ABSTRACT

Grid is a kind of a Distributed Computing Technology. Both advances in network technology and computational infrastructure make it possible to construct large scale, high performance distributed computing environments known as Computational Grid. A Computational Grid is a hardware and software infrastructure that provides dependable, consistent, pervasive and inexpensive access to high end computing capabilities in a transparent manner. Such grid is used for modeling and simulating complex scientific problems like high energy physics, seismic analysis etc. The goal of a grid computing is to create Virtual Organizations (VO) across one or more Physical Organizations (PO) or Administrative Domains (AD). An AD is a collection of resources controlled by a single administrative authority and it is called PO. VO is a collection of diverse and distributed users and resources from various AD. Such VO's are facilitated by common grid middleware for following operations viz. Resource management, Data access and Management, Application Development environment and Information Services. The grid layered architecture is modeled by Global Grid Forum (GGF). Every VO needs to be governed by the rules and policies. Every organization participating in a VO for a task has already established its own security mechanism. Such organization when it becomes a part of a VO, VO's policy plays a crucial role in deciding and implementing the solution which is interoperable and scalable. The key challenge is forming a secured environment which is focused in the connectivity layer in Grid architecture.

Hence access to such VO must be properly established by setting Mutual trust and using proper authentication mechanism. The Authentication, Trust establishment and local data protection issues are focused in this research work.

The Public Key Infrastructure (PKI), X.509 and Transport Layer Security are the mechanisms used in the current Grid middleware Globus Toolkit GT 4.0 for authentication and confidentiality. The PKI certificates are used for authentication and proxy certificates are used for delegation in Single Sign On (SSO). The certificates are validated using either Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP). There are several problems associated with the existing certificate validation mechanisms CRL and OCSP. The drawback in the usage of CRL validation mechanism leads to the performance issue of scalability. The Objective of this work is focused on the scalability issue in the existing Grid Security Infrastructure Hence in this work a Hierarchical Web Service Based Time Efficient PKI Certificate Validation Service for Global Computational Grids is designed and its performance is compared with the existing Validation mechanisms. The proposed certificate validation mechanism is Scalable, Reliable and Extendable which can withstand attacks.

Every PO establishes its own security standards to fulfill its security requirements. When such PO becomes a member of VO; the PO's authentication mechanism and security policies may not align with VO's Security Policies. In case if two different AD's need to carry out any collaborative task there is a need for translation service so that it can coexist

with each other. Hence to handle this Credential Management Service (CMS) is designed and its performance is compared with the existing CMSs.

A Multifactor Authentication Service for Computational Grid is implemented using Service Oriented Architecture and it is compared with existing Credential Federation Systems. It is designated to perform the complicated time and resource consuming task of Credential management and Validation service. Its performance is compared with existing Credential Federation mechanisms.

In recent years there is a need for a security infrastructure for ubiquitous digital life without using Public key infrastructure and shared session key cryptography algorithms. The resources in such environment possess different characteristics. The need for security services for such resource restricted environment is a challenging issue.

Hence, in this research a set of novel algorithms are proposed that uses the macro feature of the fingerprint biometric of the sender and the receiver to generate key/(s). A Finger Print based Security Algorithm (FPSA) is proposed in this work. It uses the principal's finger print biometric feature for key generation. A set of algorithms are proposed to provide Authentication, Confidentiality and non-repudiation services with the smaller key size without any overhead. A suite of encryption and decryption algorithms are developed and tested with samples of finger prints collected from 135 individuals. The time taken for key generation, encryption and decryption is computed for FPSA and it is compared with RSA. The proposed

algorithm is highly suitable for smaller and resource limited devices. It serves as a model of trust by using biometric identity of the users.

Finally, Trust Management is crucial in dynamic grid since the stakeholders of Grid like Computational nodes and grid users join and leave the system. Any solution proposed for trust management is expected to possess the following characteristics like scalability and reliability. Reliability is measured in the face of failures in two perspectives. They are user's perspective and resource provider's perspective. The existing Trust assessment techniques are focused in the user's perspective. Hence the objective of this work is to design a Trust assessment model and to propose a Defensive Architecture. It is used to establish trust between the grid user and the resource provider in Resource Provider's perspective. In this model the subjective trust is established by computing end user's trustworthiness. It is assessed by implementing sets of policies applied at the end point before the grid resources are offered to the user thereby execution trust and code trust is provided.

This thesis proposes a working prototype for each of the above and it is tested by forming an experimental setup using GT 4.0.7. The results are compared to the existing mechanisms. The accomplishment of solutions to overcome these two issues like Scalability in existing authentication and reliability in Trust management provide promising features for the acceptance of Grid just like Internet.