Journal of Theoretical and Applied Information Technology
10th May 2016. Vol.87. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ALPHA SCHEDULER APPROACH TO ENHANCE SECURITY AND HIGH PERFORMANCE IN CLUSTER ENVIRONMENT

[1]INDRAJITH.A.N, [2]MANISHANKAR.S, [3]MONIKA.B.R

[1,3]P G Scholar, Department of Computer Science, Amrita Vishwa Vidyapeetham University, Mysuru Campus, Karnataka, India
[2]Assistant Professor, Department of Computer Science, Amrita Vishwa Vidyapeetham University, Mysuru Campus, Karnataka, India
E-mail: [1]indu.an444@gmail.com, [2]manishankar1988@gmail.com, [3]monicabr56@gmail.com

ABSTRACT

Cluster computing finding increasing deployment in academic, research, enterprise for efficient resource management and coupled with this there is a increase in demand for concerns regarding the security and performance of these clusters. Security and performance are vital aspects within the field of cluster computing. However, security usually incurs a certain amount of performance varies and adds usage complexity to a field of computing where performance is pivotal and usage complexity is already high. In this paper we are presenting a security design platform and associated with security best practices, supplementing for high performance computing facilities. The planned work aims to handle issues regarding high performance computing security, specifically to mitigate the risks known within the current cluster security concerns and based on the progress we are introducing the secure job scheduling approach called ALPHA scheduler with some security features implemented in it . Planned research design and best practices arrange to give the simplest exchange between security approaches and performance. All together gives an approach of security in high performance computing cluster.

Keywords: *High Performance Computing, Cluster Security, Access Control, network-level security and protection, MPI, Security monitoring, DDOS, Service Level Agreement.*

1. INTRODUCTION

Cluster computing is a form of computing where a group of computers are linked each other so they can behave like a single entity. It is a technique of inter linking two or more computers into a network (through a neighborhood or local area network) to take benefit of the parallel processing power of those computers.

A cluster encompasses a collection of distributed resources to be unified. By definition, clusters are multiple, closely-coupled machines that are centrally administered. These machines share common resources such as network bandwidth, compute cycles, and storage area. The challenge is to secure these internal resources against unauthorized access while at the same time permitting easy access by authorized users. In contrast, the resources found in a typical enterprise- type environment are often very loosely coupled and exhibit minimal coherence of these types of resources.

A cluster provides mechanisms for resource management. The challenge here is to manage a cluster such that authorized users can utilize resources efficiently in an authorized way using an pre-arranged job prioritization system. This is distinguished from enterprise-type environments that usually do not need to manage resources between competing interests. When a user executes a job on a cluster, it is often difficult to differentiate legitimate versus illegitimate use unless there are obvious malicious signatures of users. For example, cluster users are potentially able to tamper the shared data or to excessively consume compute cycles to an extent of disrupting the service available to other cluster users.

High performance computer have to deal with, not only, the constant security problems as other computers have, but have additionally to deal

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

with special security considerations. However addressing and implementing solutions to the special security problems on HPC is hard ,since the steps taking to deal with these problems shouldn't varies the performance of those compute node. For example, by time scheduling different jobs needs a special architecture, which may reduces the security and performance of the cluster.

2. LITERATURESURVEY

There are large numbers of analysis and research carried on enhancing security models with performance. This section provides an overview of work carried out by various researchers in the field of cluster computing.

[6]William Yurcik and Gregory A. Koenig they defined a unified framework for protection techniques and methodologies that highlights the properties of cluster security that distinguish it as a novel problem space and then they conclude with an outline of preliminary progress on a monitoring project centered specifically on cluster security then the research work carried forward at the National Center for Super-computing Applications, the current methodology to cluster security is divide- and-conquer approach. Existing pre-defined security techniques are deployed against varied cluster components with the logic that, upon the composition of the endmost cluster system, the overall security of the cluster should perform to the actual fact that every cluster components are secured.

