

# Deliberate Secure Grid Computing Blueprint Design in Indian Context

Sanjeev Puri

Research Scholar, Manav Bharti University, Solan, India  
purispuri\_2005@rediffmail.com

Dr. Harsh Dev

Professor (CS&E), PSIT, Kanpur

**Abstract**— The novel concept of grid computing, clusters of computational power is constructed from a network of many small and widespread different computers servers or workstations into a single resource. We now proceed to translate the grid security problem into specific grid security requirements. The purpose of Grid technologies is to support the secure sharing and scalable coordinated use of diverse resources in dynamic, distributed VOs. We propose a secure blueprint design for grid systems that addresses requirements for single sign-on, interoperability with local policies of any grid city of India, with dynamically varying resource demands.

**Index Terms** — Grid Security Problem, Grid Security Requirements, Single Sign-On, Interoperability, Resource Demands

## I. INTRODUCTION

Grid computing means the hardware and software infrastructure that allows flexible and seamless sharing of heterogeneous network of resources for computing and data intensive tasks and provide faster throughput at lower costs. The infrastructure of an electrical power grid makes it possible for a person to access electricity by simply plugging into a wall socket, without being concerned with how and where the electricity used is generated. The concept behind grid computing is similar to that of the power grid. Organizations with both large and small networks have been adopting grid techniques in order to reduce execution time as well as to enable resource sharing.

A single large job can be split into smaller pieces and run on several, or several thousand, computers simultaneously, producing supercomputer speed from off-the-shelf hardware. Grid Computing enables the virtualization of distributed computing resources such as processing, network bandwidth and storage capacity to create a single system image, granting users and applications seamless access to vast IT capabilities. Just as an Internet user views a unified instance of content via the Web, a Grid user essentially sees a single, large virtual computer. At its core, Grid Computing is based on an open set of standards and protocols that enable communication across heterogeneous, geographically dispersed IT environments.

The Grid referred to an envisioned advanced distributed computing paradigm with capabilities to assist in solving complex science and engineering problems beyond the scope of existing computing infrastructures. The growing popularity has also resulted in various kinds of 'grids', common ones being known as Data grids, Computational grids, Bio grids, Cluster grids, Science grids, among many others. Effort is in progress to converge the concepts related to the architecture, protocols, and applications of these grids to formulate a *single* paradigm the Grid. Grid is type of parallel and distributed system that enables the sharing, selection and aggregation of geographically distributed resources dynamically at run time depending on their availability, capability, performance, cost, user quality of-self-service requirement. Grid Computing distinguishes from conventional distributed computing by applications by their simultaneous use and its focus on large-scale resource sharing, dynamic resource requirements, and use of resources from multiple administrative domains and high performance orientation. [1]

Grid computing, more specifically, a "data grid", can be used to aggregate this unused storage into a much larger virtual data store, possibly configured to achieve improved performance and reliability over that of any single machine. Grid system is established with storing capacity of data in petabytes, processing speed in terabytes and transmitting speed in gigabytes such type of huge capacity can be only met in large number of supercomputers work together, this can be achieved if one supercomputer is considering as a node is connected with other supercomputer and so on. Such type of a huge computing system can be achieved by forming a grid where node is equipped with supercomputer. The branches of nodes are made of optical fibers. The systems thus have electrical pulse movements within the computer and optical pulse movements in the branches. This hybrid system is called computational grid. [2]

In this paper, we first discuss the characteristics of grid computing in Indian scenario. Secondly, we discuss our aim and goals of secure grid computing in major domains or cities of India. Thirdly there is need to form computational VOs Grid and discuss the resource sharing coordinated problem solving in dynamic Multi-institutional grids in major cities. After that we discuss the blueprint design technology, tools and requirements

and challenges to fulfill our aim. Finally, we implement of the proposed Grid security framework in Indian scenario.

As the computational system in India are large number in nature such as scientific processing, medical processing, collaborative processing, legal processing, defense processing are even space technologies processing, metrology processing. In grid system specially like country India, the formation of topology is done first by selecting a node is a supercomputer hence it should be house in a town where there are sufficient number of uses for the computer. This node will be having a large family of computers connected to it including mainframes and many personal computers through servers. It should have provision to interact with the computers of its family. [6]

The characteristics of grid computing in Indian scenario are:

1) The user population of major cities is of variable size, large and dynamic including members of many institutions and will change frequently.

