ISSN No. 0976-5697

Volume 4, No. 4, March-April 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

PG-RM: Prognostic Approach for optimizing Grid computation using Risk Management Methodology.

Rahul Bose*[1] ,Prabhat Kumar Singh[2],Sunil Kumar Singh[3],S Venkatesan[4]
Indian Institute of Information Technology Allahabad, India
rahulbosecool@gmail.com[*1],iprabhatsingh@outlook.com[2],sunil.kumar928@gmail.com[3],venkat@iiita.ac.in[4]

***Abstract*:** With the emergence of grid computing technology to provide a high end solution for complex collaborated problems and high performance computing using the available distributed resources, it is important to implement a strong security Architecture along with a Risk Management Methodology. In this paper, a prognostic approach for optimization of grid computation is proposed, with the inclusion of an advance risk management layer. This approach is named as PG-RM grid (Prognostic approach for optimizing Grid computation using Risk Management Layer). Then the proposed model and architecture of this grid is presented with a high level work flow Model. This is a closely focused heuristic approach on the risk management methodology for improving decision making process of grid manager.

In this paper, a well-established approach for analysing the probable value of risk associated with the different security threats and vulnerabilities of the Grid is proposed. We are introducing a new risk management layer in the grid architecture Framework to provide detailed and immaculate explanation of selecting a middleware node for performing task events in the grid. Now the grid resource allocator will be able to analyse the on-going processes of the overall distributed Grid on the basis of the confidentiality, Integrity and Availability report, generated and maintained by the Risk Management Layer.

Keywords:Grid Computing, Risk Management, Resource Management, Resource Allocation, Confidentiality, Integrity, Availability, Least Risk Value, Grid Information System Manager.

I. INTRODUCTION

With the increasing demand for secure transmission, processing and sharing of the large amount of informational data, in the large geographically distributed environment, grid computing provides one of the best solutions for the purpose. Grid computing can be understood as a large combination of heterogeneous computer systems, called as resources, which is working in synchronization to each other and performs large scale computational work to minimize the computational time and simultaneously providing storage solutions [1].

Thus, grid provide secure and simple transfer of data from one point to other and making sure the resources are used in anoptimized manner. The middleware system uses proprietary algorithms (depending from organization to organization) and standards to deliver optimal quality of services. Having advantages of grid computing doesn't mean that we can overlook the security issues associated with the Grid. There are a number of security elements that need to be taken care of, such as authentication failure, unauthorized access, data integrity, access controls policies for the middleware systems, and threats related with grid itself. Thus, a need arises for a risk management methodology to be implemented on the grid, which can enrich secure allocation of tasks in risk based environment. Risk management will provide ease to the Grid information system manager, by analyzing and calculating the value of previous outcomes of risk occurrence and failures in the grid network. Based on the result of the previous history, new task would be assigned only to that middleware node which is having least risk value. For instance, we have two nodes A & B available for a task, so the grid manager will evaluate the risk associated with each respective node; and select the node with least probable value of risk failure for performing the task. Using this model the efficiency of the grid for performing a task would increase many fold.

The objective of proposing this model through this research paper is to develop a more reliable grid computing framework which is generic in nature and can be easily integrated to all the existing models of grid computing available in the market.This is a prognostic approach that uses a powerful risk management methodology to analyze and calculate the value of the risk and provides a greater efficiency and enhances the decision making capabilities of organizational grid. The research paper is significant for securing the data sharing, performance, collaboration, efficiency and accuracy.

A. *Grid Layer Architecture:*

Figure 1 shows the existing grid architecture which organizes its various components into five different layers as described below[2][3][4][5].

a. ***Grid Fabric Layer:*** This is one of the most important of all layers as its primary function is to provide permission to access, all the connected shared resources. Resources can be further segregated into physical or logical resources depending on the nature and type of service architecture. For example, individual computers distributed geographically, file systems, archives, metadata catalogs, networks, sensors, etc. This layer is important because, with an increase in fabric layer functionality, sharing operations automatically increases[6].
b. ***Grid Connective Layer:*** The given layer comprises of protocols necessary for communication and authentication. It provides aid for free flow of data between the resources and applies appropriate security mechanism. The necessity for deploying security is to provide a secure environment for single sign on functionality where the user once signed in can avail many resources remotely[6].

