An Overview of Trust Models for Resource Selection in Grid Computing

Vivekananth.P
Lecturer, IT Dept,
St Joseph College of Engineering & Technology,
Dar-Es-Salaam, Tanzania

ABSTRACT

Grid computing is distributed computing taken to the next evolutionary level. It facilitates the sharing of computer resources, allowing users to discover and use remote resources. The goal is to create the illusion of a simple yet large and powerful self managing virtual computer out of a large collection of connected heterogeneous systems sharing various combinations of resources. Users who are going to utilize the resources are not having any explicit control over the resources. A central problem for grid services is how to gain confidence that a remote system is performing in accordance with their norms. The effective and competent exploitation of grid computing services needs sophisticated and secured resource management systems. The wide range of selection and the high degree of strangeness leads to the problem in secured selection of resources grid. Without the assurance of a higher degree of confidence relationship, efficient resource allocation and utilization cannot be attained. In recent times, with larger applications in ecommerce and on-line communities, reputation mechanisms have become one of the most important techniques underpinning the distributed application and system safety. We have proposed a new approach in this paper, which intends to offer trust and reputation provide a measure for resource selection in grid computing.

1. INTRODUCTION

Grid computing is a coordinated resource sharing and problem solving in any dynamic environment. Computing resources are highly heterogeneous. Grid computing and its related technologies will only be adopted by users, if they are confident that their data and privacy are secured and the system must be as scalable, robust and reliable as of their own in their places. Reliability is the probability that a process will successfully perform it's prescribed task without failure at a given point of time. So allowing reliable transactions plays a vital role in grid computing. In the open Grid environments, it is necessary to build the mechanism of evaluating reputation especially after the combination of Grid computing and economy.

Resources and security guarantee are the two fundamental requirements in Grid applications. Coordinated resource sharing and problem resolving in dynamic, multi institutional virtual organizations are the actual and specific problems which underlies the concept of grid. Once infected shared grid resources through malicious codes planted by intruders possibly will spoil other applications running on the same Grid platform. The concerned sharing is not primarily file exchange but rather direct access to computers, software, data and other resources since it is required by a range of collaborative problem-solving and resource-brokering strategies emerging in industry, science and engineering.

The resources in Grid are shared in a flexible, coordinated and secured manner. Most of the Grid applications involve very large data bases with highly secured data. Security requires the three fundamental services: authentication, authorization, and encryption. A grid resource must be authenticated before any checks can be done as to whether or not any requested access or operation is allowed within the grid. Once the grid resources have been authenticated within the grid, the grid user can be granted certain rights to access a grid resource. But within the grid application the one who uses the resource also needs reliable and secure services. The reliability of any transaction is the probability of successful running or completion of a given task. So there is a need of trust system which ensures a level of robustness against malicious nodes. Trust must be established from both the sides.

The rest of the chapters are organized as follows. Section 2 explains about the trusted systems. Section 3 discusses it's requirements for grid resource selection . section 4 discusses the concept of trusted computing which can be used for resource selection , section 5 discusses about literature survey ,section6 talks about the model which uses trusted computing for resource selection and section 7 is the conclusion part.

2. TRUSTED SYSTEMS

The three important features of any trusted system are as follows.

- Complete mediation: Security rules are enforced on every access, not only for selected accesses.
- Isolation: The reference monitor, who is the controlling element in the hardware and the operating system of a computer, regulates the access of subject to object on the basis of security parameters. It protects data from unauthorized modification. That is known as isolation.

- Verifiability: The reference monitor correctness is verified. [4]

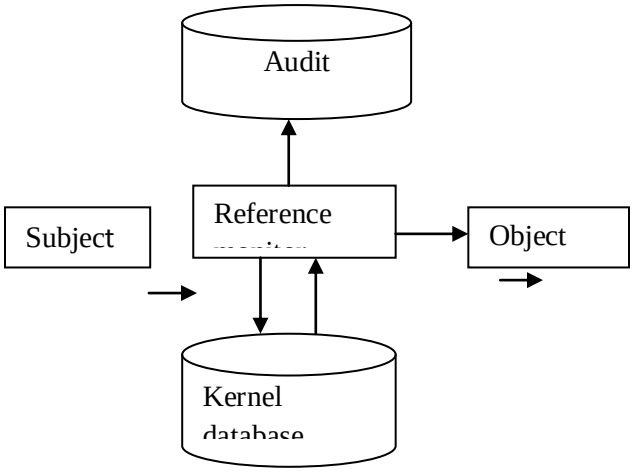

Figure 1. Trusted System

Reference monitor enforces the property of complete mediation isolation and verifiability. Trusted system gives security for data and resources. This trusted system concept serves as the core for the trusted computing model.

