Optimal Spot-Checking for Collusion Tolerance in Computer Grids

ABSTRACT

Grid computing offers a platform to execute computation-intensive tasks by different shared resources in a distributed and parallel manner. It has been used to solve complex problems such as engineering optimization, financial modeling, production planning, Earthquake, Simulation etc. The sharing can be controlled by a resource management system (RMS), which is responsible for dividing the task from a user into a set of execution blocks or task portions and then assigning those different blocks to available resources (typically heterogeneous and geographically dispersed) for parallel execution.

EXISTING SYSTEM

Many grid-computing systems adopt voting-based techniques to resist sabotage. However, these techniques become ineffective in grid systems subject to collusion behavior, where some malicious resources can collectively sabotage a job execution by returning identical wrong results. Spot-checking has been used to detect and tackle the collusive issue by sending randomly chosen resources a certain number of spotter jobs with known correct results to estimate resource credibility based on the returned results.

Disadvantages

- Shared resources may be misused by malicious users who can alter or sabotage other's running applications to return incorrect results.
- The malicious resources collude in producing identical wrong outputs to reduce the efficiency of the voting-based replication technique against sabotage.

PROPOSED SYSTEM

This paper makes original contributions by formulating and solving a new spot-checking optimization problem for grid systems subject to collusion attacks, with the objective to minimize probability of the genuine task failure (PGTF, i.e., the wrong output probability) while meeting an expected overhead constraint. The problem solution contains an optimal combination of task distribution policy parameters, including the number of deployed spotter tasks, the

number of resources tested by each spotter task, and the number of resources assigned to perform the genuine task. The optimization procedure encompasses a new iterative method for evaluating system performance metrics of PGTF and expected overhead in terms of the total number of task assignments. Both fixed and uncertain attack parameters are considered. Illustrative examples are provided to demonstrate the proposed optimization problem and solution methodology.

Advantages

- It detect the colluding malicious re-sources (CMR), the RMS sends *M* spot-checking (spotter) tasks with known output to randomly chosen resources.
- The attacker tries to corrupt as many resources are not possible.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB