International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

REVIEW ARTICLE

ISSN: 2321-7758

# AN OVERVIEW OF GRID COMPUTING SECURITY ISSUES

**VISHAL P.GAWANDE[1], Prof.S.R.JADHAO[2]**

[1]M.E.(First Year), [2]Assistant Professor Department of CSE, BNCOE, Pusad, Maharashtra, India

Article Received: 12/04/2015 | Article Revised on:17/04/2015 | Article Accepted on:20/04/2015


**ABSTRACT**

Grid is an infrastructure that involves the integrated and collaborative use of computers, networks, databases and scientific instruments owned and managed by multiple organizations. The main focus is given to enhance the security of the 'data' and the 'processes' which operate on these data, which essentially are both public in nature as far as grid computing is considered.This paper deals with the challenging security issues that demand new technical approaches.and study about the various security issues in grid computing.Also this paper provides an overview about the state-of-the-art of securityin current grid technologies.

**Keyword:** Grid, Security, Kerberos, SSL, Authentication, KDC, Digital Certificates



**INTRODUCTION:** Grid computing is the collection of computer resources from multiple locations to reach a common goal. Grids allow the simultaneous use of large numbers of resources, dynamic requirements, use of resources from multiple administrative domains, complex communication structures, and stringent performance requirements. Security is a latest topic today for the smart grid. Grid computing is a technique which provides high-performance computing; in this resources are shared in order to improve the performance of the system at a lower price. Grid computing is a system where multiple applications can integrate and use their resource efficiently. The major aim of this paper is to study about data grid security issues and provide a solution to guard data or information in Grid Services that are appeared while operating in data storage systems and we present a cryptographic & fragment based scheme to accomplish the server protection requirements associated with a standard Data Grid environments.

**LITERATURE SURVEY**

There has been a lot of research done in the area of Grid Computing security issues carried out by

the prominent authors in the recent past. In year 2014,OmerahYousuf, AbRouf Khan, Vairamuthu Sin their paper titled " Improving Data Security and Efficiency in Grid Computing using Object Based Grid Architecture"[1]' discussed improving data security and efficiency in the grid environment based on the object oriented concepts.. In the year 2013,Rashmi Bhatia in their paper "Grid Computing and Security Issues" discussed different Issues of the security[2].In year May 2014, Raafiya Gulmeher, Dr. Mohammed Abdul Waheed in their paper "Security Analysis for Data Grid Middle wares"[3] The purpose of this paper is to explore the security problems in grid computing and the steps that can be taken to solve them. Von Welch,FrankSiebenlist ,Ian Foster, John Bresnahan, Karl Czajkowski ,JarekGawor ,Carl Kesselman ,Sam Meder ,Laura Pearlman ,Steven Tuecke presented paper "Security for Grid Services"[4]. In year 2014, Neha Mishra, Ritu Yadav and SaurabhMaheshwari presented paper title as "SECURITY ISSUES IN GRID COMPUTING"[5]. Muhammad AsifHabib? and Michael Thomas Krieger, JohannesKepler University, A-4040 Linz, Austria presented paper "Security in Grid Computing"[6].This paper provides an overview about the state-of-the-art of security in current grid technologies and a discussion about possible weaknesses which have to be considered at the current approach.

**GRID SECURITY ISSUES:**

Security is one of the main issues that usually arise when considering a grid computing environment. There are some Technical security requirements that should be in place in grid computing systems.

- **Technical Issues:**
- Logging information.
- Single sign-on.
- Protection of credentials.
- Uniform credentials/certification infrastructure.
- Delegation of access rights.
- Message integrity.
- Privacy.
- Interoperability with local security solutions.
- Support for secure group communication.
- Support for multiple implementations.[3]

The grid security issues can be categorized into three main categories:

a) Architecture Issues,
b) Infrastructure Issues,
c) Management Issues.

**a) Architecture Issues:**

The architecture issues involve the overall grid system, including information security, strategy mapping, and decline, etc. The information security in grid system is briefly classified into:Secure Communications, authentication, single sign-on, and agent.

