Research Article Impact Factor: 0.621 ISSN: 2319-507X
Pankaj Washimkar, IJPRET, 2014; Volume 2 (8): 289-300 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A SURVEY OF SECURITY ASPECT IN GRID COMPUTING

MR. PANKAJ UTTAMRAO WASHIMKAR[1], S. R. JADHAO[2]

1. ME Student, Department of Computer Sc. & Engg., Babasaheb Naik College of Engg., Pusad.
2. Associate Professor, Department of Computer Sc. & Engg., Babasaheb Naik College of Engg., Pusad.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Grid computing is collection of computer resources from multiple location to reach a common goal. since this technology allows aggregation of various computer systems for usage by many users to run software's, the data stored on it which may be sensitive and private, remains vulnerable. Grid computing is also a distributed system, so it enables sharing of diverse resources. due to its multi-institutional nature, securing the grid is main challenges in grid computing. In this paper an overview of the grid security fundamentals, technique, models and the major security challenges, requirements and grid security services are studied.

Keywords: Grid computing, security, Authentication, SSH

PAPER-QR CODE

Corresponding Author: MR. PANKAJ UTTAMRAO WASHIMKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Pankaj Washimkar, IJPRET, 2014; Volume 2 (8): 289-300

INTRODUCTION

Grid computing is the aggregation of networked connected computers to form a large scale distributed system used to tackle complex problems. By spreading the workload across a large number of computers, grid computing offers enormous computational, storage and bandwidth resources that would otherwise be far too expensive to attain within traditional supercomputers. So to know grid computing and security it must be necessary to know grid.' Grid' is an instance of a service-oriented architecture, many of the issues which arises here also have a wider application in modern distributed systems [1].

High performance computational grids involve heterogeneous collections of computers that may reside in different administrative domains, run different software, be subject to different access control policies, and be connected by networks with widely varying performance characteristics. The security of these environments requires specialized grid-enabled tools that hide the aspects of the heterogeneous grid environment without compromising performance. Grid [2] computing is similar in structure to standard network computing and peer to peer (P2P).However, there are several differences. Although grids and peer to peer networks are both decentralized distributed computing environments, grid systems tend to focus on top-down issues such as resource allocation, performance and reliability, and security. Peer to peer networks, by contrast, focus on bottom-up issues such as narrowly defined services and support for tens of thousands of simultaneous users. Networks are tightly-controlled and organized, a property which stems from being owed by single entity and managed by one person or one group of people.P2P is less organized than grid computing but more easily scalable.Further,networks and grids are are both administered by centralized security policies. In general, the purpose of security mechanisms is to provide protection against malicious parties. Traditional security mechanisms typically protect resources from malicious users [1].However, in many situations within distributed applications one has to protect oneself from those who offer resources so that the problem is in fact reversed.

Overview of grid computing:

This section gives an overview of the grid computing environment, as well as a brief introduction of the security situations faced in today's distributed computing environment. Conventional security services are in terms of information confidentiality, system integrity, service availability, and commitment accountability [3]. Behavior conformity is an assurance that principals forming a collaborated computing task must each act in conformity with the rules and policy of the collaborated computing; a policy violation should not be easy, e.g. That even a platform owner or a privileged entity should not be able to read the content in a given

memory location on a platform which is even under the full control of the adversary. For another example, the policy can also specify a system integrity protection requirement, in that a malicious operating system should have no way to temper the executable code and data of a trusted process to cause a deceptive execution result to be returned to a service requester. So to enhance the policy term grid gets its superior power and functionality by utilizing synergies resulting from cooperation – i.e. resource owners sharing idle disk space and processor time with users solving complex problem that their own personal resources could not handle. There are three main types of computer grids in use today: computational grids, data grids, and service grids[2].The user of grid, be it computational, data, or service oriented, may have conflicting interests with each other, and thus would want some assurance that their grid-based transactions are safe from the eyes of the other users. The grid is also moving from primary government-and military-based options to more commercialized endowers, such as the recently launched Sun grid which rents time on a preexisting grid infrastructure to users for $1 per hour. with grid becoming more of a commercial resource, users will begin to demand the same level of security out of their grid usage as they do from any computer based commercial tool, such as e-commerce, to reliably deliver adequate results. Without security, a grid setup would is left vulnerable to unauthorized users, malicious processes, and data tampering that could possibly render it useless. With this much interest, security becomes necessary to protect the capital put in to the grid system. Any secure grid environment must employ mechanisms to secure authentication, authorization, data encryption, resource protection, and secure communication. Grid security itself presents several unique security challenges, including managing user identities across local and global networks, managing the diversity of local resource/user security system, end-user key and credential management, and providing security to resource against malicious attack.