3. TRUST REQUIREMENTS ON THE GRID

To find out the trust requirements consider the following scenario:

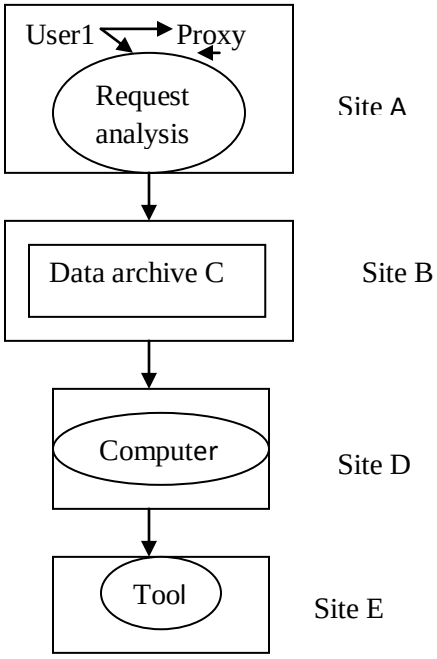

Figure 2. Scenario for trust requirement

An engineer with in organization A wants to perform an analysis on a material. By accessing a data portal at site B, he discovers a suitable data set held by data archive C. The analytical tools are provided at university D with in his virtual organization. She initiates the analysis by passing the reference to the data set from B to D which is then accessed by the analysis tools. D determines that it does not have computational resources available and determines that a computer is available at different institution E and delegates part of job there. However the analysis takes several hours so the engineer has established a user proxy agent to represent him. This particular analysis involves five sites A,B,C,D,E.

This scenario highlights the following features of the grid, which are relevant to trust:

- Using the grid requires the collaboration of resources that are controlled by different institutions. They have their own allocation policy.
- Since the allocation is purely dynamic the resources are not aware of future requirements.
- Every user may take different role in different domains.
- Mutual trust must be established between different resources.
- The entities may not be aware of other entities to whom the resources are going to be provided.
- The decision policy may be different . Different threshold values may be maintained by different entities.
- Users may delegate their job to some body else (proxy)

4. TRUSTED COMPUTING

Trusted computing can be defined as the desired and conformable system behavior, which is not only established and maintained in a platform environment, but can also, be attested to a remote challenger.

The trusted computing group describes the "technical trust" as an entity which can be trusted if it always behaves in the expected manner for the intended purpose. A trusted computing system can be defined as a system in that cannot be illegally accessed by any one or compromised by viruses. The system provides valet proof user authentication and protection of data. A trusted computer implies not only secure software but also built in security hardware. The total protection in this system lies on hardware, software and firmware.

Trusted Computing (commonly abbreviated TC) is a technology developed and promoted by the Trusted Computing Group (TCG). The term is taken from the field of trusted systems and has a specialized meaning. In this technical sense, "trusted" does not necessarily mean the same as "trustworthy" from a user's perspective. Rather, "trusted computing" means that the computer can be trusted by its designers and other software writers not to run unauthorized programs and to behave in an anticipated way.[2]

Trusted computing is somewhat controversial technology. Advocates of the technology claim that it will make computers safer and most reliable from end user perspective. But opponents on the other side believe that the technology puts too much power and control in the hands of trusted computing. System designers and users lose their anonymity in their on line transactions. Even though there are certain pitfalls in the Trusted Computing technology , We believe that used with caution and circumspectum it can solve the security problems to a larger extent, without sacrificing much through put due from grid computing.

5. REVIEW OF LITERATURE

The paper "Trust Cell: Towards the end to end Trustworthiness in data oriented Scientific Computing " by Sangmi Lee Pallickara, and Beth Plale. suggests a trust model between users and remote resources. It uses trust cell, which is a collection of resources, which are trusted and recommended discoverable services with in the domain. An organization provides one or more trust cells and a trust cell can contain more than one organization.[1]

In this trust cell model communication between the trust cells is implemented by GSI model. This paper tries to establish trustworthiness to scientific applications. Here the problem is how the trustworthiness can be quantified and measured. This can be addressed.

The paper "Study on Behavior based trust model in Security system " by Gui Xiaolin,Xie Bing,Li Yinan describes a trust model which establishes trust relation ship among users, resources and applications. Trust relationship is made on behavior tracks. The concept of reputation is used in this model. The components of reputation in the old trust model are improved in this model. Resources are assigned to users based on their old history behavior. The overall trust score is the sum of indirect trust which is the reputation and the direct trust.[7]

In this model trust is made based on reputation .A set of entities haven't direct touch with the given entity at present but had some touches before give the trust rate. Based upon that opinion reputation is calculated. So the indirect trust depends on other entities which need not be completely impartial.

The paper "A system for ensuring Data Integrity in Grid Environments " by Austin Gilbert,Ajit Abraham,Marcin Paprzcki discusses the trust model for the user based on the use of system. The trust model is developed based on reputation and feed back mechanism. It concentrates mainly on data integrity. The user must know that the data is not modified. It defines three types of reputed system namely positive, negative and hybrid. The application of redundant check and reputed system taken together forms the trust worthy model here.[8]

In developing reputed system several attributes have been taken which improves the efficiency of the model. Since feed back mechanism is also included the reliability factor is increased.

