Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal

Vol. 1, No. 2, September, 2015

Performance Evaluation on Security Models in Computational Grid Security

Mughele, E.S.
Computer Science Programme
Delta State School of Marine Technology
Burutu, Delta State, Nigeria
prettysophy77@yahoo.com

ABSTRACT

Computational grid involves the organisation, management and distribution of diverse resources in dynamic, distributed virtual organizations. The element nature of computational grid, in which expansion and evacuation of users and resources happen, presents tough security fears that request new specialized methodologies. In this research, the authors focus on performance evaluation of some existing security models in computational grid. Grid security analysis and evaluation is not easy because of its complexity, largeness and stiffness. Due to the complexity of grid systems, involving many resources and many jobs being concurrently executed in heterogeneous environments, there are not many simulation tools to address the general problem of Grid computing security.

Keywords: Performance, Evaluation, Security Models & Computational Grid Security

Aims Research Journal Reference Format:
Mughele, E.S. (2015): Performance Evaluation on Security Models in Computational Grid Security.
Advances in Multidisciplinary (AIMS) Research Journal. Vol 1, No. 2 Pp 71-80.

1. INTRODUCTION

The concept of Computational Grid (or Grid) emerged in the late 90s as a result of rapidly increasing demand for computing resources and improvements in network technology. In the area of science, Grid applications have helped scientists and researchers to solve large scale computations such as numerical simulation and data processing. In the industry, it is recognized as an efficient technology for enterprise computing and business-to-business computing (Foster and Kesselman, 1999). Computational grid involves the organisation, management and distribution of diverse resources in dynamic, distributed virtual organizations. The element nature of computational grid, in which expansion and evacuation of users and resources happen, presents tough security fears that request new specialized methodologies (Foster et al., 2002). Computational grid is making use of idle computers resources in a network in order to meet computational demand of scientific projects requiring enormous resources that cannot be provided by single computer system such as supercomputers.

Main principle of interconnecting computers in computational grid is for the sole purpose of sharing computer resources in order to achieve higher computational power. Ian Foster, considered as the father of computational grids, envisioned that computational grid be likened to power grids in which the users of electricity know nothing about generation and distribution of electricity, he only make use of it. Computational grids are envisioned to have resources pooled together and make it available to the user who hook-up with the grids. However, Alexandru and Dick (2006) noted that key features of grids are still ardent research subjects, e.g., sophisticated resource planning strategies or the adaptation of existing applications to grids. Many of these features require in-depth knowledge of the behavior of grids, and realistic performance evaluation and comparison of existing and new approaches.

In this research, the authors focus on performance evaluation of some existing security models in computational grid. Grid security analysis and evaluation is not easy because of its complexity, largeness and stiffness. Due to the complexity of grid systems, involving many resources and many jobs being concurrently executed in heterogeneous environments, there are not many simulation tools to address the general problem of Grid computing security.

1.1 Background to the study

Grid computing involves sharing heterogeneous resources which are located in geographically distributed places belonging to different administrative domains (Bendahmane et al, 2009). Grid data sharing is not file exchange but rather access to computers, software, data and other resources. According to Foster, et al (2001), a Grid can be viewed as a Virtual Organization (VO). They define the Grid problem as flexible, secure, coordinated resource sharing among dynamic collections of individuals, institutions, and resources-what we refer to as Virtual Organizations. A simplified view is that a VO is a set of participants with various relationships that wish to share resources to perform some task. The VO can be an application service provider, a storage service provider, cycle provider and consultant engaged by a car manufacturer to perform scenario evaluation during planning for a new factory.

Research has shown that different methods of attacks are used on the grid, ranging from injecting malicious code into the grids by users and resources of the network is often attack by vicious application. Patrick et al. (2001) stated that porting a complex secure application from one security infrastructure to another is often difficult or impractical. While Kerberos security is founded on trusted third party with encrypted ticket for grid user's authentication, the Grid Security Infrastructure (GSI) is founded on public key infrastructure with X509 certificate for grid user's authentication. The researchers proposed method to migrate a system from Grid Security Infrastructure to Kerberos V5 security and emphasized on the need for designers of network security software to accommodate Generic Security Services Application Program Interface (GSSAPI).

