ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 5, May 2016

AN IMPROVEMENT OF SECURITY ISSUE IN GRID COMPUTING USING MCS- (SHA-256)

Adwita Pathak , Dr. Pradeep Tomar,

School of Information & Communication Technology

Gautam Buddha University, Greater Noida, Uttar Pradesh (India)

ABSTRACT

Lack of proper authorization and security in grid computing technologies is a matter of much concern. The concept of virtual organizations which is at the core of computational grids further complicates the matter. There are many ways to access the resources of a Computational Grid, each with unique security requirements and implications for both the resource user and the resource provider. A complete set of Grid usage scenarios are presented and analyzed with regard to security requirements such as authentication, authorization, integrity, and confidentiality. The main value of these scenarios and the associated security discussions are to provide situations against which an application designer can match, thereby facilitating security-aware application use and development from the initial stages of the application design and invocation. In this paper we propose a novel algorithm namely MCS (SHA-256) to provide the security in grid commuting. The proposed technique is implemented in MATLAB environment.

KEYWORDS:-Grid computing, authentication, security, MCS, SHA-256 etc.

I.INTRODUCTION

The dynamic and multi-institutional nature of grid computing environment[1] has created challenging issues connected to its security [2]. Grids are usuallyworking in high computation oriented tasks which needs secure collaboration among the various autonomous domains geographically dispersed at various places. A lot of research has been done on authorization in distributed systems but not much work has been done in real life distributed applications such as grids. The identity based authorization which was initially put into practice maps a user's global identity(distinguished name) to a local account that has to be setup at every grid site. This is maintained in a list called "Grid-mapfile". In a scalable grid infrastructure this should not be a

likable solution for authorization purposes. The evolution of role based access-control mechanism is thus a natural choice in such a scenario [3][4].

Grid Information Service (GIS)

The role of the Grid information service (GIS) is to provide such information to Grid schedulers [6]. GIS is responsible for collecting and predicting the resource state information, such as CPU capacities, memory size, network bandwidth, software availabilities and load of a site in a particular period.

II.PROBLEM STATEMENT

In the foundational paper "The Anatomy of the Grid" [3], Foster, Kesselman, and Tuecke attempt to address this problem by (re-)defining the Grid problem as coordinated resource sharing and problem solving in dynamic, multi-institutional, virtual organizations. This concept of a virtual organization (VO) is central to Grid computing. A simplified view is that a VO is a set of participants with various relationships that wish to share resources to perform some task. In that paper, Foster et al. argue that the Grid problem is thus central not only to "e-science", but also to industry, where the coordination of distributed resources both within and across organizations is increasingly important. Grid computing has been the focus of a tremendous amount of research and development effort, both in research institutions and in industry. Even though the technology is in its early development stages and is still evolving rapidly, Grid systems are being deployed and used worldwide. This situation creates a great opportunity for computer science researchers in several areas for two reasons. First, many crucial computer science research questions need to be answered in order to deploy and operate Grids effectively.

III. SYSTEM MODEL

The Monte Carlo approach is based on the assumption that the value of the derivative is equal to the expected value of the derivative in the future discounted back to time zero, like the following equation states:

$$f(S,0) = e^{-rT} E[f(S_T, T)]$$

The simulation can be divided into 4 steps which are listed in the following:

1. Generate and simulate N number of N(0,1) outcomes under the risk neutral assumption
2. Approximate and calculate N number of terminal values
3. Calculate N number of the final payoff and then calculate the arithmetic averageof the payoff at maturity
4. The price of the option today is then found by discounted this value with the risk free interest rate

One of the advantages of simulation as an option pricing tool is its accuracy and easy implementation. This makes it a fine tool for controlling the performance of other models and methods. However, the accuracy of the simulation process depends very much on the number of simulations, and the convergence rate which can be described as:

$$\frac{\sigma}{\sqrt{N}}$$

where N is the number of simulations. This also means that in order to minimize the simulation error by half, the number of simulations should be four times higher (Empirical Finance notes, 2010, chapter 4, slide 21). One should also keep in mind that the higher the number of simulations, the longer the time before the process has been simulated. The chosen number of simulations in the analysis is 10,000.

Unfortunately, the Monte Carlo simulation sometimes contains a bias that can make the simulation less accurate.