**b) Infrastructure Issues:**

The Infrastructure issues relate to the network and host components which constitute the grid infrastructure. The main sub issues here are: data protection, job starvation, and host availability. A grid involves running alien code in the host system. Therefore, thehost can be apprehensive about the part of the system which contains important data. The external jobs should not reduce the priority of the local jobs, and hence lead to job starvation. Similarly, if the host is a server, it can be concerned about its own availability. There should be mechanisms to prevent the system from going down resulting in denial-of-service to the clients attached to the host.

**c) Management Issues :**

. Managing credentials is absolutely important in grid systems because of the heterogeneous nature of the grid infrastructure and applications. Like any distributed system, managing trust is also critical and falls under the purview of management related issues. Much of the information obtained from the monitoring systems is fed back to higher level systems like intrusion detection and scheduling systems.

**SECURITY RISKSIN GRID COMPUTING:**

When downloaded application from the internet there must be security risks. Whenever you link two or more computers together, you have to prepare yourself for certain questions. How do you keep personal information private? How do you protect the system from malicious hackers? How do you control who can access the system and use its resources? Thus Security requirements are fundamental to the grid design. The critical problems are resource discovery, authentication, authorization, and access mechanism. Without this functionality, the integrity and

confidentiality of the data processed within the grid would be at risk.

**SOLUTION TO SECURITY RISKS:**

**A. Authentication:**

Authentication is the process of verifying identity of a participant to an operation or request. Authentication methods are Password-based, Kerberos authentication, SSL authentication, Certification authorities.

1) **Password-based Authentication** :

Password-based Authentication is a simple function where one party presents a set of credentials (user ID and password combination) to a system. If the credentials match a given set on the system, the system returns a value that represents authorization; otherwise it does not. Some important issues in this are to send unencrypted passwords only when messages can't be read by un-trusted processes while on network, otherwise instead of sending passwords over network one can use password as encryption key. They can encrypt a known but non-repeating value, Send encrypted value to party verifying authentication and both parties must know password or trust a third-party to distribute it.

2) **Authentication Systems: Kerberos:**

Kerberos is a computer network authentication protocol which works on the basis of "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed primarily at a client–server model, and it provides mutual authentication—both the user and the server verify each other's identity.

**Authentication process using Kerberos:**

- client sends the user name to the KDC.
- KDC respondswith pre-authentication request.
- The client sends the Authenticator: the client's principal and the time stamp, encrypted with the user's
- The KDC sends:
  - The Ticket Granting Ticket (TGT), encrypted with the TGS key
  - A client/TGS session key, encrypted with user's key.
- The client decrypts the session key and caches the TGT. The TGT includes the TGS copy of the client/TGS session key, client principal, ticket lifetime, KDC timestamp, client IP address.
- The client sends to KDC (TGS):
  - TGT
  - Authenticator: client principal and the time stamp, encrypted with with the client/TGS session key
  - desired service principal name.
- KDC validates the TGT and the Authenticator, then sends following to the client:
  - Service ticket, encrypted with the Server key. The Service ticket includes client/Server session key, client principal, ticket lifetime, KDC timestamp, client IP address.
  - client/Server session key, encrypted with the client/TGS session key.
- The client sends the following to the application server:
  - the Service ticket
  - Authenticator (the client principal and time stamp encrypted with the client/Server session key).
- The application server decrypts the Service ticket with its key stored in the keytab, /etc/krb5.keytab,validates the authenticator and sends a confirmation encrypted with the client/Server session key.

The client decrypts the confirmation by the client/Server session key and checks whether the timestamp is correctly updated. If so, the client starts issuing service requests.[9]