Today, majority of grid systems rely on Grid Security Infrastructure for security which make use of public key infrastructure (PKI) and proxy certificate (Mohammed and Satoshi, 2010). PKI uses public key based authentication and encryption. Each grid user possesses a public key and private key that need to be kept safe. At the centre of PKI is the certificate which is used to identify the user and the public key associated with the user. Certificate Authority CA issues the certificate to user. As more users participate in the grid so is the quantity of public and private key generated increases as well as the certificate issues. The management of the certificate becomes a serious problem. As a result of this difficulty in managing, distributing and revoking compromised keys in Grid Security Infrastructure systems is generating an obstacle to wide use and adoption of Grid system (Baolin, et al 2006). This shows that no matter how effective and efficient a security model is, there is always performance trade-off among various metrics such as reliability, safety, security, optimization and scalability. Therefore, optimizing one or more metrics (in this case, safety and security) in a model leads to reduced speed (through put) as well as the scalability of the computational grid.

In general, there are two approaches for performance evaluation (Bacelli and Lin, 1992): deterministic models and probabilistic models. In deterministic models, it is usually assumed that the task arrival times, the task execution times, and the synchronisation involved are known in advance to the analysis. This approach is very useful for performance evaluation of real-time control systems with hard deadline requirements. In probabilistic models, the task arrival rates and the task service time are usually specified by probabilistic distribution functions. Probabilistic models usually give a gross prediction on the performance of a system and are good for easy stages of system design when the system characteristics are not well understood (Calin et. al., 2004). In this research, the focus is on evaluation of grid computing security systems in which various models will be considered and analysed and an efficient model with best performance gotten.

1.2 Research Motivation

The need for a performance analysis and evaluation of grid computing security systems capturing metrics such as reliability, safety, security, storage, speed and scalability cannot be overemphasised. A thorough evaluation will provide grid users with the most effective, efficient and appropriate computational grid security model to adapt and work with depending on their type of security demand. It is therefore cogent for grid users to know the inherent trade-offs and strength of any security model.

1.3 Problem Statement

Grid security analysis and evaluation is not easy because of its complexity, largeness and stiffness. Due to the complexity of grid systems, involving many resources and many jobs being concurrently executed in heterogeneous environments, there are not many simulation tools to address the general problem of Grid computing security. Building dependable grid systems is one of the most challenging research activities. The characteristics of grid systems make dependability a difficult problem from several points of view. The geographical distribution of resources and users that implies frequent remote operations and data transfers lead to a decrease in the system's safety and reliability and make it more vulnerable from the security point of view.

Moreover, adopting an efficient and appropriate model for grid security for user's various needs is tedious because no matter how effective and efficient a security model is, there is always performance tradeoff among various metrics such as reliability, safety, security, and speed and scalability. Therefore, optimizing one or more metrics (in this case, safety and security) in a model leads to reduced speed (through put) as well as the scalability of the computational grid. Therefore, this research is set out to develop a model that will evaluate the performance of some grid security models based on some metrics such as reliability, safety, security, optimization and scalability. This evaluation will help determine the model with the optimal performance among some of the existing computational grid security models.

1.4 Justification

The main security threats try to exploit the weaknesses of the existing security model. These threats tend to exploit protocols, operating systems, and attacks over databases, file sharing or multimedia applications, etc. Therefore, the need for a critical evaluation of security models which considers security aspects ranging from confidentiality of the data, authentication, non-repudiation, data integrity, access control, as well as key management cannot be overemphasized.

1.5 Research questions

The following research question includes:

1. How can the existing grid security models be analyzed and evaluated for optimal reliability and performance?
2. What tool can be applied for the performance evaluation of the existing grid security models?
3. What are the metrics to be considered for optimal performance in grid environment?
4. How can grid users select the most appropriate security model for their various needs in terms of access control, authentication and data integrity?

