International Journal of Computer Applications (0975 – 8887)
Volume 164 – No 6, April 2017

Security of Grid Computing: A Cryptographic Approach

Munindra Kumar Singh, PhD
Department of Computer Application
V.B.S. Purvanchal
University Jaunpur

Prashant Kumar Yadav
Department of Computer
Science & Engineering
V.B.S. Purvanchal
University Jaunpur

ABSTRACT
Now a days, Grid Computing is becoming very popular, because of it's ability to provide information and services that are distributed across several control domains. A grid performs some distributed computations to achieve their goal. But the problem is that, how much a grid is secure in distributed environment. Is there any security breach is possible? If yes, Then how it can be prevented? In this paper, we are trying to solve such questions.

General Terms
Grid Computing and its security. Cryptographic techniques, Grid Security algorithm

Keywords
Grid Computing, Grid Security, Cryptography: Symmetric & Asymmetric, GRAM, OGSA, RSL, SOAP, RA.

1. INTRODUCTION
The term "Grid Computing" is used to represent the collection of more than one computational machines and resources distributed globally to perform problem solving computations. There are two terms as GRID and COMPUTING. A grid is a collection of hardwares and softwares put together to achieve consistent and inexpensive computational capability, and Computing is the procedure followed by that architecture to solve any specific problem. This technology is becoming very popular due to its availability at very low cost. But there are security issues are arises when grids are made available for computation of network users.

In this era, the world wide communication media, Internet provides more convenient way to the peoples to communicate, although they are far away with each other. Internet is a widely used network which is shared to all. Hence security is going very important issue, if we are using Internet to communicate sensitive data and information.

There are different methods and techniques are available to perform secure communication. One of those are Cryptographic algorithms. The cryptography is considered as the branch of both Computer Science and Mathematics. Cryptography is an art of insuring security and is a study of securing or hiding information. Cryptography is widely used in current technological applications such as ATM transaction, Internet Banking and many more. Currently due to demonetization of old currency, the Indian economy is going towards cashless, where different technologically advanced application will take place, which all will be cryptographically armed for insuring confidentiality and security. The security of information is preserved with the help of cryptographic algorithms.

The cryptographic algorithms are categorized into two types as: Private Key Cryptography sometimes known as Symmetric Key Cryptography, and Public Key Cryptography, also known as Asymmetric Key Cryptography. Here we are proposing an algorithm which is symmetric key cryptographic algorithm for securing information which is to be transmitted over world wide.

2. CRYPTOGRAPHY
The step by step procedures followed to ensure security of information is known as cryptographic algorithm. All these algorithms work in two phase as : Encryption phase and Decryption phase. The information that can be read and understand easily without any special effort is known as plain text. The process of converting plain text into unreadable form to hide and secure information is known as encryption and hidden form of information is known as cypher text. The process to gain back plain text from cypher text is known as Decryption. All these encryption and decryption processes are used to achieve the following goals:

2.1 Authentication
This term is used to identify or authenticate both the peer entity that is supposed to receive information and the data origin entity from where the information is to be send. Digital signatures and digital certificates, used to provide authentication.

2.2 Access Control
The prevention of unauthorized use of resources is termed as access control. Access control mechanism allows only authenticated users to use information or resources.

2.3 Data Confidentiality
The protection of data from unauthorized disclosure is called data confidentiality. There are four levels of data confidentiality as:

2.3.1 Connection Confidentiality
The protection of all user data on a single connection is known as connection confidentiality. The whole connection is made confident in connection confidentiality. Data must be sent via that confident connection to ensure confidentiality.

2.3.2 Connectionless Confidentiality
In this, the protection is performed on all user data in single data block and then can be transmitted over any connection.

2.3.3 Selective Field Confidentiality
In selective field confidentiality, the protection takes place only on selected fields of information.

2.3.4 Traffic Flow Confidentiality
The traffic flow confidentiality ensures confidentiality of the information that might be derived from observation of traffic flow.