- ***c.*** ***Grid Resource Layer:*** This layer provides support to the previous connectivity layer and it consists of information protocols and management protocols for secure monitoring and accounting[6].
- ***d.*** ***Grid Collective Layer:*** Mainly concerned with sharing of resources and consists of protocols and services[6].
- ***e.*** ***Grid Application Layer:*** Helps in user applications and provides services of different layers[6].

B. Resources:

Further the resources can be classified primarily into three main domains, namely:

a. Computational Resources.
b. Storage Resources.
c. Network Resources.

Computational Resources: This falls under the category of machines, physical in nature. The core concern is the processing part of grid computation and scheduling. These are again sub grouped into four types [7].

a. End User Systems which consist of computational machines and are homogeneous in nature.
b. Group of computers known as CLUSTERS linked to each other and work in highly homogeneous environment. The advantage of clusters over single computer is that it helps greatly in improving the performance, speed and availability of the resource with optimized scheduling and cost effectiveness[7].
c. Intranets comprise of large interconnected networks of local resources deployed diversely and heterogeneously within the sub domain of a single or multiple organizations.
d. Extranets also called network of networks or interconnection of intranet networks. These are most heterogeneous in nature and are for multiple organization architecture unlike Intranets which are primarily dedicated for Single organization.

Storage Resources: The specialty of storage resources are that they can hold, retain large chunk of data within the storage machines. The data are usually ranging from a simple file system to large and complex database[7].

Network Resources: All the network level devices like routers, switches, hubs, firewalls, IDS, IPS etc. that makes up for the entire architecture of a physical network and is measured on the basis of bandwidth and latency[7].

C. Scheduling:

Scheduling in the grid can be understood as the allocation of the task to resources for performing any job asked by user. Scheduling is a challenging operation in the grid as reliability and efficiency of grid depends on it, consider a situation where a resource is assigned a job meant for batch processing, but the resource is capable of sequential jobs thus; this scheduling will decrease the performance of the grid. Job scheduling in the grid is considered as NP complete problem in which optimal result can be achieved in different ways[8]. Other issues related with scheduling of tasks are heterogeneous jobs to be executed by heterogeneous resources with the concern of security in grid. There are different types of scheduling algorithms available for assigning the task to them, but all varies in their efficiency. For example, a task “T” is divided into n subparts which can be solved by “N” resources of the grid. This method may increase the performance, but even a single task failure may lead to the situation where completion of the task becomes impossible, thus to complete task “T”, assigned resource will have to try again to get that failed work done. Thus, working of the grid becomes slow and less reliable[9]. This problem is solved to a large extent by the proposed model, with the use of a heuristic approach for selecting resources which has very less chance of failure due to a prediction of the result based on the previous records. This approach that is used in this paper minimizes the failure rate of the jobs and increases the overall grid efficiency.

D. Resource Management for Grid Environment:

The grid architecture is highly distributive and has the possibility that a resource can be heterogeneous or homogeneous in nature, depending from one organization to another organization and are dispersed widely over the geographical terrain. Hence it becomes very complex to manage such a large number of resources especially when different organizations apply different policies to manage the resources and uses different access models.

It is also evident that resource management is a prima factor to achieve a maximum expected efficiency. The resource management can be understood as a process segregated into different phases. Firstly remote submission of the requested job is done. Secondly, getting updates of the same while the job is in the process. Whenever there is a demand of resource, after the user submits a job, it generates urgency to discover the available resources using an appropriate directory service[10]. The Grid Scheduler takes the important scheduling decisions like the selection of resources for a given job on a particular grid node that has to be run based on the resource discovery decision by resource management.