1.6 Aim and Objectives

The main objective of this research is to develop a model that will evaluate some of the existing computational grid systems to determine dependability which is a function of reliability, safety, availability, security, speed and scalability; this is to determine the security system with optimal performance. The set objective will be achieved through the following specific objectives

1. To analyze the existing grid security models and tools for optimal reliability and performance.
2. To offer the possibility of evaluating grid security in a more general context, considering the entire context of grid systems, with its specific characteristics.
3. To help grid users in selecting the most appropriate security model for their various needs in terms of access control, authentication and data integrity.
4. To developed a system which includes mechanisms for evaluating grid security models

1.7 Proposed Methodology

The methodology to this research study entails classifying various grid security models based on their characteristics and strength. This classification will be done under four (4) categories. Each category will be considered for performance evaluation based on their features. From the features obtained in any category, a fuzzy based evaluation system will be developed using security demand by a job and a trust evaluation of the resource site. Necessary analysis will be carried out using statistical methods of analysis.

This work will also include:

1. A simulation test of grid security sites with respect to their specific components and characteristics.
2. Analysis of results obtained from developed model and presented.
3. Obtaining analysis and developing the model using Microsoft excel and MATLAB

1.8 Scope of the Study

This research work is limited to the development of a performance evaluation model for grid security systems using fuzzy logic. This work reviews various literatures on grid security models that have been developed over the years. It proposes a fuzzy inference system evaluation of using security demand of jobs and the trust value (TV) of resource sites. This model is based on the assumption that all resource sites have prior agreements to participate in the Grid operations and that grid sites truly report their site configuration, computing power, and security conditions to each other. In other words, all sites are assumed cooperative in security and handling. Selfish Grids are not within the scope of this work. Testing and validation will be carried out and a model for efficient performance evaluation model for grid security systems is proposed.

2. RELARED LITERATURE

Computational grid is becoming popular among researchers to solve complex computational problem ranging from Engineering, Mathematics to science application such as weather forecast. Security of the grid is one major obstacle against wide use of the grid. Several attempts and methods have been employed to provide adequate security for users and resources in the grid against unauthenticated and unauthorised users with appreciable level of achievement. Patrick et al. (2001) stated that porting a complex secure application from one security infrastructure to another is often difficult or impractical. While Kerberos security is founded on trusted third party with encrypted ticket for grid user's authentication, the Grid Security Infrastructure (GSI) is founded on public key infrastructure with X509 certificate for grid user's authentication. The researchers proposed method to migrate a system from Grid Security Infrastructure to Kerberos V5 security and emphasized on the need for designers of network security software to accommodate Generic Security Services Application Program Interface (GSSAPI). Research has shown that different methods of attacks are used on the grid, ranging from injecting malicious code into the grids by users and resources of the network is often attack by vicious application.

The capability of biometric authentication for securing users authentication cannot be overemphasized, as this was emphasised in the research work of (Ratha, et al 2001). The researchers outlined the capability of biometric authentication system and identified the weak links in the system. They proposed a solution to some of the identified weak links. Marty et al (2005), categorised activities to be secured in the grid to include naming and authentication; secure communication; trust, policy, authorization; and enforcement of access control. The researchers then examined the available mechanisms in securing these activities and then proposed new methods for the security requirements of Grids. (Baolin et al 2006) proposed a security for grid based on trust model that compute and compare trust worthiness of entities in the autonomous and different domain. Their model provides different methods to deal with the malicious attack of users and resources belonging to the same or different domains and simulates experiment to evaluate the trust model. While this research work provides protection for grid users and resources against malicious attack, it did not address the problem of user and resources authentication.

Ming and Renato (2007) presented a Secure Grid File System (SGFS) which supports GSI-based authentication and access control, end-to-end message privacy, and integrity. The researchers used user-level virtualization of Network File System (NFS) to provide transparent grid data access leveraging existing, unmodified clients and servers. The researchers' method supports user and application-tailored security customization per Secure Grid File System session, and leverages secure management services to control and configure the sessions. The system conforms to the GSI grid security infrastructure and allows for seamless integration with other grid middleware. A SGFS prototype is evaluated with both file system benchmarks and typical applications, which demonstrates that it can achieve strong security with an acceptable overhead, and substantially outperform native NFS in wide-area environments by using disk caching.