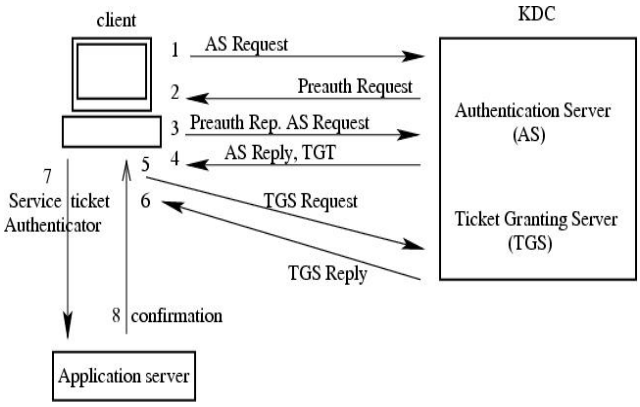


**Fig. 1.**Authentication process using Kerberos

3) **Authentication Systems: Secure Sockets Layer (SSL) :** Secure Sockets Layer (SSL) is a method for providing security for web based applications. It is designed to make use of TCP to provide a reliable end-to-end secure service. SSL are cryptographic protocols that provide communication security over the Internet. Every Client authenticates identity of the server by sending a session key from client to server to set up an encrypted communication.SSL is not a single protocol but rather two layers of protocols as illustrated in fig.It can be seen that one layer makes use of TCP directly. This layer is known as the SSL Record Protocol and it provides basic security services to various higher layer protocols. An independent protocol that makes use of the record protocol is the Hypertext Markup Language (HTTP) protocol.

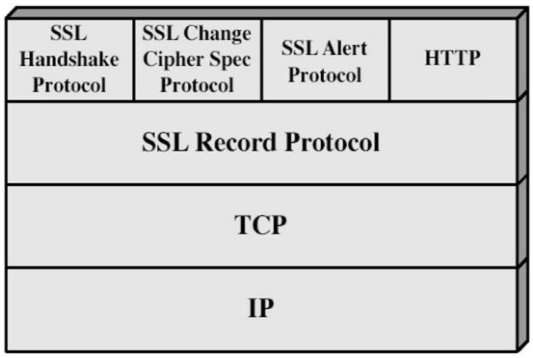


**Fig 2.**SSL protocol stack.

Handshaking procedure between client and server using SSL is as follows:

- The client sends a Hello message to the server.
- The server responds by sending a Hello message to the client. This message includes:
  - The algorithm to use.
  - A random number, which will be used to generate the keys.
- The server sends its certificate to the client.
- The client authenticates the server using the server's certificate.
- The client generates a random value encrypts it using the server's public key, and sends it to the server.
- The server uses its private key to decrypt the message to retrieve the pre-master secret.
- The client and server separately calculate the keys that will be used in the SSL session. These keys are not sent to each other because the keys are calculated based on the pre-master secret and the random numbers, which are
  - Encryption key that the client uses to encrypt data before sending it to the server
  - Encryption key that the server uses to encrypt data before sending it to the client
  - Key that the client uses to create a message digest of the data.
  - Key that the server uses to create a message digest of the data. The encryption keys are symmetric, that is, the same key is used to encrypt and decrypt the data.
- The client and server send a finished message to each other. These are the first messages that are sent using the keys generated in the previous step (the first "secure" messages).
- The finished message includes all the previous handshake messages that each side sent. Each side verifies that the previous messages that it received match the messages included in the finished message
- The client and server now transfer data using the encryption and hashing keys and algorithms.

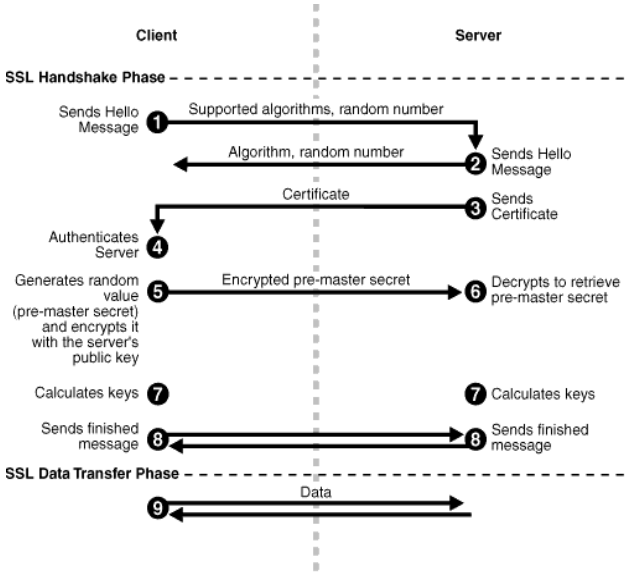


**Fig.3**.Handshaking procedure between client and server using SSL

**4) Digital Certificates and Certification Authorities (CA):**

Digital Certificates is the electronic document used to prove ownership of a public key. Certification authority (CA) is an entity that issues digital certificates. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