The grid resource allocation is done based on the resource discovery by taking into account various aspects like using applications files, hardware requirements and unified computational resources. The middleware system provides services to the grid scheduler which in turn is responsible for functions like allowing users to single unified grid resource, resource selection after resource discovery etc. Here, one of the major problems that persist is that, the entire grid environment is heterogeneous in nature and thus different sites apply different resource management systems that lead to different configurations and integration. Another area of concern in resource management is co-allocation; ifa single site is unable to accomplish the need of resource requirement for a grid job, the only possible solution is allotment of resources at different sites and also a strong mechanism needed while in case of a failure of resource allocation, a need for collection of information and submit to multiple resources to accomplish the job.

E. Risk Management in Grid:

Risk management is a process of finding undesirable events that may occur in the grid during the allocation of task for performing any job and reduce the impact of failure and bring it to an acceptable level. These events arise due to threats and vulnerabilities associated with the grid such as human error or malicious intent of any user, natural hazards like earthquake, flood, fire, etc. or some technical fault that may occur in the grid network[11].

All the above mentioned issues lead to a negative impact on values of confidentiality, availability &integrity in the grid system thus decreasing the reliability of middleware system. In the proposed model with the addition of risk management layer will help in keeping the value of impact for risk in an acceptable level by using a heuristic approach of checking risk report, (mentioned below) before allocating resource for any request made for system.

This risk management framework applied in a grid comprises of different processes; however, it is noteworthy to say that it does not means, the end of all risk but, surely mitigation of risk is done. The proposed model helps grid manager to decide, which resource to be allocated to a particular job considering the threat and impact factor in mind. Thus, it provides great help to maintain information security for both job and user data. Grid manager takes the decisions regarding the categorization of the risk in accordance with confidentiality, availability & integrity model.

For example, a risk related with Denial of service attack falls under the class of Availability type.

Risk management frameworks for information security consist of four phases [12].

a. Risk Identification[12].
b. Risk Analysis[12].
c. Risk Evaluation[12].
d. Risk Treatment[12].

Firstly, the risk identification starts with the occurrence of any failure that comes in the picture. Such failures can be a network failure which is unable to support the transfer of data or information exchange from one system to the other due to the occurrence of a fault caused intentionally by an attacker or by an accidental breakdown of cables.

Secondly, analysis of risk is done where the cause of risk, type and capacity to cause harm is estimated and documented.

Thirdly, risk evaluation is done by calculation and measurement of the impact of risk. With the increase in the value of impact, the probability of the grid middleware being unreliable also increases, which means the chances of attack on that middleware system is high.

Finally, the treatment of risk is done after having an idea of risk capabilities and decision for either accepting, mitigating, avoiding or transferring the risk is taken. Depending upon the risk value generated by the risk management layer, grid manager decides most suitable action which his either accepts it, mitigate it, avoid it or transfer it.

For example, a small risk incurred during the placement of middleware system for a given location inside the organization can be accepted by providing proper physical security. Risk of virus attacks needs to be mitigated by using firewalls and updated anti-viruses solutions.

Risk regarding compromising of middleware system by DDOS attack or man in the middle attack need to be avoided by securing the parameters of grid by Intrusion detection systems and intrusion prevention system.

In case of risk transfer process, grid manager will deny those users, having a high degree of risk involvement; and by doing so, the allocated task as well as the risk would be transferred.

Thus, we have seen how risk management can help improve the information security in the grid computation and provide effective capability to handle the request from users and make a decision that yield sophisticated optimal result for the computation.

Table: 1 List of Risk Classified in terms of CIA.

TYPES OF RISK	C	I	A
Buffer Overflow	✓		✓
Denial of Service			✓
Network Breakdown			✓
Social Engineering	✓	✓	
Missing Patches		✓	
Software Vulnerabilities	✓	✓	
Route Hijacking	✓		✓
Viruses		✓	
Earth quake			✓
Flood			✓
Data Theft	✓	✓	
Fire			✓
Packet Sniffing/Monitoring	✓	✓	
Utility Failures			✓

C= Confidentiality; I= Integrity; A= Availability

Table 1 of this paper, shows how we have considered various types of risks which can cause impact on confidentiality, integrity or availability.

II. RELATED WORK

Recently there is a lot of research work being conducted on Grid computing. Our work is inspired by the simple fact that most of the recent work has failed to acknowledge, about developing an architectural framework for risk management which can be integrated to the main model of grid computing framework. By doing this, the new model will enhance the security of the overall grid with better decision making based on the increased reliability and efficiency achieved through this model.