3. Security challenges in grid computing:

The security challenges faced in a grid computing can be grouped into three categories: integration with existing systems and technologies, interoperability with different hosting environments e.g., J2EE servers, .NET servers, Linux systems. Trust relationship among interacting hosting environments. Relationship between these categories is as shown in figure1 [1].

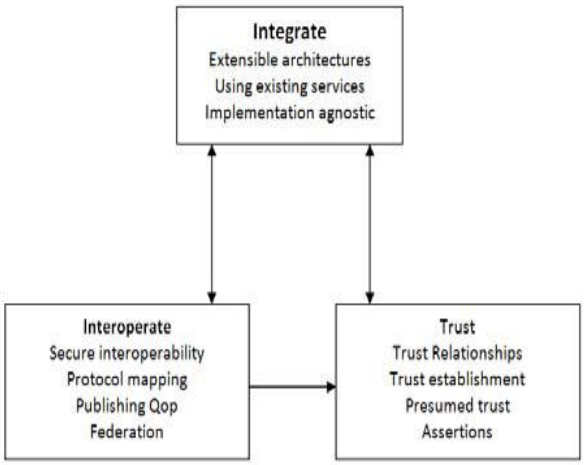

Figure1- Security Challenges in Grid Computing [1].

The integration challenge for both technical and pragmatic reasons, it is unreasonable to expect that a single security technology can be defined that will both address all grid security challenges and be adopted in every hosting environment. Existing security infrastructures cannot be replaced overnight. Similarly, authentication mechanisms deployed in an existing environment that is reputed secure and reliable will continue to be used. Each domain typically has its own authorization infrastructure that is deployed, managed, and supported. It will not typically be acceptable to replace any of these technologies in favor of a single model.

The interoperability challenge needed for services that traverse multiple domains and hosting environment need to be able to interact with each other. At protocol level , it is required mechanisms that allow domains to exchange messages; this can be achieved via HTTP. At the policy level, secure interoperability requires that each party be able to specify any policy it may wish in order to engage in a secure conversion and that policies expressed by different parties can be made comprehensible.

In the simple case, personal knowledge between parties in the VO allows policies to be derived from identifiable trust. An example in current grid systems is the use of certificate authorities to root certificate-based identity mechanisms. For these to work, one must “know” about the trustworthiness of the certificate authority used to establish the identity of a party in order to bind it to specific usage policies[1].

4. Security Requirement in a grid computing:

In order to shield the resources the resources on the grid from unlawful visitation, a reliable privacy, data integrity, data confidentiality, non repudiation, availability, authorization as well as authentication must assured and provided.

4.1 Authorization: For any organization to allow its resources to be jointly shared between all parties involved there is need for authorization as per who should have access any particular resources and who should not. It also allows that permission is given to only the authorized nodes on the network. [6] Globus Toolkit files, VOMSs (virtual organization membership services) are authorization measures usually adopted in grid computing.

4.2 Authentication: Impersonation has been identified as a big threat in a grid environment. Authentication is important to purposely prevent the resources from illegal access. The main purpose of authentication is solely to conform that the user is he who claims to represent and not any other person. In both the shared and personal computer system, authentication is usually carried out with the use of a password and username. It has been established that when a password can be stolen hence the information on the system can be vulnerable. Digital certificates, verified by a certificate authority, are taken as the best way to ensure authentication on the internet [6].

4.3 Availability: Irrespective of security attacks, data must be readily available across the network to satisfy the demand of grid computing user at any point in time. Data availability means that data is available at all times. In a grid computing, data availability is usually achieved through redundancy which has to do with how data is stored and how such data can be reached. Also, essential and adequate services must be made available by a node at any time.

4.4 Data confidentiality: The purpose of the data confidentiality is to protect data from being divulged to the wrong or an unintended party. Two steps can be used to achieve data confidentiality, data encryption, and data decryption. Also, two main types of cryptography can be used to provide data confidentiality they are: Symmetric and Asymmetric [6].

