International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:4, 2010

Fortification for P2P Grid Computing Used for Resource Discovery

Bhawneet Singh Marwah, Rishabh Rastogi and Shinon Kochar

***Abstract*—**Grid computing provides an effective infrastructure for massive computation among flexible and dynamic collection of individual system for resource discovery. The major challenge for grid computing is to prevent breaches and secure the data from trespassers. To overcome such conflicts a semantic approach can be designed which will filter the access requests of peers by checking the resource description specifying the data and the metadata as factual statements. Between every node in the grid a semantic firewall as a middleware will be present The intruder will be required to present an application specifying there needs to the firewall and hence accordingly the system will grant or deny the application request.

***Keywords*—**Grid Computing, Metadata, Semantic, Peers, Resource Discovery, Firewall.

I. Introduction

GRID computing is the emerging technology which is enabling massive parallel sharing of resources in a peer to peer network [1]. Various resource discovery mechanisms are being developed in the exemplar of distributed systems. Goal of almost every mechanism is efficient and effective resource management in fault tolerant and scalable manner. The term peer refers to the fact that every node is of equal weight age despite of any hierarchies in the overall grid system. In this system the nodes can spontaneously collaborate without the intervention of the central coordination system. This helps in development of highly scalable and dynamic grid. Peer to peer grid or p2p grid provides two functionalities i.e. node management or peer management and resource discovery[2].Since in the real world of computing the environment is heterogeneous and highly unpredictable therefore the underlying mechanism are suppose to be highly optimized and scalable to prevent any illegal intrusion of malicious agents in the grid. The grid by its own nature involves access to computer systems and data outside ones own company or institution .Goal of almost every mechanism is efficient and effective resource management in fault tolerant and scalable manner conference page limits. [3]

Bhawneet Singh Marwah is in Lingaya's Institute of Management and Technology (Department of Computer science and Engineering), Old Faridabad, Haryana, India (phone: +9109953036123; e-mail: bhawneet.marwah@gmail.com).

Rishabh Rastogi is with the Lingaya's Institute of Management and Technology (Department of Computer science and Engineering), Old Faridabad, Haryana, India (phone: +9109990911947; e-mail: xyzrishabh@gmail.com).

Shinon Kochar is with the Lingaya's Institute of Management and Technology (Department of Computer science and Engineering), Old Faridabad,Haryana,India(phone:+9109871848724;email:shinondelhi@yahoo.co.in.

II. Peer To Peer grid computing

Peer to peer grid computing involves a mesh in which there the term peer refers to the fact that every node is of equal potential despite of any hierarchies in the overall grid. In this system the nodes can spontaneously collaborate without the intervention of the central coordination system. This helps in development of highly scalable and dynamic grid. Peer to peer grid or p2p grid provides two functionalities i.e. node management or peer management and resource discovery. P2P systems are more popular for file sharing e.g. Bit Torrent. These systems are also used for real time transfer; Skype is a famous example of telephony. The participation of any user in P2P environment is highly dynamic since any user can join the environment [4].

From a common desktop and request for shared files or telephony connection. Therefore the way of participation is unpredictable and highly dynamic as participants can join,

Unsubscribe or rejoin at any time. Usually resource discovery queries in P2P systems are not attribute dependent as in most of the Grid systems but discovery is done either by the file name specification or range queries.

III. Security issues in P2P Grid

The multi-institutional nature of grid environments introduces challenging security that demands new technical approaches. Security requirements within the Grid environment are driven by the need to support scalable, dynamic, distributed virtual organizations. Computer security systems are designed to overcome following types of threats such as an intruder reading your confidential data as well as manipulating it, denial of services to genuine users, an intruder using your system to launch third party attacks and using your data for nefarious purposes [5].

IV. Drawbacks in The conventional Method TO implement grid security

To implement in-depth security in the grid systems a proxy chain policy is used for example, Globus [6] was designed to use encryptions in authenticated communication between the peers. In this system users must authenticate themselves using a PKI certificate when they logo onto a Globus grid [7].