Previous works like proposed fault tolerance model, talks much about how fault masking and the reconfiguration which helps to achieve faults prevention by restoring the grid middleware system to a previous state of operations and eliminating faulty components from systems[9] [13].

The above approach is limited only to observing that a fault has occurred and then deploy any recovery procedure that can be initiated.

III. PROPOSED MODEL

In grid computing model, the risk management layer increases the efficiency of the task by providing a risk value to make a decision for the selection of a particular node for performing the given tasks. Earlier grid architecture takes in account the functionality of computations resources, sharing and services but the risk involved with all these processes are never calculated. In this model, we are proposing to add a new layer parallel to the complete grid architecture as shown in the figure.

Risk management layer provides an extra advantage to the existing model of advance architecture of grid computing through accreditation of information security and mapping out the risk value in terms of confidentiality, availability& integrity for each layer. An intellect is provided to the grid computing and a prediction mechanism is developed for the events (job allocation, resource optimization, time efficiency, resource sharing). A computational value is obtained from the previously analyzed results and quantifies it based on the analysis done in the present.

This model eradicates the previous known disadvantage of grid computation for the allocation of task with optimal utilization of the resources. Hence with the inclusion of advanced prognostic methodology of risk management, a better decision making ability by the grid information system manager is done as it allocates the job based on the heuristic approach of assigning tasks to various middleware nodes.

The proposed Model consists of four major sections.

a. Grid Architecture Workflow
b. Input logs Record Database.
c. Risk Assessment Layer.
d. Risk Report.

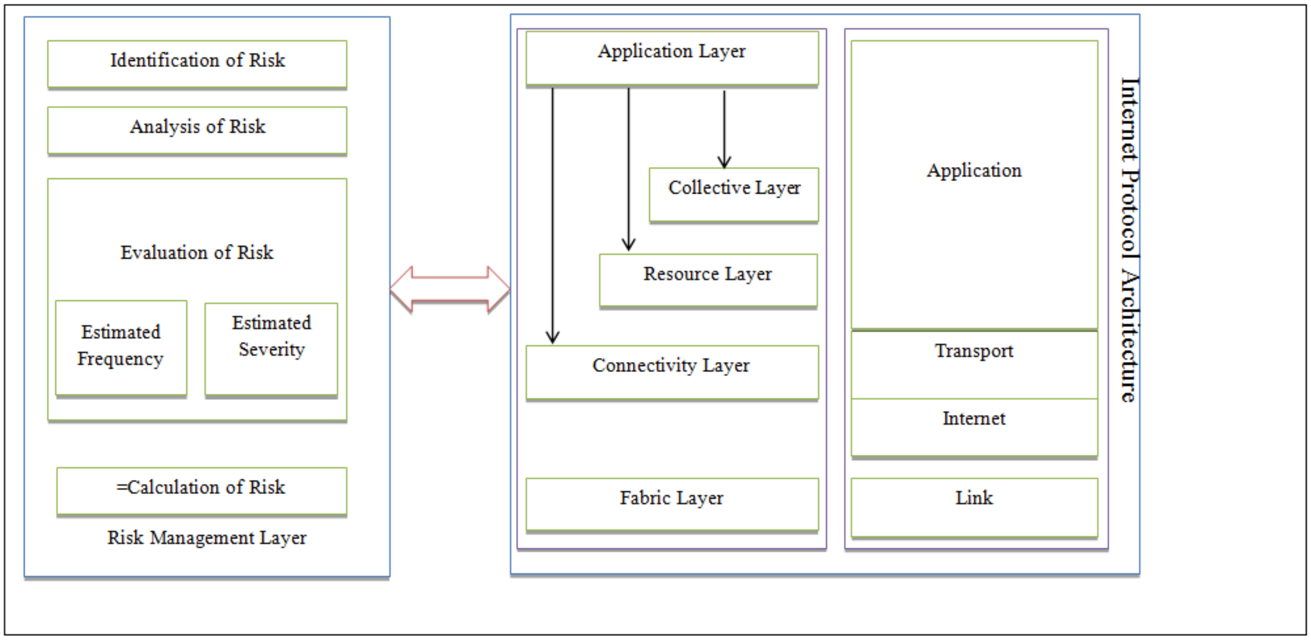

Figure 1. High Level view for Grid layered Architecture [2]

The figure 1 is divided into two Sections. The right side of the figure is taken from and shows a high level model of existing grid architecture and the left portion is our proposed layer for risk management[2].