Obtaining a client or a server certificate from a CA involves the following steps:

- The grid user requiring certification generates a key pair.When a grid client wants to start a session with a grid recipient.
- The user signs its own public key and any other information required by the CA.
- The signed information is communicated to the CA. The private key remains with the client and should be stored securely
- The CA verifies that the user owns the private key of the public key presented.
- The CA needs to verify the user's identity. This can be done using out-of-band methods.
- The CA creates a certificate by signing the public key of the user, thereby associating a user to a public key. The certificate will be forwarded to the RA for distribution to the user.

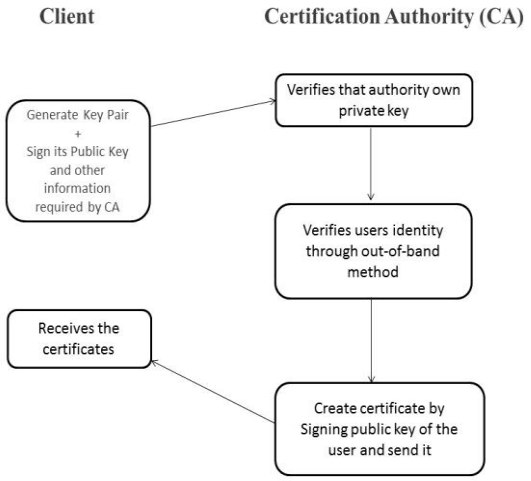


**Fig.4** .Process of obtaining a certificate

- The recipient receives the communication with the certificate and then checks the signature of the Certificate Authority within the certificate. If the signature was signed by a certifier that he or she trusts, the recipient can safely accept that the public key contained in the certificate is really from the sender. This prevents someone from using a fraudulent public key to impersonate the public key owner.

**B. Authorization :**

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. Authorization is important to limit access for security reasons and also to allow only certain users to access the full capabilities of the network to avoid deadlock by flooding control node with processing requests. Like any resource sharing system, grid systems also require resource specific and system specific authorizations. That is why the authorization systems can be mainly divided into two categories:

**a) VO Level Systems:**

A virtual organization (VO) is defined as a dynamic group of individuals, groups, or organizations who define the conditions and rules (business objectives and policies) for sharing resources.VO level grid authorization systems are centralized authorization for

an entire Virtual Organization (VO). These types of systems are necessitated by the presence of a VO which has a set of users, and several Resource Providers (RP).

**b) Resource Level Systems:**

VO level and resource level authorization systems look at two different aspects of the grid authorization. Different resource level authorization Systems are Akenti, Privilege and Role Management Infrastructure Standards Validation (PERMIS), and the GridMap system.

**C. Integrity and Confidentiality :**

There is a need to protect data during transmission on network because anyone connected to an open network may observe, insert or possibly remove message. In a grid computing environment where risk is high, one must ensure integrity and confidentiality of the data being transmitted.

Here are some techniques used for creating secure grids as follows:

1) **Symmetric key encryption:**

Symmetric encryption, also known as secret key encryption, is the one of the form of encryption in which the sender and recipient share a common secret password, pass-phrase or key. The sender uses the key to encrypt plaintext and sends cipher text to the recipient, who, in turn, uses the same key to recover the plaintext. Symmetric encryption is typically faster than asymmetric encryption, but it can't be used unless the sender and recipient have already exchanged keys. Indeed, the main limitation of symmetric encryption is the need to distribute large numbers of keys securely.

