International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016
ISSN 2229-5518

Security Issues in Grid Computing

Akanksha[1], Dr. Kanwal Garg[2]
Scholar[1], Assistant Professor[2]
Department of Computer Science & Applications, Kurukshetra University, Kurukshetra[1, 2]
akanxa9@gmail.com[1],gargkanwal@kuk.ac.in[2]

Abstract: **The premise of this paper is to specify the security requirements of grid computing. The dynamic nature of Grid environments introduces challenging security concerns that demand new technical approaches. In this brief overview the author provides key Grid security issues and outlines a new method to resolve architectural level issues in grid environment. The frequent itemset mining in grid environment provides resources to transform data into useful sequences by providing front end accessing and done in most secured manner.**

Keywords: Grid Computing, Authentication, Authorization, Security, OGSA, Virtual Organization (VO).

1.Introduction: Grid computing is emerging as a viable option for high-performance computing, as the sharing of resources provides improved performance at a lower cost than if each organization were to own its own "closed-box" resources [1]. According to Foster and Kesselman a grid is a system that conforms to three specific categories: it coordinates resources that are not subject to centralized control, it uses standard, open, general purpose protocols and interfaces, and it delivers nontrivial quality of service. Kon et al define grid computing as, "coordination of resource sharing and dynamic problem solving in multi-institution virtual organizations [2]. The goal of grid networks is to integrate all of hardware and software capabilities of the different sets of computers as a comprehensive system, in order to calculate and process data. Grid computing is defined in literature as "systems and applications that integrate and manage resources and services distributed across multiple control domains" [3].

A common scenario within Grid Computing is the formation of dynamic" virtual organizations" (VOs) comprising group of individuals and associated resources and services united by a common purpose but not located within a single administrative domain. The need to support the integration and management of resources within such VOs introduces challenging security issues. Research in grid computing is producing solutions to some of these problems based around not direct inter organizational trust but rather the use of the VO as a bridge among the entities participating in a particular community or function [4].

1.

2. Security Requirements: Security is a latest topic for the smart grid, and progresses are being done in this field every day. Most of the communications use standard cryptographic algorithms AES-128 to protect the data on the network. Grid computing is a technique which provides high performance computing [5].

In Grid computing resources are shared in order to improve the performance of the system at a lower price. Grid systems & applications require standard security functions which are authentication, access control, integrity, privacy and no repudiation. Authentication and access control issues are following:-

It provide authentication to verify user's computation and resources used by the processes to authenticate.

It allows local access control mechanisms to be used without change [6].

Single Sign On: A user should authenticate once and they should be able to acquire, use them, and release them and to communicate internally without any further authentication.

Protection of credentials: User passwords, private keys etc. should be protected.

Interoperability with local security solutions: Access to local resources should have local security policy at a local level. Despite of modifying every local resources there is an inter domain security service for providing security to local resources.

Exportability: The code should be exportable i.e. they cannot use a large amount of encryption at a time. There should be a minimum communication at a time.

Support for secure group communication: In a communication there are no. of processes which coordinate their activities. This coordination must be secure and for this there is no such security policy.

Support for multiple implementations: There should be a security policy which should provide security to multiple sources based on public and private key cryptography [7].

3. Grid Security Challenges: Two organizations, A and B, each operate their own corporate security solutions that address certification, authentication, and authorization. Between the two organizations, however, no trust relationship exists. Assume that an entity in sub domain A1 wishes to access a resource managed by another individual in sub domain B1 in collaborative activity.
Multiple resources provide the control policies to the third party. The VO is one which coordinates the resource sharing and use. The dynamic policies and entry of new participants in the system gives the need for three key functions which are:

Multiple security mechanisms: Organizations which participate in a VO have investment in security mechanism and infrastructure. Grid security interoperates with these mechanisms.

Dynamic creation of services: Users must be able to create new services (e.g., "resources") dynamically without administrator permission. These services should coordinate and interact with other services. So, we must be able to name the service with acceptable identity and should be able to grant rights to that identity without any contradiction with the governing local policy.

Dynamic establishment of trust domains: VO needs to establish coordination between its user and all the resources so that they can communicate easily. These domains must establish trust dynamically whenever a new user join or leave a VO. A user-driven security model is needed to create new entries of the user so that they can coordinate with the resources within the VOs [8].

Distributed data: The data to be mined is stored in distributed computing environments on heterogeneous platforms such as grids. Both for technical and for organizational reasons it is impossible to bring all the data to a centralized place. Consequently, development of algorithms, tools, and services is required that facilitate the mining of distributed data.