The Grid Architecture has its usual workflow except for the new model consist of well-defined approach where all the errors reported by individual Grid/resources is stored in a file called as “Error Report” will be submitted to the Risk Assessment Layer.

The Risk Management Layer will employ an approach to process the information by thorough and rigorous risk identification methodology followed by a risk analysis process. In the risk evaluation phase, the calculation of the risk is done on the basis of the estimated frequency and estimated severity.

Calculated Risk = Estimated Severity * Estimated Frequency

The final phase of the risk management layer is the “treatment of the risk”. The calculated risk will be well defined and classified under any one or more parameters concerning to confidentiality, integrity &availability. The Grid Information System Manager will have a parallel processing of the generated risk report which is stored in the database parallel to the scheduler. Risk based on this report is compared with the risk already stored in the previous logs.

IV. PROCESS

Figure 2 show that the proposed architecture works in a systematic way, where a user register itself through a user interface and avail the various services of the grid. For a particular instance, more than one user can log into the grid using their registered username, password. After the authentication process is done, the user, on the basis of their privileges set by the Grid Information System Manager will request for a service.

There are mainly three types of grid system [14]

a. Computation Grid[15]
b. Data Grid[16]
c. Service grid [17]

This request will be materialized by the Grid Information system manager (GISM) whose primary role is to locate the live resources as the resources are dynamically updated based on the availability. Further the scheduler will allocate the job to a resource on the basis of its availability and reliability.

For a particular instance the reliability of the network is R(T) at time t, this will depict that, all nodes are operational and up to the mark with a minimum probability of any degradation and a maximum probability that all the nodes are able to communicate with each other at the time interval [0,t].

Likewise, the reliability of the path is determined as the availability of the paths from the source to destination which are operational in the given time interval [0, t]. Grid Information system manager is also responsible for maintaining the Bandwidth of the network by calculating the maximum rate of flow of messages in the given networks. This record will help to establish the report which will log the peak hour's bandwidth. During peak hours, bandwidth generally degrades due to the number of failures in the nodes and links connected in the network. All these calculation will determine the network connectability which will be evaluated by the number of connected pairs or links in the networks despite the faults or drops in the network.

We are dividing the proposed PG-RM model into different phases. The first phase describes the scenario, where a resource is being requested by the user for performing an application task in the grid. This request is processed by grid manager, and allocation ofa resource is done only after checking the previous risk management reports for such related request. In the second phases, a decision for allocating the appropriate grid/resources is made by analyzing the risk report. What happens here is that the grid looks for the resource having optimal values of risk related for the task after analyzing the reports available with this grid manager. When the task gets completed, result (success or failure report) is stored in the logs so that it can be used for later allocations. This process is continuous in nature and helps in optimizing the risk and calculating its severity and impact. The database stores the error logs and an exclusive error report with the impact rating of the risk are given. For an instance, if a user demands a computational resource from the grid manager which is connected to other subordinate grids, the grid manager classify the job type from logs and search for the grid which provides similar type of services and allocates the grid to user. Now the selected grid will further funnel down the request to the appropriate subordinate resources for performing the task. Again every subordinate grid will have grid information system manager along with a risk management layer. If no error occurs user will be acknowledged else if any error occurs, log will be maintained, and the risk management layer will classify the error type based on the criteria of confidentiality, integrity and availability.

For example, suppose a process is in progress, after the scheduler has assigned a task to a particular resource or a node and suddenly due to a malicious attack the network based IDS raises an alarm, immediately as a repercussions the grid manager will terminate the task and a log update for future reference will be made with error type classified under "integrity" compromised [Table 2].