4.4.1 Symmetric: Is known as Single key encryption or secret and private key encryption. In this process, during the encryption/decryption same secret key is used to convert the plaintext into the cipher text and cipher text into plaintext [4].

4.4.2 Asymmetric encryption: In this process, during encryption two keys are used one is public and second private key [4].

4.5 Privacy: The main purpose of privacy is to ensure that information being shared on the grid computing is protected. Every grid user wants his sensitive information to be completely secured from misuse and abuse [6].

4.6 Non-repudiation: Since transaction takes place often on the internet, this security service protects that parties involved in a transaction from denying that a particular transaction has taken place when such a transaction has been carried out. Non repudiation therefore ensure that both the receiver and the sender cannot deny that a message has been sent or received. This security measure can assist in knowing, detecting as well as isolating any node on a grid that is compromised [6].

5. Security provider in grid computing:

To provide security for the grid various aspects are defined which enable the user to protect and secure the content and data.

5.1 Cryptography: To overcome this approaches cryptography are used to provide the security of data and information over the network during transmission of data. In this technique various algorithms provides the different security services, as data integrity, Confidentiality, Authentication etc. Which are all protects against the intruder. Intruder is an attacker who can do modification in messages and release messages on users behalf [5]. Intruder can attack in so many ways on users system to harm them and get the benefit in different ways like to hack some ones web site or users bank account number and password so he can transfer the money easily. If intruder successfully attacks the system he can access user or organization. All the attacks are further divided into two categories: Active attacks and passive attacks, the attack is active when it attempts to alter system resources and try to affect their operation so it compromises with Integrity and Availability. The passive attack are attempt to learn and make use of information from the system but does not affect any system resources, so it compromises with confidentiality [4]. Cryptography is the science of encrypting a plaintext such that it is rendered unreadable to others except the person for whom the message is intended. It involves two processes of encryption and decryption. Encryption: The process of encryption converts the plaintext into encrypted form which is known as the cipher text. Decryption is the process converting cipher text into the original plaintext.

5.2 Single sign on: A user should be able to authenticate once and initiate computation that acquire resources, release resources, and communicate internally, without further authentication of the user.

5.3 Uniform credential/certification infrastructure: Inter domain access requires, at a minimum, a common way of expressing the identity of a security principal such as an actual user or a resource. Hence, it is imperative to employ a standard for encoding credentials for security principals.

5.4 Kerberos: It is used alone or under the distributed computing environment authenticates users through a secure transaction with a centrally maintained key server. Kerberos achieves inter organizational. Kerberos meets many of the basic requirements for virtual organization authentication, but it presents two problems [5]:

- Using Kerberos for inter-site authentication also means using it for intra-site authentication, which is often not feasible because of equipment and staffing costs.
- Site must negotiate many cross-realm authentication agreements, and many sites resist surrendering too much control over local policy.

5.5 Secure Shell:

Secure shell (SSH), a widely used login technology, meets a number of our requirements: It is based on public-key authentication technology, uses link encryption to protect user credentials, and is easily deployed. Users like SSH because it provides basic remote login and file copy capabilities without a lot of complexity. SSH, however, have two significant drawbacks [5]:

- It requires users to manage their own cross site authentication relationships by copying public keys (or keeping track of passwords) for all sites they access, a task that can be burdensome if they access many sites. Moreover, SSH does not give sites control over authorization, so they cannot, for example, deny access to a particular user without invading user privacy.
- SSH supports only limited capabilities-remote shell and file transfer but not others that require authentication such as collaborative environments and web browser.

6. Grid Security Model:

Ensuring the integrity, confidentiality, and security of Web services through the application of a comprehensive security model is critical, both for organizations and their customers, which is the fundamental starting point for constructing virtual organizations. The secure interoperability between virtual organizations demands interoperable solutions using heterogeneous systems. For instance, the secure messaging model proposed by the Web Services Security roadmap [7] document supports both public key infrastructure (PKI) and Kerberos mechanisms as particular embodiments of a more general facility that can be

extended to support additional security mechanisms. The security of a grid environment must take into account the security of various aspects involved in a grid service invocation. A Web service can be accessed over a variety of protocols and message formats it supports.

This is depicted in Figure 2.