Distributed operations: In future more and more data mining operations and algorithms will be available on the grid. To facilitate seamless integration of these resources into distributed data mining systems for complex problem solving, novel algorithms, tools, grid services and other IT infrastructure need to be developed.

Massive data: Development of algorithms for mining large, massive and high-dimensional data sets (out-of-memory, parallel, and distributed algorithms) is needed.

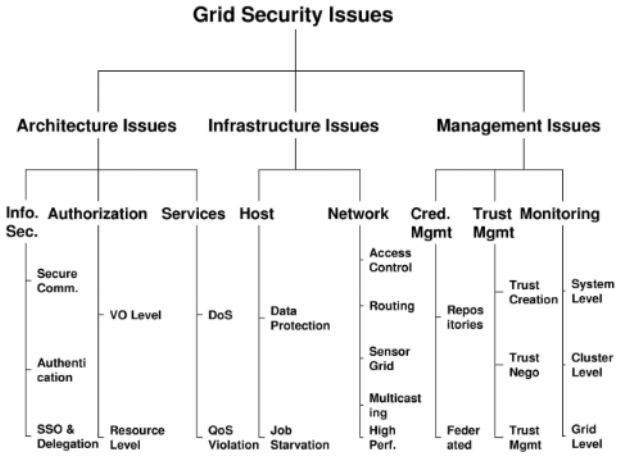
Complex data types: Increasingly complex data sources, structures, and types (like natural language text, images, time series, multi-relational and object data types etc.) are emerging. Grid-enabled mining of such data will require the development of new methodologies, algorithms, tools, and grid services.

Data privacy and governance: Automated data mining in distributed environments raises serious issues in terms of data privacy, security, and governance. Grid-based data mining technology will need to address these issues.

User-friendliness: Ultimately a system must hide technological complexity from the User. To facilitate this, new software, tools, and infrastructure development is needed in the areas of grid-supported workflow management, resource identification, allocation, and scheduling, and user interfaces.

4. Grid Security Issues: The issues and concerns that we had for personal safety, trust, authorization, etc. are important issues for grid computing systems as well. A grid system is a mechanism to pool resources on-demand to improve the overall utilization of the system [9]. The grid security issues can categorize into three main categories:-

- Architecture Issues
- Infrastructure Issues
- Management Issues



TAXONOMY OF GRID SECURITY ISSUES

Architecture Related Issues: These issues address the affairs pertaining to the architecture of the grid. The users of the grid are concerned about the data powdered by the grid and hence there is a need to protect the data confidentiality and integrity as well as the user validation [10]. Architecture level issues may include issues like information security, authorization and service level security which destabilize the whole system. Grid systems require resource specific and system specific authorizations. It is important mainly for systems where the resources are shared between multiple departments or organizations. The authorization systems are of two types: Virtual organization level systems and resource level systems. Virtual organization level systems have a centralized authorization system which provides credentials for the users to access the resources and resource level systems allow the users to access the resources based on the credentials presented by the users. The grid service level security issues are of two types: QoS Violation Issues and DOS (Denial-of-Service) related issues. The QoS violation issue is about the forced Qos violation by the adversary through congestion, slowing or dropping packets or through resource hacking. The Denial-of-Service is more dangerous where the access to a certain service is denied [11].

Infrastructure Related Issues: These issues are related to the network and host which are found in the grid infrastructure. Host level security issues are individual's issues that make a host apprehensive about affiliating itself to the grid system. The issues that are related to the infrastructure may include data protection, job starvation, and host accessibility [12]. Grid computing infrastructure must address several potentially complicated areas in many stages of the implementation. These complications arise in the areas of security, resource management and information services and data management. The infrastructure related issues are of two types: host security issues and network security issues. The host level security issues are those issues that make a host comprehensive about affiliating itself into the grid system .The main sub issues include data protection issues and job starvation [11].

Management Related Issues: The third set of issues relate to the management of the grid. Managing pass is absolutely important in grid systems because of the mixed nature of the grid frame and applications. The different management issues are related to scheduling, rescheduling, monitoring, auditing and logging. Management of trust is very difficult in a dynamic grid scenario where grid nodes and users join and leave the system. Monitoring of resources consists of different stages such as collection, processing, transmission, storage and presentation of the data.