Similarly, if a data required by the resource for performing the allocated job, as requested by the user to the main middleware system is being under espionage, by an attacker, using a network monitoring tool like Wireshark, tcpdump, ettercap, dSniff etc. can lead to the matter of confidentiality in case of espionage or eves dropping. The attacker gathering information using network packet sniffer can analyze the whole data which will destroy the fundamental of confidentiality.

Finally, the Grid scheduler will analyze and merge the two reports viz. success report generated on the completion of the task successfully and the risk report which contain the numerical value calculated by the summation of the product of all the failure events and the severity of such failures on the respective classes of Confidentiality, Integrity, and Availability.

The frequency of failure is subdivided into four different events like Human involvement failure frequency(EHF), Technical failures frequency (ETF)Natural or Environmental Failures frequency (ENF) and Unknown failure frequency (EUF).

So, the total failure frequency (EF) for a single process can be calculated by the union of all four individual Events as shown in Equation 1.

$$. \; E_F = E_{HF} \bigcup E_{TF} \bigcup E_{NF} \bigcup E_{UF} \qquad .1$$

As we know, in the grid environment, there can be "n" number of processes running simultaneously. So the total failure (TF) of the overall Grid process is given by summation of all "n" individual processes.

$$TF = \sum_{i=1}^{n} E_{F_i} = (E_{F_1} + E_{F_2} + E_{F_3} + \ldots + E_{F_n}).$$

Table 2 shows how the grid information system will maintain a list of records which will contain different attributes like user id, request type, job id, and resource id. Based on the outcome the final report will be classified under Success or Failure.

The failure will consist of attributes like, the type of failure, cause of failure, error response time and impact of failure on the basis of confidentiality, integrity and availability. The error response time will show gap or difference of time interval between the occurrences of the error and reporting of the error to the grid scheduler.

Table: 2 Database attributes table.

S. No	**User ID**	**Request Type**	**Job ID**	**Resource ID**	**Success**	**Failure**			
						Type of Failure	**Cause of Failure**	**Error Response Time**	**Impact of Failure(C,I,A)**
1.	xx	computational	01	0x889c	yes				
2	yy	service	02	1x880c	No	Resource Unavailable	Network Breakdown	t seconds	Availability Disrupted