[7] M. Smith, M. Schmidt worked on Optimizing Security Configurations of Service Level Agreements. .some cluster security mechanisms are already configurable, where as several others like firewalls and advanced sand boxing techniques are sometimes configured statically per site keeping in mind that the specific user community requires. In their research work, authors present a WS-Agreement approach for a fine grained security configuration mechanism to permit an optimization of application performance supported with specific security needs in the cluster environment.

[8] Satish Kumar Thalod, Ram Niwas worked on Security model for computer network based on cluster computing. Although a cluster might comprises of just a few personal computers connected by a straight forward network, this cluster architecture can also be used to achieve high levels of performance and computing. A cluster computing security model could be theme for enforcing and implementing security schemes. Their research work proposes a security approach for a computer network based on cluster computing architecture by numerous tools accessible in TCP/IP security model.

3 PROPOSED WORK

After carried out the detailed survey and analysis on improving and enhancing the security features in a cluster environment ,in order to precedence our efforts in protecting

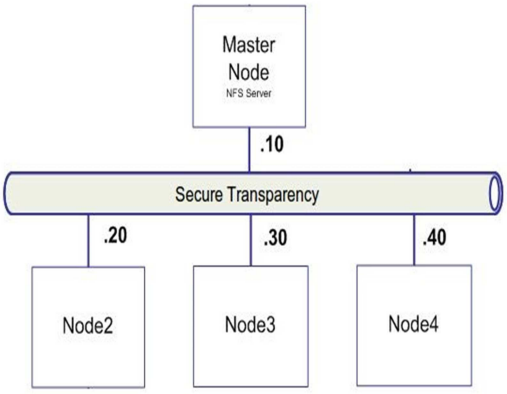

Figure 1: Secure Transparency

Clusters the proposed research work presents the following techniques which are the features of alpha scheduler approach. We adopted these techniques to give extra protection to the clusters as follows.

3.1.1 Protection against potentially unwanted nodes: Compute Cluster server will not permit unapproved nodes being added to the cluster

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

family as compute nodes. If an intruder could add a computer as a node, the Job Scheduler will send its jobs and credentials to that node which has added by the attacker, which can potentially contain sensitive Data Any node that is added to a cluster family encompasses a standing of unfinished level Approval, and remains in the same state until the cluster head/manager approves and resumes the computation node to an approved level.

3.1.2 Securing Computer cluster network topology: Computer cluster topology, is the one which isolate the cluster nodes from the general public network, the topology provides a hyperbolic security by exposing solely one network interface of the master node to the public network. These topologies provide an excellent way to secure MPI traffic from DOS, DDOS, Information Disclosure threats and Data Tampering issues. The most basic level of security is physical security which makes sure you that limit the access to the administrator or master node in order to further protect the encrypted user credentials and jobs/data stored in the Scheduler Database which is only accessible to master node.

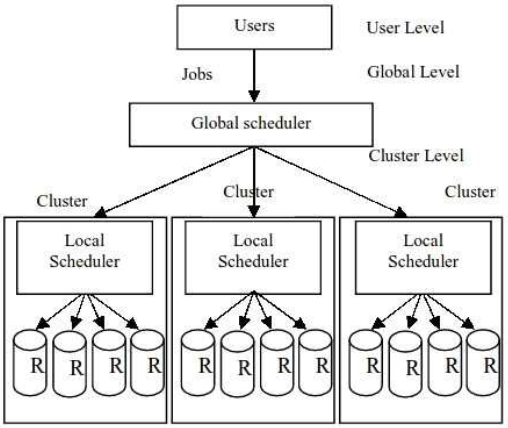

Figure 2. Secure Job Scheduling

3.1.3 Secure Job Credential Handling: Each job submitted to the computing cluster uses the verification credentials such as combination of user name and password / Unique NONCE given by the job owner/Mater node to the user group. Since jobs runs on the user, nodes have access to the similar network resources that are accessible to the user, simplifying the task of building a new job and debugging a job

3.1.4 User level security: Compute Cluster Servers limits the use and administration of the compute cluster from child nodes and also user groups on the head node. If you produce a file share on the master-node, make sure to limit access to the cluster administrator and cluster user-groups. Thus defining levels of security among the cluster user groups and components.