Wenbo et al. (2008) proposed identity based signcryption scheme to meet the requirement of cross-domain authentication in computational grid. Based on their proposed scheme, the researchers presented identity based authentication model for multi-domain and mutual entity authentication. Although the proposed scheme is efficient in term of communication and computational cost, it has to battle with key distribution and management among participating entities.Shengbao et al.(2008), research is similar to Sindhuja et al (2009). The researchers examined certificateless authentication and key agreement protocol for securing the grid based on Diffie Hellman key agreement protocol. The protocol provides mutual authentication among users and resources in the grid and secured communication using common shared session key. Sindhuja et al. (2009) proposed identity based cryptography for grid security. The scheme was based on Hierarchical Identity Based Encryption and Hierarchical Identity Based Scheme. It was highly efficient and scalable when compared with previous similar scheme for grid security but not for grid user authentication. To improve encryption and decryption algorithm use in securing grid, (Hisham and Khaled 2009) used highly efficient scheme to accelerate RC4 algorithm, which is a stream cipher by about 873.52% when compared to other scheme to secure grid environment. Thus, time taken to identify and accept an authorised user is reduced while time taken to reject an unauthorised user also greatly reduced. The researchers only focused on how to improve encryption and decryption algorithm use in securing grid, however, a more efficient method for grid user authentication was not explored.

Safieh et al. (2009) proposed two level securities for grid security based on trust model system. The benefit of this model over previous trust models is the possibility of adding new domains without compromising the security of the grid and choosing of provider that has closest to users. Rather than using one server to store password, (Ruckmani and Sadasivam, 2009) used two separate servers; authentication server and backend server to store password for authenticating grid users. The protocol is based on the fundamental concept of trigon and the parameters of the trigon are used to authenticate the users of the grid. The user is assumed to be authenticated only when the two servers authenticate the user successfully. The main advantage of the model is that an adversary cannot achieve his aim by having access to one server and it is difficult to have access to the two servers by an adversary. The model involves the use of password for user authentication. However, if the password is compromised by any means, the two servers can therefore be accessed by an adversary.

Jaspher and Kirubakaran (2011) emphasised that the existing grid security is based on open grid security architecture (OGSA) which uses traditional PKI. They proposed authentication of the grid based on password, ID, biometric and position of the user. The results of the scheme provide enhance security and reduce operational time taken. The researchers also gave the advantage of their proposed scheme as a method for reducing disk space use during user authentication since reusability of the already authenticated biometric data will not be required for subsequent access to the grid resources. This however will enhance the user identification process. Abdulraheem et al (2014) presented an authentication model based on biometric fingerprint for computational grid security. The model has the advantage that the user chooses his own password for the card at will; the card stores the whole fingerprint. The fingerprints are integrated when the users have successfully completed the login process in the authentication phase. The model is robust toward authentication and network attacks.

The summary of the various schemes/models for securing the computational grid is presented in the table below (Table 1). From the table, it can be observed that no matter how effective and efficient a security model is, there is always performance tradeoff among various metrics such as reliability, safety, security, and speed and scalability. Therefore, optimizing one or more metrics (in this case, safety and security) in a model leads to reduced speed (through put) as well as the scalability of the computational grid. Grid security analysis and evaluation is not easy because of its complexity, largeness and stiffness. Due to the complexity of grid systems, involving many resources and many jobs being concurrently executed in heterogeneous environments, there are not many simulation tools to address the general problem of Grid computing security.

3. PROPOSED METHODOLOGY

3.1 Introduction

The methodology to this research study entails classifying various grid security models based on their characteristics and strength. This classification will be done under four (4) categories. Each category will be considered for performance evaluation based on their features. From the features obtained in any category, a fuzzy based evaluation system will be developed using security demand by a job and a trust evaluation of the resource site. A simulation test of grid security sites with respect to their specific components and characteristics. Necessary analysis will be carried out using statistical methods of analysis.