5 Grid Security Areas: The main methods for the above discussed grid security challenges and issues are following:-

Authentication: Most security considerations in grids are focused on the authentication and authorization to access the available resources on the grid. From a usability point of view to access the grid and all its resources users should enter their login credentials only once. This single-sign-on approach to access the heterogeneous and distributed environment of grids is a corner stone of the success and further growth and distribution of grids [13]. Using public key infrastructure (PKI) based on X.509 certificates has become the standard for grid middleware – like Globus or gLite – to implement the single-sign-on approach. The usage of this PKI establishes a mutual trust relationship between the user and the entry point to the grid allowing not only the grid to check the user's certificate but also vice versa allow the user to verify the entry to the grid via it's certificate. In addition to this basic authentication the middleware Globus and gLite use a user proxy approach to delegate the credentials to the systems either used

for computations by the user or the user's processes or containing data required by the user or the user's processes. Using a proxy the user delegates the rights to it, which again can delegate the rights to processes started by the user and needing to access other systems of the grid infrastructure. To avoid the exposure and publication of the user's credentials the proxy uses its own credentials which are only valid for short period of time, usually for about 12 hours. In Globus and gLite this user-mapping is based on grid map-files. In Globus and gLite the access to resources can also be limited by requiring users to be members of virtual organizations (VO). By restricting the access to systems of the grid infrastructure to special VOs, only members of those VOs are authorized to access them [14].

Scheduling: The scheduling of jobs and managing a job's access to data, especially if the executed process is very data intensive [15], is an important topic in grid computing. Processes running in grid environments do not only require CPU time but also bandwidth and data storage, which should be reserved for the processes. Due to the structure of grids and resources which are managed, distributed scheduling of tasks improves the scheduling performance and according to makes a system portable, secure, and capable of distributing scheduling workload among an array of computational sites in the system.
In a scheduling approach is presented, where the discrepancy between the requested security levels and offered security levels influences the scheduling of jobs on the grid. The mapping from global user accounts to local user accounts on computing elements of a grid may lead to such deficiencies, which have to be considered at scheduling time, so that sensitive data or computations may not be modified or accessed by unauthorized users.

Globus Toolkit Security Model: The Globus Toolkit's Authentication and Authorization components provide the basis standard for the "core" security software in Grid systems and applications. Globus software development kits provide programming libraries, Java classes, and essential tools for a PKI, certificate-based authentication system with single sign-on and delegation features, in either Web Services or non- Web Services frameworks. Grid security technology such as GSI and CAS are used to provide security. These technologies are used to represent the security and are used in various grid projects. Web security services work under the OGSA architecture. It is used to represent refactoring, refinement and repacking of various Grid protocols so that better use of useful resources can be done [17]. OSGA is used with the Globus toolkit to provide WSDL for interface to provide Grid services. OOSGA is also used to provide an interface for discovery of grid services. Recent goal of OSGA security work is to provide relationships between OSGA security mechanism and emerging WS security mechanism.

6. Proposed methodology:

In this research work the author verifies the main security issues and works on architecture level issues. As architecture level issue is composed of information security, authorization and service level security; to control these security issues the researcher provides a method which is the combination of Authentication and GT4 model.

To control the illegal users to access the Grid environment is the major challenging aspect as grid is virtual environment in which multiple organizations can access each other's resources, databases etc. So to maintain who can do what and who can access what including the owners of individual resources and also the users who initiate data processing is the major task. Authentication is a process in which the credentials provided are compared to those on file in database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. On the systems themselves the grid users are mapped to local user accounts, which allow the execution of the requested jobs and access to data necessary for the execution of the request. In Globus and gLite this user mapping is based on gridmap-files. The Globus toolkit software is a set of libraries and programs that address common problems that occur when building distributed system services and applications. GT4 model is based on Grid Resource Allocation Management **(GRAM)** which provides a web services interface for initiating, monitoring, and managing the execution of arbitrary computations on remote computers.

A complete security solution must always be a system that combines components concerned with establishing identity, applying policy, tracking actions etc. to meet specific goals. For this the users must authenticate themselves to make sure that their access is completely legal. Now if the user is authenticated user and all his information matches with the existing database then

GT4 model will work for protection of architectural level issues.

GT4 is highly standards-based security components in which at lowest level the implementation of credential formats and protocols that address message protection, delegation etc. In this each user and resource is assumed to have a X.509 public key credential. Hence entities validate each other's credentials, establish a secure channel for message protection and to create and transport delegated credentials that allow remote users to access resources, databases etc.