2.4 DATA INTEGRITY
Data integrity is an assurance that the data which is received must be exactly same as sent by an authorized entity. Data integrity may be of different kind as:

- Connection Integrity with recovery, which detects any unauthorized modification on entire data sequence with recovery attempt.

- Connection Integrity without recovery, only detects unauthorized modification on entire data without recovery attempts.
- Selective-field connection integrity provides integrity for selected field within the user data with recovery attempt and without recovery attempts as needed.

3. GRID SECURITY

To overcome the security challenges as described above, the term "Grid Security Infrastructure (GSI)" is used. It is used to provide basic security, required by grid which includes confidentiality, authentication and integrity of data. GSI is made by the collection of command-line tools for managing certificates and a set of GSS-API for easily integrating security into other web services. The grid security module contains following component :

- Application specific components
  - Credential and Identity Translation (CIT).
  - Access Control Enforcement (ACE).
  - Secure conversation.
  - Audit and Non-repudiation.
- Policies and rule components
  - Identity/Credential mapping.
  - Authorization.
  - Privacy.
  - Services/end-point.

3.1. Grid Overview

Different kinds of GSI protocols can be created along with GRAM (Grid Resource Allocation and Management). GRAM provides different web services for initiating, monitoring, execution and termination of processes on remote machines. It is also responsible for parsing and processing the RSL (Resource Specification languages).There exist the most important grid computing architecture named as Open Grid Services Architecture (OGSA). The foundation of OGSA is Web Services. SOAP is known as one of the most important standard of web services. SOAP stands for Simple Object Access Protocol, which provides a method for communication between services requester and service provider. SOAP creates an envelop for communication and this envelop can be delivered using different protocols as FTP, HTTP or HTTPS.

The OGSA defines policies and capabilities which grid systems mainly concerns, such as establishment of authentication, access control etc. It is also responsible for deployment, discovery and monitoring of physical or logical resources distributed across different heterogeneous environments. As we know that the Grid System is a service-oriented architecture and OGSA uses the concept of web services. With web services we will use some security specifications that will create an integrated, inter-operable secure web services for users. Following is the protocol architecture of grid, defined in five layers:

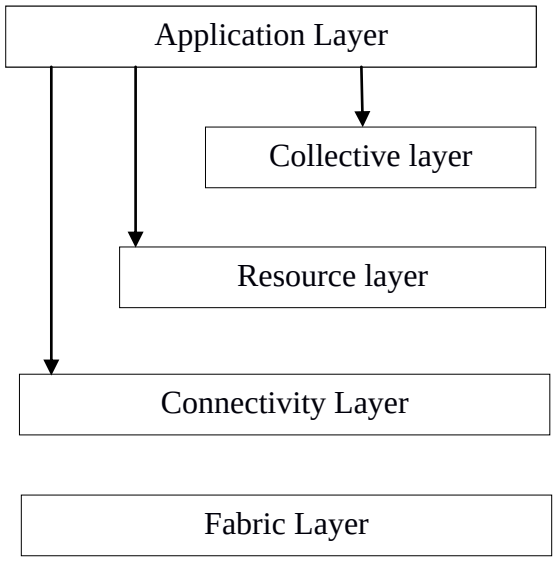

Figure. 3.1: Grid Protocol Architecture

FABRIC LAYER is responsible for providing access to different resources such as network resources, code repository etc. The fabric layer provides the resources to which the shared access is controlled by the grid protocols. The resources normally include physical and logical entities. Physical entities are resources like storage systems, catalogs, servers, and network resources. The resource may be a logical entity like distributed file system, computer cluster or distributed computer pool, and database systems to store structured data. The Grid mechanism normally permits the capability for the resource management, which involves discovery and control.

CONNECTIVITY LAYER is used to define authentication protocols and provides secure communication for network transactions. The connectivity layer defines core communications and authentication protocols required for Grid specific network transactions. These protocols enable the exchange of data between fabric layer resources. The resource layer, based on the connectivity and authentication protocols, controls the access resources.

RESOURCE LAYER uses GRAM protocols for allocation, monitoring and control of computational resources.