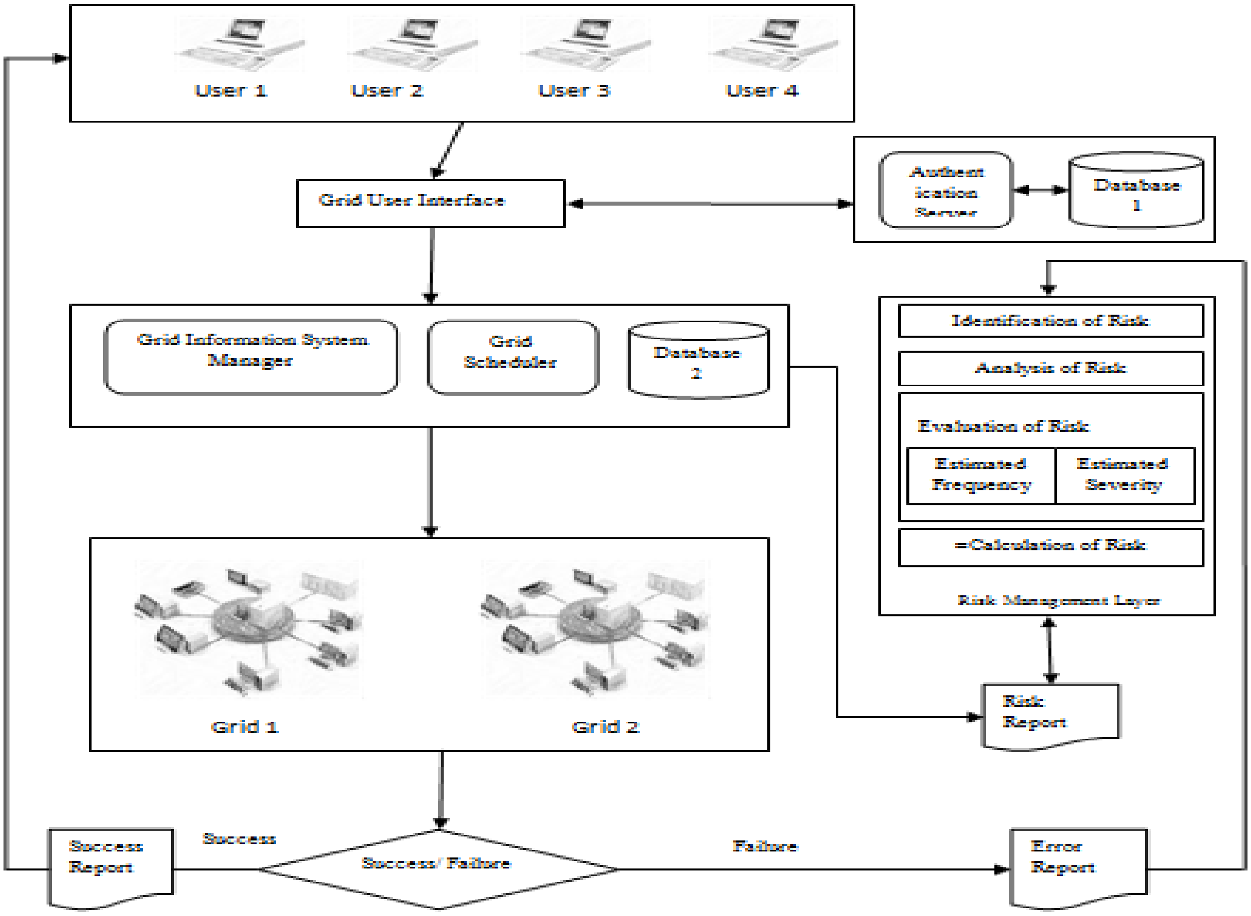

Figure 2. Process flow diagram for proposed grid model.

Figure 2 shows the following activities.

Step 1. Registered user's log-in using credentials for accessing the services provided by the grid.

Step 2. Registered users are authenticated by authentication server which is connected to database 1 which stores user's credentials which is provided by the user during registration process.

Step 3. Authenticated users ask for services and submit their job to the grid information system manager.

Step 4. Scheduler is allocating the reliable resource which has a least risk value, to the job by analyzing the risk report.

Step 5. After the process is done by the resource, a success or failure status report is submitted.

Step 6. If job is done successfully; acknowledgement is sent to the user and the success status log is updated this is maintained by the grid information system manager.

Step 7. If failure occurs; an error report is formulated and forwarded to risk management layer.

Step 8. Risk management layer analyze the error report and calculates the risk value and send it to the database 2 which merge the failure and success report.

Step 9. Finally, the log is updated in accordance with Table Number 2.

Step 10. The more number of processes, the more accurate will be the value for predicting the outcome.

V. CONCLUSION AND FUTURE SCOPE

Grid computing is rising as a powerful tool for performing large complex calculation among the scientist across the globe. With the increase in the efficiency and reliability for getting the output from grid resources, risk involved with the process in the grid could be reduced by a great deal. Proposed model with an addition of Risk management layer [11] makes the working of grid much more reliable and bring it close to a situation where number of faults or errors is very less and also provide information security by protecting Integrity, Availability along with Confidentiality [19][20].

The salient feature of this paper is that, it helps the grid manager in selecting the resource in an optimal manner by minimizing the risk that may lead to failure and provide stable selection of resources.

The approach is heuristic and evaluates different type of risk on the basis of risk management cycle and it classifies and prioritizes risk in terms of its confidentiality value, integrity value and availability value.

Currently in this paper, the work done by the grid manager for risk assessment and risk treatment is manual. Future work will focus on the extension of this paper, by proposing an automated solution for organizations with the use of neural networks and fuzzy logic which will enhance the precision for computing the risk for different jobs and increase the overall efficiency of the grid.

VI. REFERENCES

[1] Raid Abdullah Alsoghayer, "Risk Assessment Models for Resource Failure in Grid Computing," The University of Leeds School of Computing, February 2011, pp. 28-34.