3.1.5 Disk Quotas We might consider setting disk quotas on each head node and child nodes to stop a user from filling the Storage space. Running out of storage space on the master node can end the operation run by Job Scheduler. Running out of storage space on a compute node can impact job and task execution. So here we are defining the dynamic storage allocation.

3.1.6 Security Transparency: We outline the security transparency done by keeping security operations hidden from direct access to the applications and/or operating systems as much possible. We tend to believe that this is often the foremost vital feature to reduce (or completely stop) applications' or OSes' code modification and likewise reducing performance overhead.

4. ALGORITHM DESCRIPTION FOR ALPHA JOB SCHEDULING APPROACH:

Step 1: **Vn** Verify the addition of node, authorize and approve it.

Step 2: **PaP** Set privilege and access permission to the newly added node

Step 3: Dq Set the disk quotes**.**

Step 4: **J** Start assigning the jobs.

Before assigning the job, verifying the cluster nodes by a secure code which is generated during the node registration. To check whether the node belongs to our

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cluster family.

Step 5: **Tj.SubT** placing Jobs J in the queue (During submit time).

Step 6: **Tj.StartT** Taking out the jobs J at beginning time

Step 7: WHILE (waiting queue is non empty) {
Get the head of queue (job J);
IF (resources are free to start J) {
START J;
Remove J from queue ;
}
ELSE {
Back fill other jobs from queue ;
}
}

Step 8: Calculating Average response time .

AvResT = 1/j * (Tj.endT - Tj.subT)

Step 9: Calculating Cluster utilization .

$$UTIL = \frac{\Sigma j\ (Nj * (Tj.endT - Tj.startT))}{N * (lastEndT - firstSubmitT)}$$

Vn	for verifying the node
PaP	For Access Permission
Tj.subT	for the submit of job j
Tj.startT	for the begin time of job j
Tj.endT	for the end time of job j
Nj	for the occupied number of nodes of job j
Jt	for the total number of jobs
N	for the total number of available nodes
firstSubmitT	for the first submit Even occurred (min jTj.subT)
lastEndT	for the time the last end Event occurred (maxjTj.endT)

Table 1: Algorithmic Variables

Back-filling is a well known technique to enhance the performance of space-sharing schedulers. A back filling scheduler searches for free slots within the schedule and make use of them with appropriate jobs while not delaying jobs which are already scheduled. For that, users should provide an estimated run-time for their scheduled jobs, so that the scheduler will predict once jobs are finished and others can be initiated. Jobs are canceled, if they run longer than expected.

Journal of Theoretical and Applied Information Technology
10th May 2016. Vol.87. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

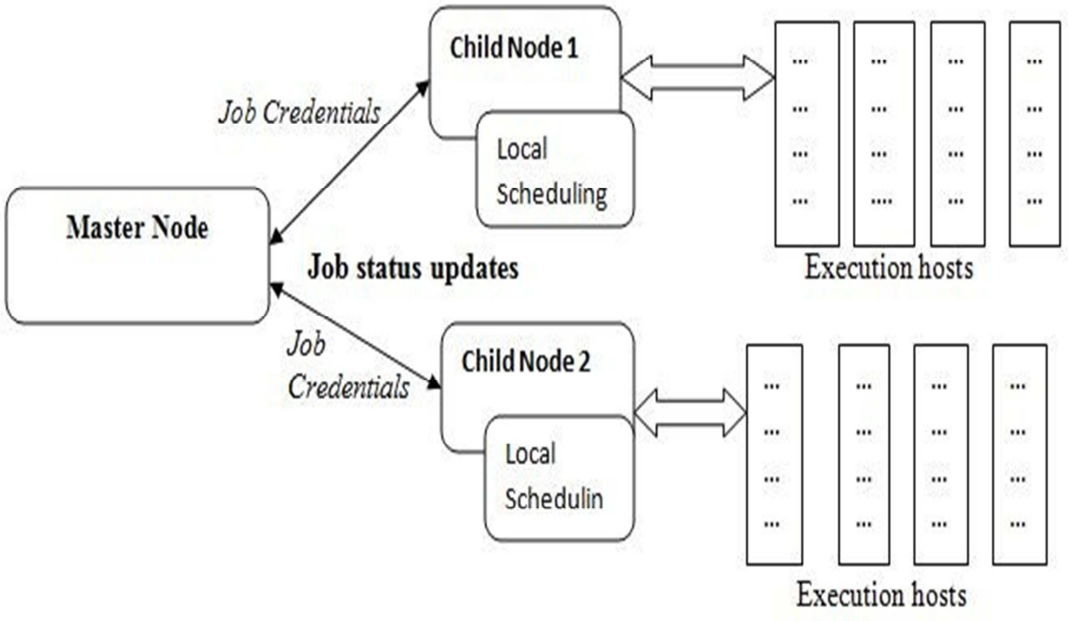

Figure: 3 Secure Job Credential Scheduling

Figure 4. Heap Memory Usage Of Performance By 20%.

Journal of Theoretical and Applied Information Technology
10th May 2016. Vol.87. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 5. CPU Threads Utilized

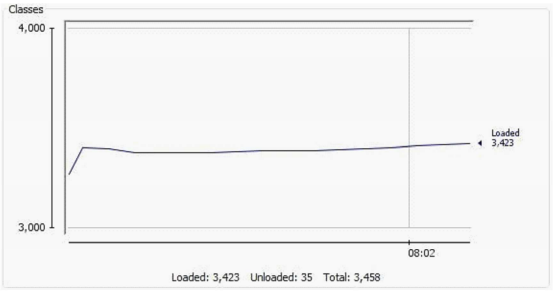

Figure 6:CPU Classes Utilized

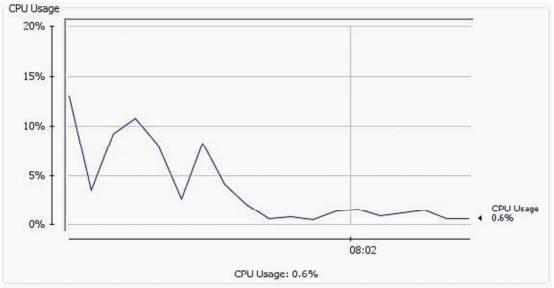

Figure 7: Cpu Usage

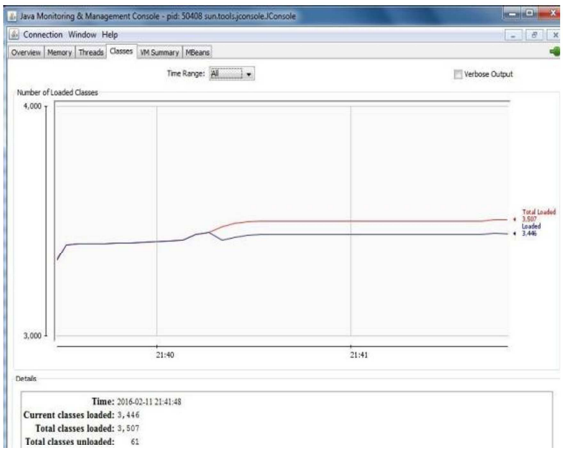

Figure 8. Performance Comparison(20% Increased)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSION

In the present paper we have conferred complementary security approaches for High-Performance Computing clusters. The corresponding security methodologies and approaches we present for this cluster environment is a unified security model including distributed authentication, access control and user level security. At the HPC cluster environment end of the cluster environment , clusters must be versatile to handle a dynamic user constituency executing a large vary of applications. The corresponding security suggestions/techniques we present for this HPC cluster environment focuses on Secure job scheduling ,job credential handling, user level security, secure transparency There is much more work to be done in areas such as intuitive human interfaces to security tools, scalable cluster monitoring, masquerade detection, interconnect security, and versatile protection that progressive with incremental cluster growth. And the secure scheduling approach that we showed and the simulated results from this paper can also be achieved in a real environment.