COLLECTIVE LAYER is responsible for capturing interactions across resources. It uses MDS (Monitoring and Discovery Services). The collective layer services deals with the directory brokering services, scheduling services, data replications services, and diagnostics/monitoring services. These services are not associated with any one specific resource but focus on interactions across resources.

The programming models and tools define and invoke the collective layer functions. This layer is a key component in the whole grid architecture and its functioning. This is the layer that glues all the resources together in expedient exchange.

APPLICATION LAYER The top layer, User Applications, comprises the user applications that operate within a Virtual Organization (VO) environment.

3.3 Grid With Cryptography

In layered architecture of grid computing, the connectivity layer plays very crucial role for providing secure communication. If we enrich this layer with some cryptographic algorithms, then our goal will be achieved. Here we are trying to implement security protocols with connectivity layer protocols. We will

use symmetric key cryptography with OGSA.

The OGSA is responsible for successful execution of different web services and protocols. With OGSA protocols we need to implement symmetric key cryptography. For doing so, we have to use a Registration Authority (RA).

3.3.1 REGISTRATION AUTHORITY

The responsibility of registration authority is to register new incoming nodes which wants to access grid, by cross-checking their credentials. This will be performed on OGSA architecture. The OGSA uses different security protocols for secure communication but it never assures that the incoming node is authenticated for accessing grid services and resources or not.

Registration Authority uses algorithms for both service-user end and service-provider end. Following is the proposed algorithm which is to be followed by new incoming nodes:

Service-User end

1. Start
2. Generate a request to establish a communication link with RA via OGSA.
3. Identify itself by providing their identity credentials.
4. Wait for RA response.
5. If

   received message is : Unauthorized access.

   go to step 7.
6. If

   received message is : Authorized.

   use grid resources & services.
7. Exit.

Service-Provider end

1. Start.
2. If

   there is no any request for communication

   go to step 1.

   Else

   go to step 3.
3. Receive identity credentials from new incoming node.
4. Perform verification of received credentials.
5. If

   identity verification failures,

   send a message : Unauthorized access.
6. If

   identity verification successful,

   send a message : Authorized.
7. Exit.

Using above algorithms, we can easily identify that new incoming node have the authority to access grid resources and services or not, according to their credentials provided to registration authority.

4. CONCLUSION

Our proposed system with RA powered OGSA will become more secure than traditional grid computing system. In traditional grid computing systems the OGSA is only responsible for providing security and there is no any clear infrastructure exist for providing security from unauthorized access. But hear, with the help of symmetric key cryptography and registration authority, we are trying to implement new security infrastructure for grid computing.

The only drawback of our proposed system is that, using RA concept, we have to maintain a large database for new incoming nodes. This will become very tedious job.

5. REFERENCES

[1]. M. K. Singh, Dr. S. Pal “Five Layer Security Architecture and policies for Grid Computing System” International Journal of Computer Science and Information Technology, Volume2(2), 2011.

[2]. M. K. Singh, Dr. S. Pal “Security Issues in Grid Computing” Pragyan Journal of Information Technology, Volume8: Issue 1, pp1-4, June 2010.

[3]. M. K. Singh, Dr. S. Pal “Requirements for Developing Open Grid Services Architecture” Varahmihir Journal of Computer and Information Science, pp 97-103, 2008.

[4]. Harmeet Kaur, Kamal Gupta “Challenges in Grid Computing” International Journal of Scientific Research & Technology (IJSRET), Volume 2, Issue 3, pp141-144, June 2013.

[5]. Jianmin Zhu and Dr. Bhawani Thuraisingham “Secure Grid Computing” International Journal of Computer Science and Network Security, Volume 6, No.8B, August 2006.

[6]. James C. Browne “Grid Computing as Applied Distributed Computation: A Graduate Seminar on Internet and Grid Computing” IEEE International Symposium on Cluster Computing and the Grid. 2004.

[7]. Gurlin Kaur, Indraprit Chopra “Grid Computing Challenges Confronted and Opportunities offered” Department of Computer Applications, PCTE, Ludhiana.