3.2 The Fuzzy Based Performance Evaluation Model

Adapted from the work of Shanshan Song et. al. (2005), where a Trusted Grid Computing with Security Binding and Trust Integration is developed, we propose a model specifically designed for the evaluation of security enforcement in computational Grids. This model applies fuzzy inference system to evaluate the security demand of jobs and the trust value (TV) of resource sites. The aim is to aggregate security demands of jobs and trust value of resource sites into a single value output. The aggregated values are then used to determine the security level (SL) of any Grid security model. To completely specify a job security demand, we need to use complex vectors of attributes to fully specify the requirements involving all of parameters and attributes as shown in fig 3.1 below.

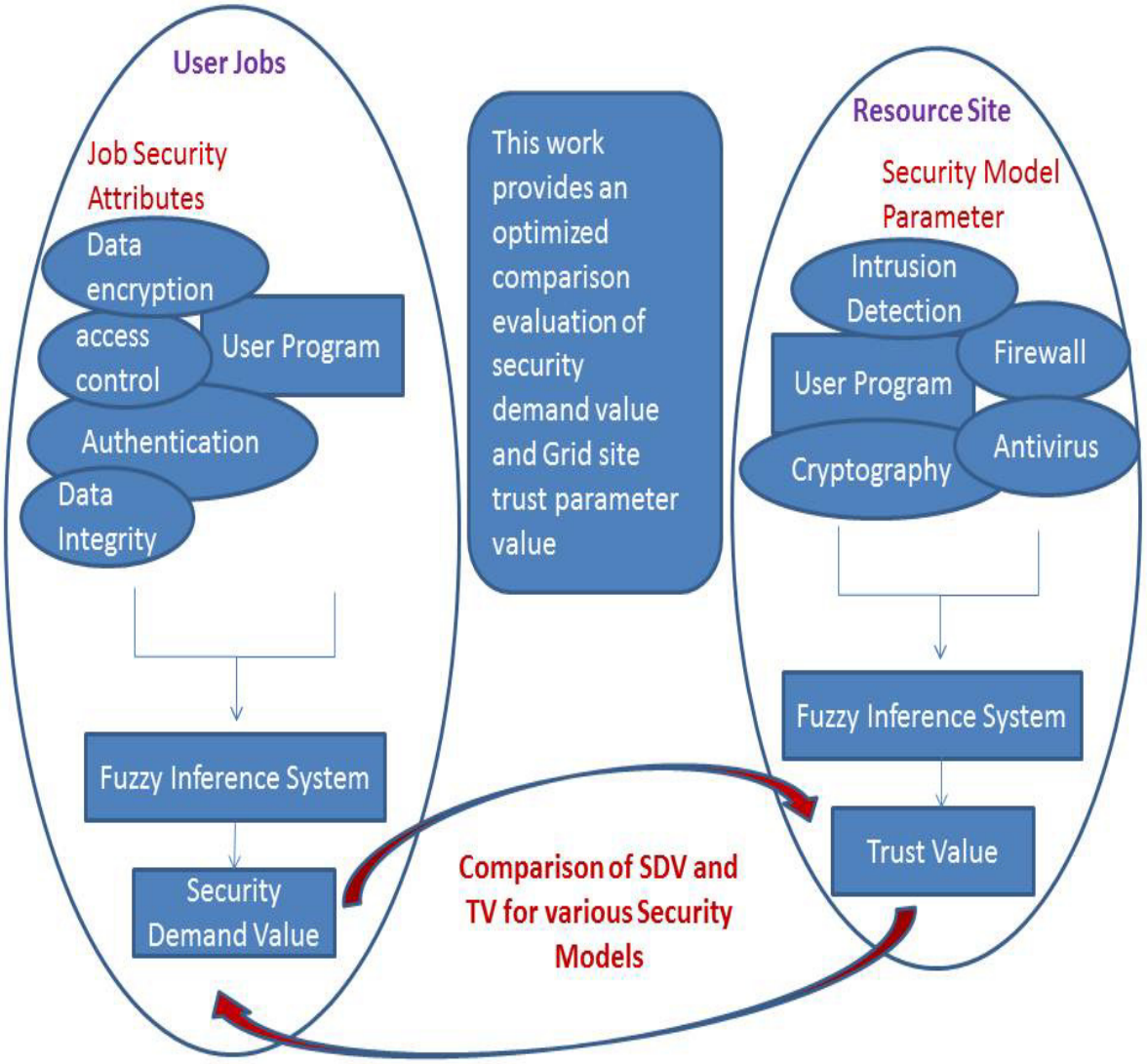

Fig. 3.1: The Fuzzy Based Performance Evaluation Model

In this work, the job Security demand value (SDV) is supplied by the user programs as a single parameter from aggregation. The demand may appear as a request for authentication, data encryption, access control, etc. The Trust value (TV) of a resource site is also lumped into a single parameter, which is aggregated through our fuzzy-logic inference process over all related parameters. Specifically, we propose a two level *fuzzy-logic based model* to enable the aggregation of numerous parameters and security attributes into scalar quantities that are easy-to-use in the Security evaluation analysis. The TV is normalized as a single real number with 0 representing the condition with the highest risk at a site and 1 representing the condition which is totally risk-free or fully secured.

3.3 The Fuzzy Inference System

The system is designed using fuzzy inference system which a popular computing framework based on the concept of fuzzy is set theory, fuzzy if-then rules, and fuzzy reasoning.