REFERENCES:

[1] A.Mitra and R.Nayak, ‘‘ Studying Security Issue in HPC(Super Computer) Environment”,In proceedings ofInternational Journal of Computer Communication Technology(IJCCT),Issue:2,3,4,pp309-312, 2010.

[2] Yurcik, W., Koenig, A., Meng, X. and Greenseid, J. ‘‘ Cluster Security as a Unique Problem withEmergent Properties:Issuesand Techniques’’. 5th LCI International Conference on Linux Clusters, Presentation, May 2004 .

[3] Pourzandi, M., Gordon, D., Yurcik, W. and Koenig, G. ‘‘ Clusters and Security: Toward Distributed Security for Distributed Systems”. IEEE Cluster Computing and Grid (CCGrid), 2005.

[4] A. Streit. On Job Scheduling for HPC-Clusters and the dynP Scheduler. TR-001-01, PC2 - Paderborn Center for Parallel Computing, Paderborn University .

[5] Mogilevsky, D., Lee, A. and Yurcik, W. “DefiningaComprehensiveThreatModelfor High Peformance Computational Clusters ’’. Preprint: arXiv:cs.CR/0510046. 16October, 2005 .

[6] WilliamYurcik,GregoryA,KoenigXin,Meng Joseph Greenseid ‘‘ Cluster Security as a Unique Problem with Emergent Properties: Issues and Techniques “

[7] M. Smith, M. Schmidt, N. Fallenbeck, C. Schridde, B. Freisleben “Optimising Security Configurations with Service Level Agreement”.

[8] Satish Kumar Thalod, Ram Niwas ‘‘ SECURITY MODEL FOR COMPUTER NETWORK BASED ON CLUSTER COMPUTING ’’ International Journal Of Engineering And Computer Science ISSN:2319-7242Volume2Issue6June,2013 Page No. 1920-1927.

[9] John Rittinghouse, HPC: Implementation, Management and Security, 2009.

[10] Y. Shuyuan, H. Dake and W. Jianbo, ‘‘ Security Issues in National High performanceComputingEnvironment”,IEEE 2003,pp227–230.

[11] H. Mantel, ‘‘ On the Composition of Secure Systems, ’’ IEEE Symposium On Security and Privacy, 2002.

[12] MohMatthew Smith, Michael Engel, Thomas Friese, Bernd Freisleben, Gregory A. Koenig, and William Yurcik. Security issues in on-demand grid and cluster computing.In CCGRID ’ 06:ProceedingsoftheSixthIEEE International Symposium on Cluster ComputingandtheGrid(CCGRID ’ 06),page 24, Washington, DC, USA, 2006. IEEE Computer Society.

[13] Deepak Chaturvedi. Kashish Gupta, ‘‘ HIGH PERFORMANCE COMPUTING CLUSTER ’’ , International Journal of Scientific&EngineeringResearch,Volume 5, Issue 5, May-2014,ISSN: 2229-5518 , Pages117-121.

[14] R.SumitSrivastava, Mr.Pankaj Dadheech, MrMahender Kumar Beniwal, ‘‘LoadBalancing using HighPerformance Computing ClusterProgramming’’, IJCSIInternational JComputer Science

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Issues, Vol. 8, Issue 1, January 2011, Pages:62-66.

[15] Mit Desai, " High Performance Computing and Virtualization " , Research Paper: CSCi-555 Advanced Operating Systems, 2012, Pages:1-11.

[16] A.Mitra and R.Nayak, " Studying Security Issue in HPC(Super Computer) Environment",InproceedingsofInternatio nal Journal of Computer & Communication Technology (IJCCT), Issue:2,3,4, pp 309-312, 2010 .

[17] John Rittinghouse, HPC:Implementation, Management, and Security, 2009

[18] Michael Miller, " HPC: Web-Based Applications ThatChange the Way YouWork and Collaborate Online " , Online Journal, August,2008.

[19] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity" Assurance, In Proceedings. of IEEE INFOCOM, 2009.

[20] Y. Shuyuan, H. Dake and W. Jianbo, " Security Issues in National High performanceComputingEnvironment",IE EE 2003,pp227–230.