IV. PROPOSED IMPLEMENTATION

SHA-256 Algorithm

- Each step t ($0 \leq t \leq 63$): Word expansion for W_t

If $t < 16$

- W_t = t^{th} 32-bit word of M_j

If $16 \leq t \leq 63$

- $S_0 = (W_{t-15}$rightrotate 7) □ (W_{t-15}rightrotate 18) □ (W_{t-15}rightshift 3)
- $S_1 = (W_{t-2}$rightrotate 17) □ (W_{t-2}rightrotate 19) □ (W_{t-2}rightshift 10)
- $W_t = W_{t-16} + S_0 + W_{t-7} + S_1$
- Each step t ($0 \leq t \leq 63$):

- S_0 = (A rightrotate 2) □ (A rightrotate 13) □ (A rightrotate 22)

- maj = (A ^ B) □ (A ^ B) □ (B ^ C)
- $t_2 = S_0 + maj$
- S_1 = (E rightrotate 6) □ (E rightrotate 11) □ (E rightrotate 25)
- ch = (E ^ F) □ ((← E) ^ G)
- $t_1 = H + S_1 + ch + K_t + W_t$
- (A, B, C, D, E, F, G, H) = ($t_1 + t_2$, A, B, C, D + t_1, E, F, G)
- Finally, when all 64 steps have been processed, set

  $H_0 = H_0 + A$

  $H_1 = H_1 + B$

  $H_2 = H_2 + C$

  $H_3 = H_3 + D$

  $H_4 = H_4 + E$

  $H_5 = H_5 + F$

  $H_6 = H_6 + G$

  $H_7 = H_7 + H$
- When all M_j have been processed, the 256-bit hash of M is available in H_0, H_1, H_2, H_3, H_4, H_5, H_6, and H_7

Web services

A programming model based on composing together functionality provided by multiple web services

Similar to the use of shared libraries/DLL files common functionality provided by shared entity (service) composition program builds additional functionality by making use of one or more services

Service composition programs can themselves be exposed as web services

Can then be accessed by clients

Or used as part of even higher-level service compositions

- Web services allow you to invoke programs already installed on a remote machine.
- Remote code execution allows you to execute arbitrary code on a remote machine.
- The latter is used for job submission and cycle stealing systems.

MCS WITH SHA-256 FOR GRID COMPUTING ISSUES

Grid Computing Systems (GCS) have been proposed as an effective technology in purely distributed resource coupling for applications that require large space for computations and resources.

- Security and Reliability has proved to be one of the most important criteria in grid systems. In such systems, dynamic access to the required resources is complex, and therefore achieving security tends to be very difficult.
- In this work we propose an algorithm to estimating reliability of programs and grid system based on Monte Carlo simulation. Our suggested algorithm considers the transmission rate of data between nodes through links and processing time on nodes to estimate the reliability of involved nodes and links which requires less time and complexity for running and it is appropriate for GCS.
- Monte Carlo methods are a class of computational algorithms that rely on repeated random sampling to compute their results. Monte Carlo methods are often used in simulating complex systems. Because of their reliance on repeated computation of random or pseudo-random numbers, these methods are most suited to calculation by a computer and tend to be used when it is infeasible or impossible to compute an exact result with a deterministic algorithm.
- In Security, Monte Carlo simulation method is used to calculate the value of companies, to evaluate economic investments and financial derivatives. On the other hand, Grid Computing applies heterogeneous computer resources of many geographically disperse computers in a network in order to solve a single problem that requires a great number of computer processing cycles or access to large amounts of data. In this paper, we have developed a simulation based on Monte Carlo method which is applied on grid computing in order to predict through complex calculations.

V.RESULT

Grid computing is a modern concept that not just speeds up computing and cut costs, but causes a paradigm shift in computing. However, several challenges still weigh down the technology. 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. This paper addresses the security needs of both user and resource provider. This analysis on the one hand will help to increase the reliability and security in grid computing and on the other hand will lead to develop new applications based on grid computing.

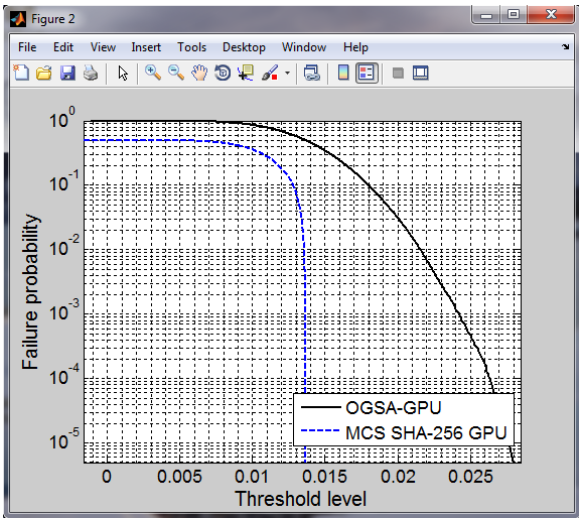

Figure 4.1: Failure probability of OGSA-GPU and MCS SHA-256 GPU on Threshold level