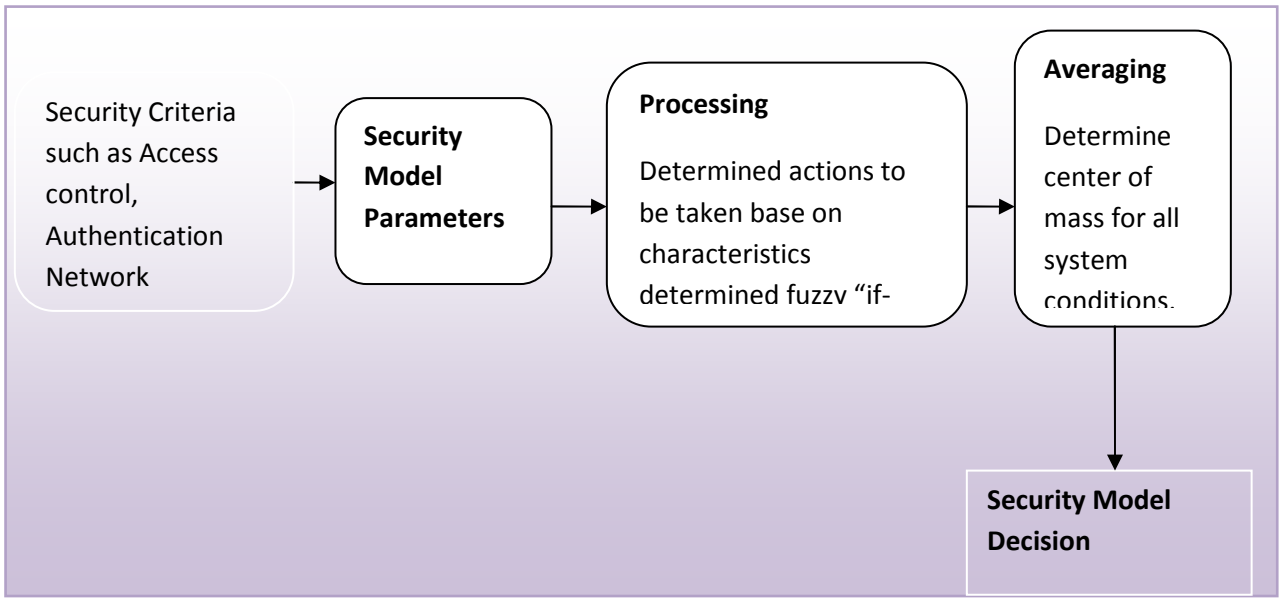

Figure 3.2: Architecture for Fuzzy Model

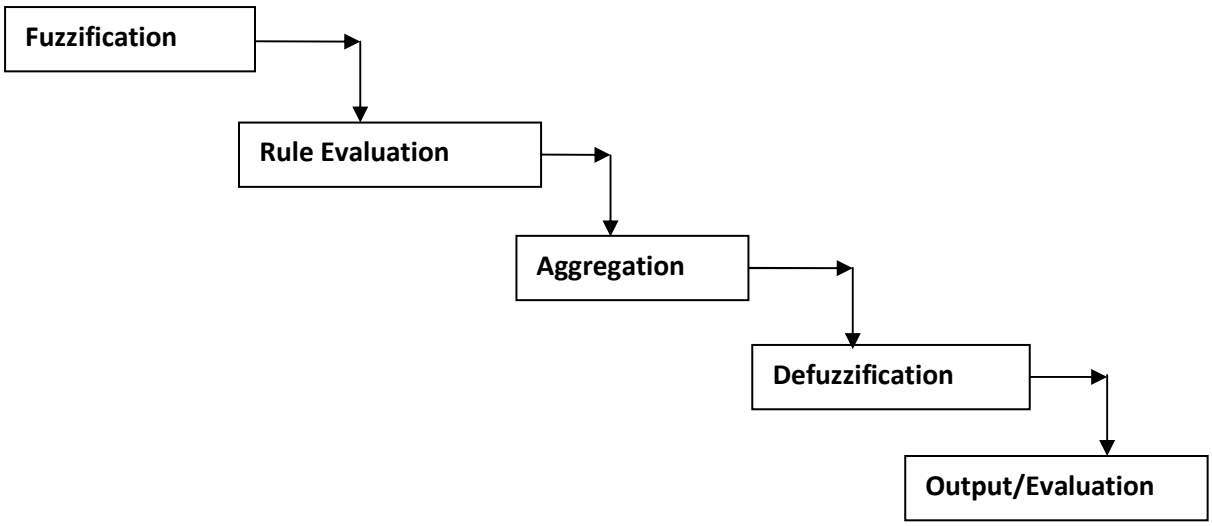

Fig. 3.3: Fuzzy Model Steps

A. Fuzzification: This is the process of changing parameter values to fuzzy values (linguistic values) with defined membership function. The first step is to take the crisp inputs and determine the degree to which these inputs belong to each appropriate fuzzy set. This crisp input is always a numeric value limited to the universe of discourse. Once the crisp inputs are obtained, they are fuzzified against the appropriate linguistic fuzzy sets.
Membership function is designed for each attribute which is a curve that defines how each point in the input space is mapped to a membership value (or degree of membership) between [0, 1].

B. Rule Evaluation: This is the second step where the fuzzified inputs are applied to the antecedents of the fuzzy rules. Since the fuzzy rule has multiple antecedents, fuzzy operator (AND or OR) will be used to obtain a single member that represents the result of the antecedent evaluation. We apply the AND fuzzy operation (intersection) to evaluate the conjunction of the rule antecedents. This step involves with the definition by using "if-then" rules to be relevant to human sense and proper path loss.

C. Aggregation of the rule outputs: This is the process of unification of the outputs of all rules. In other words, we take the membership functions of all the rules consequent previously scaled and combine them into single fuzzy sets (output). Thus, input of the aggregation process is the list of scaled consequent membership functions, and the output is one fuzzy set for each output variable.

D. Defuzzification: This is the last step in the fuzzy inference process, which is the process of transforming a fuzzy output of a fuzzy inference system into a crisp output. Fuzziness helps to evaluate the rules, but the final output this system has to be a crisp number. The input for the defuzzification process is the aggregate output fuzzy set and the output is a number. This step will be done using centroid technique.

3.4 Model Evaluation

An important feature of our model is that if a site's trust value does not match with job security demand, i.e., SDV > TV, our model will deduce the level of security disparity thereby comparing various values for different Grid security models. Any model with minimal security disparity is considered most secured i.e. the model with closest TV to SDV. This feature can be a guide for the site security upgrade.

We propose a fuzzy-logic based model with two basic assumptions as shown below:

1. All resource sites have prior agreements to participate in the Grid operations; and
2. The Grid sites truly report their site configuration, computing power, and security conditions to each other. In other words, all sites are assumed cooperative in security and handling. Selfish Grids are not within the scope of this work.