Frequent Itemset Mining in Grid Environment: For efficient knowledge discovery data is transformed into useful patterns, aiding comprehensive knowledge of the concrete domain information. For this data mining process is to be deployed in grid environment. Grid framework provides easy to use front end for accessing a distributed system supporting complex operations. Grid furnishes necessary resources to deploy a state of the art distributed patterns recognition applications. As in grid environment authenticated access of users is allowed then the mining of frequent itemsets would become secure. Let us take an example of Online Shopping the frequent patterns are arranged in grid environment. The mining of frequent patterns is done with the help of market basket analysis process as it is an important component of analytical system in retail organizations to determine the placement of goods, designing sales promotions for different segments of customers to improve customer satisfaction and hence increase in profit of organization.

C**onclusion:** Grid computing has become a hopeful way for distributed supercomputing from its very beginning and attracts many attentions worldwide. There are many ways to access the resources of a computational grid and each method is associated with a unique security requirement and it also has implications for both the resource user and the resource provider [11]. This paper contributes to the overall body of research concerning security in grid computing & provides an overview of security issues concerned with authentication scheduling and globus toolkit security model. The researcher further proposes a method to resolve the architectural level issues problems by using authentication and GT4 model. The author defines the frequent itemset mining in grid environment by taking example of online shopping. Further strong authentication procedures must be developed in future for the sake of security of resources in the grid environment.

7. References

[1] A.R. Butt, A. Sumalatha, N.H. Kapadia, "Grid computing portals and security issues" , Journal of Parallel and Distributed Computing 63 (10) (2003) 1006–1014.

[2] I. Foster, K. Kesselman, "The Grid: Blueprint for a Future Computing Infrastructure" (Morgan Kaufmann in Computer Architecture and Design), 1999.

[3] M. Humphrey, M.R. Thompson, K.R. Jackson, "Security for grids", Proc. of IEEE 93 (3) (March 2005) 644–652.

[4] Ian Foster, Frank Siebenlist, Steven Tuecke, Von Welch, "Security and Certification Issues in Grid Computing" retrieved on 28th March, 2016 from https://pdfs.semanticscholar.org/115d/c00ae0551636e2c1f691849f06ae70657ced.pdf.

[5] Neha Mishra , Ritu Yadav and Saurabh Maheshwari, "Security Issues in Grid Computing", International Journal on Computational Science & Applications (IJCSA) Vol. No.1, February 2014.

[6] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, June 17, 2009 [online] Available: http://www.nist.gov/smartgrid/InterimSmartRoadmapNISTRestructure.pdf .

[7] Ian Foster, Carl Kesselman & S Tuechkor (2001), "The Anatomy of Grid: Enabling Scalable Virtual Organization" retrieved on 29th March, 20016 from http://toolkit.globus.org/alliance/publications/papers/anatomy.pdf.

[8] Energy Assurance Daily, Sept 29,2007,US Department of Energy, Office of Electricity Delivery & Energy Reliability, Infrastructure Security & Energy Restoration Division 28th March, 2016.

[9] A. Chakarbarti, "Taxonomy of Grid Security Issues" retrieved on 24th March, 2016 from

http://link.springer.com/chapter/10.1007%2F978-3-540-44493-0_3#page-1.

[10] Globus Alliance: 2008, “GT 4.0 Reliable File Transfer (RFT) Service”, March 2008.

[11] R. Geetha & D. Ramyachitra, “Security Issues in Grid Computing”, International Conference on Research Trends in Computer Technologies, Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887), 2013.

[12] Anirban Chakrabarti, “Grid Computing Security (GCS)” , 2008.

[13] Muhammad Asif Habib and Michael Thomas Krieger, “Security in Grid Computing”, Johannes Kepler University, A-4040 Linz, Austria, 2008.

[14] Butler, R., Welch, V., Engert, D., Foster, I., Tuecke, S., Volmer, J., Kesselman, “C.: A National-Scale Authentication Infrastructure”, Computer 33(12) 60–66, 2000.

[15] Kim, B.J., Hong, S.J., Kim, and “Ticket-based fine-grained authorization service in the dynamic VO environment”, In: SWS ’04: Proceedings of the 2004 workshop on Secure web service, New York, NY, USA, ACM (2004) 29–36.

[16] Xue, Y., Wan, W., Li, Y., Guang, J., Bai, L., Wang, Y., Ai, J, “Quantitative retrieval of geophysical parameters using satellite data”, IEEE Computer 41(4) (2008) 33–40.

[17] EGEE JRA3 team, “EGEE Global Security Architecture for web and legacy services”, EU Deliverable DJRA3.3 (2005).