As we see that the failure probability of the existing algorithm (OGSA-GPU) is more than the MCS SHA-256 GPU. Comparison table is given below:

Threshold value	OGSA-GPU (Failure probability)	MCS SHA-256 GPU (Failure probability)
0	0.8	1
0.005	0.8	0.9
0.01	0.6	0.8
0.015	0.07	0.5
0.02	--	0.06
0.025	--	0.005

Table 1: comparison table of OGSA-GPU and MCS SHA-256 GPU

Lab 1:

Training with TRAINLM.

Calculation mode: Parallel with MATLAB Workers

Epoch 0/1000, Time 0.022, Performance 20.485/0, Gradient 25.8544/1e-07, Mu 0.001/10000000000, Validation Checks 0/6

Epoch 3/1000, Time 0.08, Performance 2.2563e-22/0, Gradient 9.2403e-11/1e-07, Mu 1e-06/10000000000, Validation Checks 0/6

Training with TRAINLM completed: Minimum gradient reached.

ans = 0

nnet:gpu:NotAbleToUseParallelPool

No GPU available.

nnet:gpu:NotAbleToUseParallelPool

No GPU available.

VI.CONCLUSION

Monte Carlo simulation generically exhibit naturally parallel and computationallyintensive characteristics. Moreover, we can easily fit the dynamic behaviormodel, which works so well for Monte SHA-256, onto a grid system to implement large-scale grid-based Monte Carlo computing. Also, security based on the analysis of grid-based Monte Carlo applications, we may take advantage of the statistical nature of Monte Carlo calculations and the cryptographic nature of random numbers to enhance the performance and trustworthiness of this Monte Carlo grid-computing infrastructure at the application level.

Future direction

After doing this research, I have to suggest for future a Grid-Computing Infrastructure for Monte Carlo Applications (GCIMCA) will implement on MATLABusing the techniques described in this paper. The infrastructure software aims to provide grid services to facilitate the development of grid-based Monte Carlo simulation and the execution of large-scale Monte Carlo computations in a grid-computing environment.

REFERENCES

[1] Neha Mishra1, Ritu Yadav2 and SaurabhMaheshwari "SECURITY ISSUES IN GRID COMPUTING " International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

[2] Energy Assurance Daily, September 27, 2007. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Infrastructure Security and Energy Restoration Division. April 25, 2010.

[4] Seyyed Mohsen Hashemi, Amid KhatibiBardsiri: "Cloud Computing Vs. Grid Computing", ARPN Journal of Systems and Software, VOL. 2, NO.5, MAY 2012, 2009-2012 AJSS Journal.

[5] Milan KantilalVachhani and Dr. Kishor H. Atkotiya: "Similarities and Contrast between Grid Computing and Cloud Computing", Indian Journal Of Applied Research, Volume- 3, Issue-3, March 2013.

[6] Mayank Kumar Maheshwari, AbhayBansal, **"**Process Resource Allocation in Grid Computing using Priority Scheduler **",**International Journal Computer Applications "(0975 – 8887) Volume 46– No.11, May 2012 20

[7] Seung-Hye Jang, Xingfu Wu, Valerie Taylor, Gaurang Mehta, Karan Vahi, EwaDeelman,**"**Using Performance Prediction to Allocate Grid Resources**",**GriPhyN Technical Report 2004-25

[8] Javier Carretero, FatosXhafa, Ajith Abraham, "GENETIC ALGORITHM BASED SCHEDULERS FOR GRID COMPUTING SYSTEMS", *International Journal of Innovative Computing, Information and Control* ICIC International °c 2005 ISSN 1349-4198 Volume 3, Number 6, December 2007 pp. 0–0 .

[9] Akash K Patel, Kinjal A Faldu ,Meghna R Goswami , Mehta Prashant, "Grid Computing:
An Overview", Volume 3, Issue 2, February 2013) pp-602.

[10] D. B. Skillicorn, "Motivating Computational Grids," in 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'02*)*, May 2002, pp. 401–406. ISSN: 2277-3754 ISO 9001:2008 Certified

[11] DarshanKanzariya, Sanjay Patel, "Survey on Resource Allocation in Grid", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 8, February 2013.