The paper "Grid Security with behavior conformity from Trusted Computing" by Wenbo Mao,Fai Yan,Chunrun Chen suggests a Trust model which uses trusted computing model as the basic model. The behavior trust model is built upon Trusted platform module. This paper demands that the Grid resource selection can be improved by merging trusted computing in the behavior model.[6]

This paper suggests a model, which gives solutions for resource selection by touching the middleware. Operating system aspect may also be included.

The paper "Trusting Agents for Grid Computing " by Justin R.D. Dyson, Nathan E.Griffiths,Helene N.Lim Choi Keung describes a trust frame work for grid security which enables users to execute their job on reliable and efficient resources. Trust model is built by using agent frame work. It introduces the concept of contract net on the principle of contract tendering.[8]

In this model the chance of getting unreliable request is there. Since Grid computing involves dynamism the chance of changing the conditions can be included in this model

The paper "Trusted grid computing with security assurance with resource optimization " by Shanshan song and Kai Hwang suggests a model which aims at securing grid resources with optimized resources subject to budget constraints. It works well with increasing number of divisible jobs and sustain efficiency even when new sites are added. Fuzzy logic is used to build the trust model. Based on previous job execution the trust worthiness is measured.[7]

Since this model uses previous statistical results of jobs in a particular resource the number of iterations must be more in order to get the accurate judgment regarding the resources

6. TRUSTED MODEL FOR GRID RESOURCE SELECTION

The following issues in Grid can be addressed by Trusted Computing. TC can be embedded in grid hardware so that secured resource selection is made.

6.1 Storage of Cryptographic Credentials

Unattended user authentication is an important requirement in the Grid system. This means that a user working in a VO via his proxy. A system of collaborators and resource providers to support variety of users form any virtual organization (VO). Proxy becomes necessary since the grid solution often take several hours or days to complete segment and it may be difficult for the user to present all the time. However working in the grid environment involves several dynamic sessions of resource allocation requires user authentication. With user mostly being absent user client platform issues proxy certificate for the agent. Keys of this certificate are stored in the file system taken care by the operating system. The problem of leaving the keys in the file system is overcome by shortening the life time of certificate. A new certificate must be issued every 12 hours.

This problem can be easily handled by using Trusted computing. In Trusted computing there is Trusted Platform Module which can take care of this issue. TPM is a tamper resistant one for the secure storage of keys.

6.2 Policy Conformation of organizations in VO :

Any Grid participant has concern about his policy conformation. The Grid secutiy solutions should take care whether the resources of a particular organizations are used in accordance with their policies. This issue also can be handled by TC.

Remote platform attestation is a ready solution for this sort of service. Each user has ID Keys which can sign Platform Configuration Register PCRs in a TPM. . A PCR is a securely stored cryptographic checksum of a specific executable . [3]

6.3 Virtual Operating System:

Many machines in any organization are not utilized effectively. A small area of memory in computer can be separated to provide a simulated computer, which is a virtual computer. These virtual PCs can be combined and organized to provide services for grid users. The virtual OS must provide security for user's data and process. This kind of secured OS can be implemented by using TPM module in TC.

7. CONCLUSIONS

Grid resource selection is becoming more and more important topic, a number of problems still remain to be tackled by the current Grid solutions. Group-oriented security and distributed system behavior conformance are identified among the essential requirements for Grid resource selection. The trusted computing technology, with its inherent properties of group-oriented security and system behavior conformation, can provide suitable solutions to the identified Grid resource selection problems. Hardware and software support for TC is gradually becoming available. It must be seen how such tools can be used to enhance the trust and security in Grid environments. Trusted computing technology combined with fuzzy logic can solve some of the problems of resource selection in grid environment.

REFERENCES

[1] sangami Lcc Pallickaran,and Bcth Plalc "Trust Cell : Towards the End-to-End Trustworthiness in Data-oriented Scientific computing, " in proceedings of the 2006 international conference on parallel processing workshops.

[2] Wenbo Mao ,Hai Jin and Andrew Martin "Innovations for Grid Security from Trusted Computing," in Oxford University Software Engineering center on 7th June 2005

[3] Luis Ferreira, Viktors Berstis, Jonathan Armstrong, Red book " Introduction to Grid Computing with Globus "

[4] William Stallings "Cryptography and network security" third edition.

[5] Shanshan song and Kai Kwang "Trusted Grid Computing with security assurance and resource optimization" in proceedings of the 17 th international conference on parallel and deistributed compting systems " September-2004.

[6] Wenbo Mao, Fei Yan, Chunrun chen "Daonity-Grid security with behavior conformity from Trusted computing"

[7] Gui Xiaolin, Xie Bing, Li Yinan, Qian Depei "Study on Behavior-based Trust Model in Grid Security System " in the proceedings of the 2004 IEEE

[8] Justin R.D. Dyson, Nathan E.Griffiths,Helene N.Lim Choi Keung "Trusting Agents for Grid Computing "

[9] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the Grid: Enabling scalable virtual organizations." Int. J. Supercomputing, vol. 15, no. 3, pp. 200-222, 2001