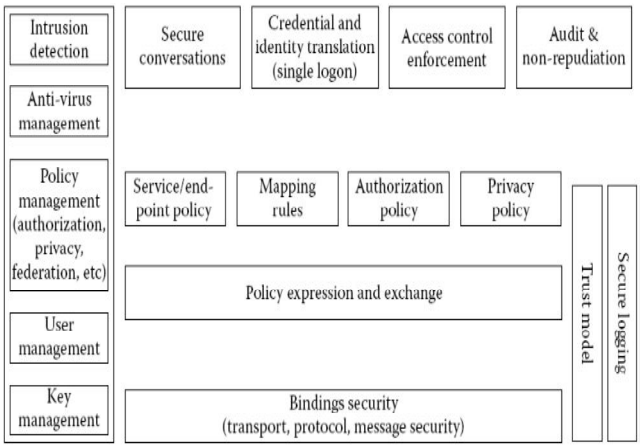

Figure2: Component of grid security model [1].

Each participating end point can express the policy it wishes to see applied when engaging in a secure conversation with another end point. Policies can specify supported authentication mechanisms, required integrity and confidentiality, trust policies, privacy policies, and other security constraints. Given the dynamic nature of grid service invocations, end points will often discover the policies of a target service and establish trust relationships with it dynamically. Once a service requestor and a service provider have determined the policies of each other, they can establish a secure channel over which subsequent operations can be invoked. Such a channel should enforce various qualities of service including identification, confidentiality, and integrity. The security model must provide a mechanism by which authentication credentials from the service requestors' domain can be translated into the service providers' domain and vice versa. This translation is required in order for both ends to evaluate their mutual access policies based on the established credentials and the quality of the established channel.

6.1 Layered Security Model:

Binding Security Layer: Binding security layer deals with transport and message level security. It deals with providing basic security requirements like authentication, confidentiality and integrity of messages when they travel through different domains. The security of a binding is based on the security characteristics of the associated protocol and message format. Grid

services use SOAP to transport message. Security information can be carried in the SOAP message itself in the form of security tokens defined in the WS-Security specification. SOAP messages can also be integrity and confidentiality protected using XML Digital Signature and XML Encryption respectively[8]. Signature and encryption bindings defined in WS-Security can be used for this purpose. Policy Expression Layer: Services have certain requirements that must be met in order to interact with them and those are the service policies.

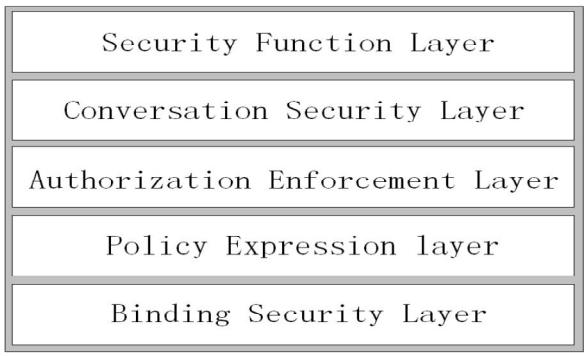

Figure3. A layered security model in hosting environment [8].

A hosting environment should have access to policies associated with a hosted service so that it can enforce the security requirements to protect the service when which is accessed. Because grid is a dynamic environment, it is important for service requestors to discover these policies dynamically and make decisions at runtime. We will adopt WS-Policy specification, which describe how both service providers and service requestors specify their requirements and capabilities. WS-Policy specification is fully extensible and has not place limits on the types of requirements and capabilities that may be described [8].

Authorization Enforcement Layer: Authorization is an important part of the security model. Each service will typically have its own authorization policy to make its own access decisions. Authorization is typically associated with the hosting environment such that it controls access to a service based on the policy of the service. WS-Authorization specification will describe how access policies for a service are specified and managed. In particular it will describe how claims may be specified within security tokens and how these claims will be interpreted at the end-points.

Conversation Security Layer: A service requester and a service provider are likely to exchange more messages and submit requests subsequent to an initial request. In order for messages to be securely exchanged, policy may require service requester and service provider to authenticate each other. In that case, a mechanism is required so that they can perform

authentication and establish a security context. This security context can be used to protect exchange of subsequent messages. The security model adopts WS-Secure Conversation specification to establish security contexts and exchange message securely. WS-Secure Conversation described how to establish mutually authenticated security contexts.