For maintenance of transparency and especially performance Globus application are allowed to spawn new process without an authenticated communication direct from the user whereas each process is provided with a proxy

certificate allowing it to initiate and sign its own communication. This proxy certificate is signed by the parent process and the first (login) process is signed by the user, so the chain of proxies can be treated back to user and is considered to be under the users control [7].Thus allowing the uploading and running the user's code on the machine in which they have to access as illustrated in figure 1[6]

The degree of trust placed in the users and the proxies makes all participants and users of such a grid vulnerable if any node is compromised. This approach thus provides limited rings of security as a matter of fact if users own key pair, or grid infrastructure software or any other user defined application process, or any sites on which the user's application executes is compromised then the resulting intrusion is immediately serious and yet may be almost impossible to detect. Hence it is desirable to come out with a technique which uses policies so as to filter by using the data and the metadata such as semantic firewall [7].

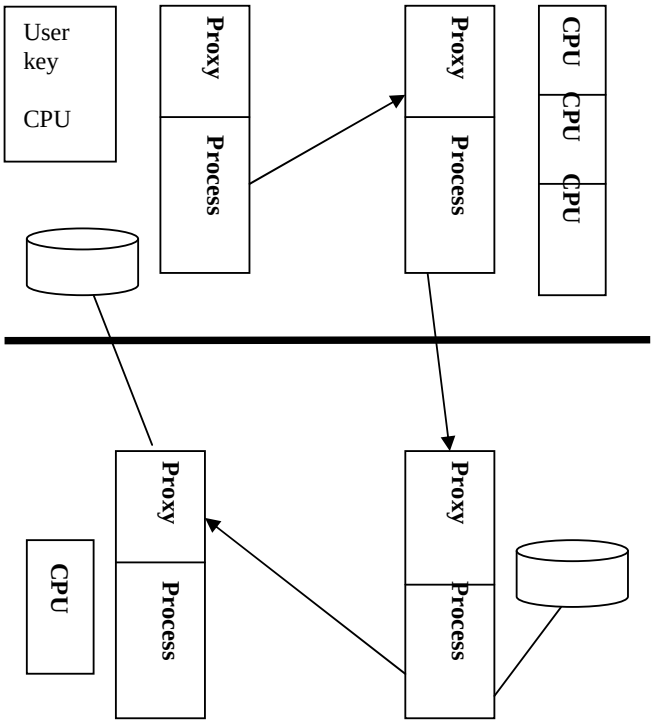

Fig. 1:A Grid Certificate Policy for Proxy Chain

V. SEMANTIC APPROACH IN FIREWALL

One of the greatest challenges faced in Grid Computing regards the ability to unequivocally share and deploy knowledge to be used for the development of innovative Grid infrastructure, and for Grid applications. To address this challenge the semantic firewall should be deployed in between the peers who will produce the technological infrastructure for the rapid prototyping and development of knowledge-intensive distributed open services for the grid. The results are aimed at developing grid systems that optimize cross-process, cross-company and cross-industry collaboration, which the firewall will show by adopting a use case-guided development and evaluation strategy based on the data provided by the intruding user to the firewall as mandatory policy and thus the firewall exploits the data and the metadata to check the validity of the intrusion. This system is so called because it will exploit semantic web techniques and use machine reasoning about the data messages. The main idea behind this system is that the user application will no longer be responsible for management of the grid security rather these application will provide a profile describing their needs to the semantic firewall which will be devised at a local or a remote site .this will be mandate to all the agents in the network to provide crucial data as matter of policy for securitization process of the firewall [8].