[2] Foster, I., C. Kesselman, and S. Tuecke, "The Anatomy of the Grid, in Grid Computing: Making the Global Infrastructure a Reality," F. Berman, G. Fox, and A.J.G. Hey, Editors. 2003, J. Wiley: New York, pp. 169-197.

[3] Foster, I., "The Grid: A New Infrastructure for 21st Century Science, in Grid Computing: Making the Global Infrastructure a Reality," F. Berman, G. Fox, and A.J.G. Hey, Editors. 2003, J. Wiley: New York, pp. 51-63.

[4] Foster, I. and C. Kesselman, "Concepts and Architecture, in Thegrid: blueprint for a new computing infrastructure," I. Foster and C. Kesselman, Editors. 2004, Morgan Kaufmann: Amsterdam; Boston, pp.37-64.

[5] Berman, F., G. Fox, and T. Hey, "The Grid: Past, Present, Future, in Grid Computing: Making the Global Infrastructure a Reality," F. Berman, G. Fox, and A.J.G. Hey, Editors. 2003, J. Wiley, New York, pp. 9-50.

[6] Raid Abdullah Alsoghayer, "Risk Assessment Models for Resource Failure in Grid Computing," The University of Leeds School of Computing, February 2011,pp. 33-35.

[7] I. Foster and C. Kesselman, "The grid: blueprint for a new computing infrastructure," ed. 1999, San Francisco: Morgan Kaufmann Publishers.

[8] P. Latchoumy and P. Sheik Abdul Khader, "Survey on Fault Tolerance in Grid Computing," by P. Latchoumy and P. Sheik Abdul Khader, BSA University, Vandalur, Chennai, Tamil Nadu, India.

[9] http://www.ukessays.com/essays/engineering/a-survey-on-grid-computing.php#ixzz2NnAfzvMH[last accessed on 18th march 2013 2:45 pm]

[10] NIST Special Publication 800-37,"Guide for Applying the Risk Management Framework to Federal Information Systems," Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8930.

[11] http://en.wikipedia.org/wiki/Risk_management [last accessed on 18th march 2013 2:50 pm].

[12] Radha,"A Detailed Study of Resource Scheduling and Fault Tolerance in Grid", Dept. of Computer Applications, Sri Ramakrishna College of Engineering, Coimbatore-641 022, India And Dr.V.Sumathy Prof. Dept. of ECEs, Government College of Technology,Coimbatore-641 022, India.

[13] Krauter, K., R. Buyya, and M. Maheswaran, "A Taxonomy and Survey of Grid Resource Management Systems for Distributed Computing. Software: Practice and Experience," 2002. 32(2), pp. 135-164.

[14] Foster, I. and C. Kesselman, Chapter 2: "Computational Grid, in Thegrid: blueprint for a new computing infrastructure". 1999, Morgan Kaufmann Publishers: San Francisco, pp. 15-53.

[15] Chervenak, A., et al., "The Data Grid: Towards an Architecture for the Distributed Management and Analysis of Large Scientific Datasets Journal of Network and Computer Applications," July 2000. 23(3), pp.187-200.

[16] Foster, I., et al., "The Physiology of the Grid, in Grid Computing: Making the Global Infrastructure a Reality," F. Berman, G. Fox, and A.J.G. Hey, Editors. 2003, J. Wiley,New York. pp. 217-249.

[17] Yuan-Shun Dai and Jack Dongarra."Reliability and Performance Models for Grid Computing," Yuan-Shun Dai and Jack Dongarra, University of Tennessee, Knoxville.

[18] Site Assessment and Probabilistic Risk Analysis (PRA) of Grid Computing Facilities by Joe Higgins Staff Engineer Sun Labs and Robert Sewell Senior Staff Engineer Sun Microsystems.

[19] http://en.wikipedia.org/wiki/Grid_computing[last accessed on 18th march, 2013 3:15 pm].

[20] Hai Jin, W. Fan, Z. Wu, and J. Yang ,"Challenges of Grid Computing," (Eds.): WAIM 2005, LNCS 3739, pp. 25 - 31, 2005.