REFERENCE

1. Abdulraheem Muyideen, Aremu Dayo R., Adewole Kayode S. and Muhammed Kamaldeen J (2014) Fingerprint Biometric-Based Cryptographic System as a Security Approach in Grid Environment. Journal of computation and modeling vol 4, N0.2 Pp 41-58
2. Alexandru Iosup and Dick H.J. Epema, (2006), On Grid Performance Evaluation using Synthetic Workloads
3. Baolin, M., Jizhou, S., & Ce, Y.(2006), Reputation-based Trust Model in Grid Security System, *Journal of Communication and Computer*, **3**(8),
4. Bendahmane, M. Essaaidi, A. El Moussaoui, A. Younes, (2009) "Grid Computing Security Mechanisms: State-of-The-Art", International Conference on Multimedia Computing and systems ICMS '09, pp535-540,
5. Calin I. Ciufudean, Camelia I. Petrescu, and Constantin L. Filote, (2004),Performance Evaluation of Distributed Systems

6. F. Bacelli and Z. Lin (112), "Compresion properties of stochastic decision free Petri nets", IEEE Trans. Autom. Contr., vol 37, no. 12, pp. 1905-1920, 1992.
7. Foster, C. Kesselman, S. Tuecke, (2001) "The anatomy of the grid: enabling scalable virtual organizations", Int. J. High Performance Computing,
8. Hisham and Khaled.(2009), A New Accelerated RC4 Scheme Using Ultra GradSec and HIMAN and use this Scheme to secure HIMAN data, *5th International Conference on Information Assurance and Security*,
9. Ian, F., & Carl, K. (1998). *The Grid: Blueprint for a Future Computing Infrastructure.*Morgan Kaufmann Publishers Inc.San Francisco, CA, USA©1999 ISBN:1-55860-475-8
10. Ian Foster (2002) "What is the Grid? A Three Point Checklist", http://dlib.cs.odu.edu/WhatIsTheGrid.pdf. Accessed November 2014
11. Jaspher, W. K., &Kirubakaran, E.(2011), Biometric Authentication and Authorization System for Grid Security, *International Journal of Hybrid Information Technology,* **4**(4), 43-58
12. Marty, H., Mary, R. T., & Keith, R. J.(2005), Security for Grids, *Proceedings of the IEEE*, **93**(3),
13. Ming, Z., & Renato, J. F. (2007), *A User-level Secure Grid File System*, (Accessed June 2014)
14. Patrick, C. M., Wilbur, R. J., & Richard, J. D.(2001), Adapting Globus and Kerberos for a Secure ASCI Grid, *Association for Computing Machinery*, (Accessed June 2014)
15. Ratha, N. K., Connell, H. J., &Bolle, R. M.(2001), Enhancing security and privacy in biometrics-based authentication systems, *IBM Systems Journal*, **40**(3),
16. Ruckmani, V., &Sadasivam, S. G.(2009), A novel trigon-based dual authentication protocol for enhancing security in grid environment, *International Journal of Computer Science and Information Security*, **6**(3), 64-72.
17. Safieh, S., Amir, M. R., & Mehran, M.(2009), Proposed platform for improving grid security by trust management system, *International Journal of Computer Science and Information Security*, **6**(1), 143-148.
18. Sindhuja, R., Varsha, P., &Sumathi, G.(2009), An Improved ID Based Entitled Verifier Cryptography for Grid Systems, *International Journal of Recent Trends in Engineering*, **2**(1), 68-72.
19. Shengbao, W., Zhenfu, C., &Haiyong, B.(2008), Efficient Certificateless Authentication and Key Agreement (CL-AK) for Grid Computing, *International Journal of Network Security,* **7**(3), 342-347.
20. Shanshan Song, Kai Hwang and Yu-Kwong Kwok. (2005), Trusted Grid Computing with Security Binding and Trust Integration. Journal of Grid Computing (2005) © Springer 2005
21. DOI: 10.1007/s10723-005-5465-x
22. The Globus Security Team (2005) Globus tool kit version 4 Grid security Infrastructure: A standard perspective. http://toolkit.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf. accessed 20-03-2015
23. Wenbo, Z., Hongqi, Z., Bin, Z., & Yan, Y.(2008), An Identity-Based Authentication Model for Multi-Domain in Grid Environment, *International Conference on Computer Science and Software Engineering*, 165-169.