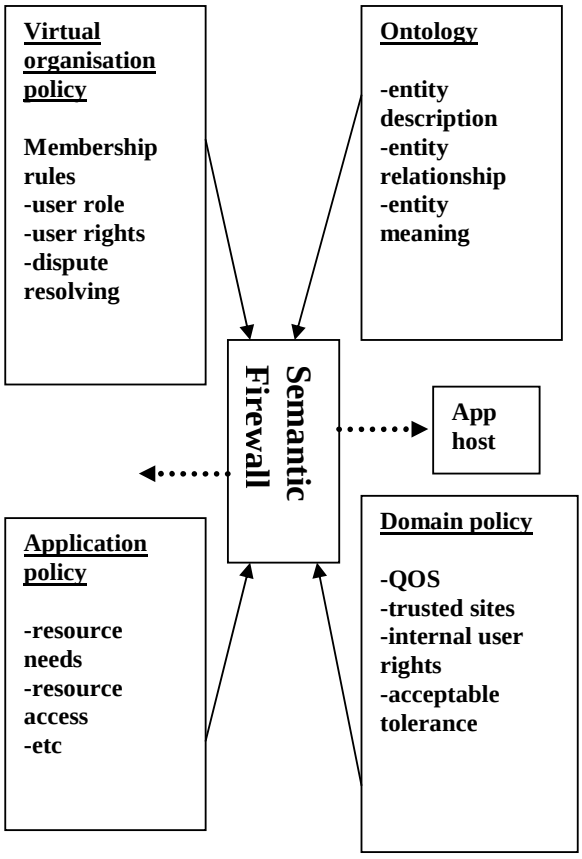

Fig. 2:Policy Description in Semantic Firewall

The figure 2 shows the various controlling features in the semantic firewall. in totality the semantic firewall checks the facts and by the process of machine reasoning it scrutinizes whether the intrusion is acceptable or not. This forms the resource description schema for the firewall. The body of knowledge modelled by a collection of statements may be subjected to reification, in which each statement including the subject, predicate and the object are assigned a domain policy and treated as a resource about which additional statements can be made, as in "BOB says that ALICE is the author of document ALPHA". Now here the validity is checked by the sematic firewall and if it finds the facts, data and metadata to be trustful then it allowed using the various resources of the p2p grid. In the due course of the resource discovery, this

includes massive computation, database, application software and etc [9].

VI. Algorithmic APPROACH TO the proposed securioty system in the P2P grid

The following procedure can be used to develop a semantic firewall for P2P gird so that security issues are in control

A. Function to implement the network policy rules in the grid engine

Step 1: Initialize The Grid engine and check if all the nodes are working properly.

Step 2: Initialize function ADD_FILTER(IPfilter),this will be the very first line of guard for the intruding peer.
Step 3: Add the filter rule to the grid engine driver by passing the parameter as IP filter.

Step 4: Initiate function verify_IP(IPaddress),the purpose of this function is to verify the validity of the IP address. The function keeps track of the dangling IP addresses also in a holistic environment where the router keeps changing the IP addresses on every clock pulse.

Step 5: If the input string IPaddress contains any invalid entry like a alphabet or any other symbol then report a threat and abort immediately.

Step 6: As a container class, run the function Purpose_of_intrusion (parameters), the parameters passed in the function are the LOG FILE, SCRIPT FILE, MAC ADDRESS, RESOURCE. Here the resource signifies the available resources in the node .If the intruding node demands some resources then the host node will scrutinize each and every resource requirement and if it has the same then it will further check the intruding node's LOG FILE to asses the previous behavior

Step 7: A socket programming is done in the class wizard to access the lowest level of the network at the session layer. The socket program acts as kernel security injector between the parallel processes.

The above steps can be implemented in Visual C or in java. This can made to run in a Linux environment where the open source allows manipulating the kernel by socket programming.

VII. Advantages of semantic firewall over proxy certifi cate security system

Semantic firewall is more scaleable due to the fact they have cohesive checking of the dynamic collections of resources that require p2p and bidirectional event notification.

The semantic firewall easily detects threats in the high performance UDP whereas in the proxy certificate system it is very difficult to do so.

VIII. Conclusion

In this paper we tried to define the emerging field of grid computing with a new peer to peer approach for highly scalable and extensive resource discovery grid along with the security glitches in the proxy certificate system. We stated the reasons citing the importance of semantic firewalls and there method of tackling the network intrusion as compared to the traditional proxy certificate system. We hope that other researchers would be benefited from our work and could utilize the information provided to mix with their research works.

References

[1] www.cs.mu.oz.au/research/dc.html [online].
[2] F Berman, G Fox, AJG Hey, 2003 - books.google.com[book]
[3] http://www.jimpinto.com/writings/grid.html
[4] www.skype.com [online].
[5] "Secrets and lies : Digital Security in a Networked World", John Wiley & Sons ,2000(ISBN 0-471-25311-1) [book]
[6] The Globus project is described in: I Foster Kesselman," GLOBUS: A METACOMPUTING INFRASTRUCUTRE TOOLKIT", In J supercomputer applications, 11(2):115-128,
[7] www.globus.org[online]
[8] http://www.semanticgrid.org/links.html[online]
[9] http://www.cs.cmu.edu/afs/andrew.cmu.edu/usr/shadow/www/afs.html#general .[online]