Security Function Layer: Based on the capability provided by the layers above, this layer provides advanced security features like dynamic trust establishment, audit trails, secure logging, management of certificates etc. When deal with security of the trust relationship between two entities in the grid environment, we use WS-Trust and WS-Federation specification. And other features which hosting environment related are provided by inner infrastructure of the hosting [8].

7. Grid architecture:

In grid architecture the dynamic trust is the most important in cross organizational authentication. In this architecture for credential mapping to overcome the heterogeneity problem in different organizations. By using the credential mapping, it is possible to make dynamic and fast trust relationship between the cross organizations regardless of their local security. The grid deals with the authentication tokens. The credential mapping is more secure and fast for the dynamic trust between the cross organizations. The credential mapping is lightweight, integrate and open source service for grids. Drawback of the paper is that it only deals with the authentication token mapping not with the authorization and attribute mapping [7].

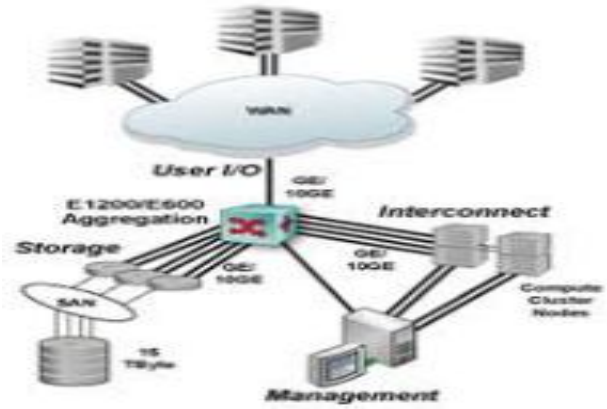

Figure3: Grid architecture[7]

The approach is very much efficient in the sense that authentication and authorization is tackled at different layers. Strength of the paper is that, is that service requestor is discovered by the policies dynamically and make decisions at runtime, which is more suitable in a dynamic

environment like grid [7]. One of the best functionality of this model is that authorizations is performed locally and have thus level of access and the authentication mechanism is treated different based on the authorization level.

The grid computing and technologies address seamless integration of services with existing resources and core application assets. As discussed in the Grid Security Model section, the grid security model is a framework that is extensible, flexible, and maximizes existing investments in security infrastructure. It allows the use of existing technologies such as X.509 public key certificates, Kerberos shared-secret tickets, and even password digests. Therefore, it is important for the security architecture to adopt, embrace, and support existing standards where relevant. Given grid services are based on Web services, grid security model will embrace and extend the Web services security standards proposed under the WS Security roadmap [1].

8. Conclusion:

In This paper various security requirements and also the challenges incur the grid computing i.e. integration, interoperability and trust relationship and the relationship between them. The security architecture and the grid security model are also described in this paper which includes security, model. As grid computing and security is becoming a more and more important area, a number of problems remain un-tackled by the existing grid security solutions. policy and requirement a far is an essential topics for grid security, for any distributed computing where a partner and model applies.

References:

1. Kalra, Sarbjeet and Sukhvinder "Grid Security-an Adaptive Technique". IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010

2. Erin Cody a, Raj Sharman, Raghav H. Rao, Shambhu Upadhyaya "Security in grid computing: A review and synthesis" Available online at www.sciencedirect.com.

3. Haibo Chena, Jieyun Chenb, Wenbo Maoc, Fei Yand "Daonity – Grid security from two levels of virtualization". Available online at 2007 www.sciencedirect.com

4. Kamal Jyoti Enhanced Amalgam Encryption Approach for Grid Security". ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013

5. Prasenjit kumar Patra, Pranshu Saxena, Rajwinder Singh "Different Aspect Grid Security; based on User Authenticity and Message-based Security Service: A Review". International Journal of Computer Applications (0975 – 8887) Volume 67– No.24, April 2013

6. Azeez, tiko, M.venter "Grid Security: Evaluation of active and passive attacks with proposed countermeasures". Research journal information technology3(3)181-190,2011

7. Muhammad naeem khan, Shahid Hussain "Grid Computing Security Implementation Challenges". IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.2, February 2013

8. Zhongping Zhang Kunbo Wang Jianfeng Luan "A Combined Grid Security Approach Based on Web Services Security specification". 2008 ISECS International Colloquium on Computing, Communication, Control, and Management 2008.