in your system.

8. CONCLUSION

Security architecture Legion, Globus, and CRISIS has common features include authentication, authorization, least privilege, isolation, and Access control. Focusing on these features, we shortly indicate the differences between these systems. Furthermore, we discuss the pro and cons among these systems, and make a conclusion how to combine this architecture and form a hybrid architecture which provide better security..

For instance, the CA/OLA hierarchal trust mechanism could be added to a Globus based system in order to achieve Isolation. In addition, the flexibility of Legion could provide researcher a test environment of new security issues. Having such review of security in Grid Computing helps me understanding in different major studies, security concerns depend on vary requirement.

9. REFERENCES

[1]Security in Grid Computing TakLon Wu B534 project 3 Computer Science Dept. Indiana University Bloomington, IN 47405 taklwu@indiana.edu

[2]Security Implications of Typical Grid Computing Usage Scenarios Marty Humphrey Computer Science Department University of Virginia Charlottesville, VA 22904 humphrey@cs.virginia.edu Mary R. Thompson And Distributed Security Research Group Lawrence Berkeley National Laboratory Berkeley, CA 94720MRThompson@lbl.gov

[3]Book Grid Computing by C.S.R. Prabhu

[4]A Survey of Job Scheduling and Resource Management in Grid Computing from World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:4, No:4, 2010 by Raksha Sharma, Vishnu Kant Soni, Manoj Kumar Mishra, Prachet Bhuyan.

[5] Ian Foster and Carl Kesselman, "The Grid: Blueprint for a New Computing Infrastructure," Elsevier Inc., Singapore, Second Edition.