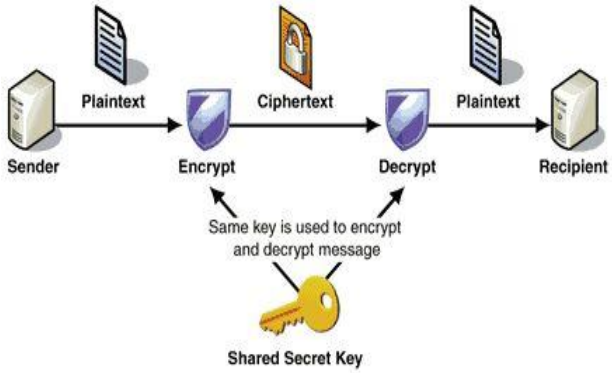


**Fig.4.**Symmetric key encryption using a shared secret key

2) **Asymmetric key encryption:**

This type of system uses two keys. One that is known to everyone, called as public key and the other key, the private key, that is only known to the recipient of the message i.e. one key is used for encryption and the other for decryption. You publish public key to the world while keeping the private key secret. Anyone who has the public key can encrypt the information but cannot decrypt it. Only the person having the private key can decrypt the information. The need of sender and receiver to share secret keys via some secure channel is eliminated; all communication involves only the public keys and no private key is ever transmitted or even sharedA message when encrypted by the public key can only be decrypted by the private key corresponding to the public key.For this reason, public key encryption is often used to securely transmit a symmetric encryption key between the two parties, and all further encryption is performed using this symmetric key.

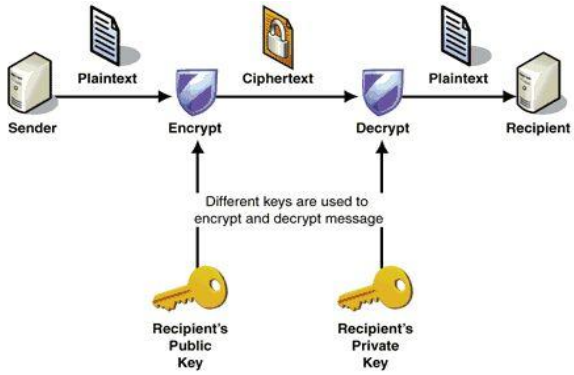


**Fig 5.**Asymmetric key encryption

**CONCLUSION**

Security is one of the major challenges in the Grid Computing architecture, which needs to be addressed very wisely. Resolving security problems with grid computing is one such major challenge. It requires an adequate understanding of both the security issues in grid computing implementation as well as the solutions presently available to address these.In this paper, we have provided a high-level overview of security issues mainly concerned with authentication , authorization, integrity and confidentiality.

**REFERENCES**

[1]. OmerahYousuf, AbRouf Khan, Vairamuthu S(July 2014)“ Improving Data Security and Efficiency in Grid Computing using Object Based Grid Architecture”

[2]. RashmiBhatiya (August 2013) “Grid Computing and security Issues”

[3]. RaafiyaGulmeher,Dr. Mohammed Abdul Waheed (May 2014) “Security Analysis for DataGrid Middle wares”

[4]. Von Welch,FrankSiebenlist ,Ian Foster, John Bresnahan, Karl Czajkowski ,JarekGawor ,Carl Kesselman ,Sam Meder ,Laura Pearlman ,Steven Tuecke “Security for Grid Services”

[5]. Neha Mishra, RituYadavand SaurabhMaheshwari “SECURITY ISSUES IN GRID COMPUTING”

[6]. Muhammad AsifHabib? and Michael Thomas Krieger,JohannesKepler University, A-4040 Linz, Austria “Security in Grid Computing”

[7]. Kamal Jyoti (April 2013 )“Enhanced Amalgam Encryption Approach for Grid Security: A Review”

[8]. NirmalyaMukhopadhyay,AvijitBhowmick ( April 2012 ) “Advanced Authentication Scheme for Enhancing Security Issue in Grid Environment”

[9]. Authentication Systems: Kerberos(online) **Available:**http://www01.ibm.com/support/knowledgecenter/SSNW2F_4.5.1/com.ibm.p8.doc/admin/security/sec_authenticate_ws.html

[10]. Authentication Systems: Secure Sockets Layer (SSL) (online) Avialable:http://docs.oracle.com/cd/B14099_19/core.1012/b13995/ssl_intro.htm

[11]. Symmetric key encryption and Asymmetric key encryption (online) Available: http://www.ustudy.in/node/11858