2) The resource pool is large and dynamic. The quantity and location of available resources can change rapidly.

3) A dynamic group of processes running on different resources and sites and a variety of mechanisms, including unicast and multicast. Grid coordinates resources that are not under centralized control. It utilizes standard, open, general-purpose protocols and interfaces.

4) Resources may require different authentication and authorization mechanisms to coordinate diverse access control policies and to operate securely in heterogeneous environments. In this framework follow common inter-grid protocols for authentication, authorization, access control, resource discovery, resource access, and resource sharing.

5) These should include Kerberos, plaintext passwords, Secure Socket Library (SSL), and secure shell, PKI and PMI infrastructure at grid layer ensure proper authentication and authorization, digital certificates at different levels of users. And promise to deliver non-trivial qualities of services at different sites.

6) Resources and users may be located in different cities or VOs sites. In large scale country like India and An individual user will be associated with different credentials, or accounts, at different virtual sites at different cities of India.

The Grid Computing discipline provides mechanisms for resource sharing by forming one or more virtual organizations providing specific sharing capabilities.[3] Such virtual organizations (VOs) are constituted to resolve specific research problems with a wide range of participants from different regions of the world. This formation of dynamic virtual organizations provides capabilities to dynamically add and delete virtual organization participants, manage the "on-demand" sharing of resources, plus provisioning of a common and integrated secure framework for data interchange and access. The grid computing has emerged to cater the need

of computing-on-demand. In grid computing, geographically dispersed heterogeneous computing stations belonging to diverse administrative domains can connect to the grid and offer services or request services in a loosely coupled environment with services-on-demand style. Grid computing exploits idle or unused processing cycles of all capable computers in a network in order to solve problems.

The main goals of secure grid computing in Indian context are: [8]

- To link surplus computing power and other spare resources with different grid cities' clients of India who have periodic needs beyond the capacity of their machines. Analyze the unique security requirements of grid computing framework according to Indian cities topographies and processing of nodes of different cities or sites.
- Investigate security requirements to specifications according to nodes attributes.
- Grid computing software divides a task into subtasks, finds spare processors and other critical resources on the network, distributes the subtasks, monitors their progress and restarts any subtasks that fail. Grid computing engines aggregate the results of the subtasks of different cities of India so the job or task can be completed.
- The real basis of grid computing is coordinated secure resource sharing (Sharing in a grid sharing of files, hardware, software, data and other resources), and problem solving in a dynamic, multi-organizational cities of Indian environment.
- The inter-domain security solutions used for grids must be able to interoperate with, rather than replace, the diverse intra-domain access control technologies inevitably encountered in individual domains. A security policy that addresses requirement for single sign-on interoperable with local policies.
- Optimized network reliability, computing, and operational support for grid communications. Founding of an India's Grid framework for meeting regulatory compliance requirements with secure access and data privacy for smart grid information.
- To study different possible security threats in intra-grid. To investigate how DoS attack affect the grid performance.
- Specific technical issues raised by this policy, including local heterogeneity and scalability.
- Evaluation of existing security framework with proposing Grid security model and new protocols that provide seamless fault free high speed access to the compute, data & other resources on the Grid among these major cities of India.

There is enormous concern about data and application security both during its flow across the Internet and also when staged on the grid resources like more grid nodes in India like country. The first concern is mainly because it is possible for someone to tap your data (passive listeners) and possibly modify it on its long path. The second concern is that when you use others computers or nodes in the grid, it is possible that the owners of those

computers may read your data. These can be addressed by sophisticated encryption techniques both during transmission and also during their representation/storage on external resource.

Scalability, performance and heterogeneity are desirable goals for any distributed system, the characteristics of computational grids lead to security problems that are not addressed by existing security technologies for distributed systems. However, without an adequate understanding of the security implications of a Grid, both the Grid user and the system administrator who contributes resources to a Grid can be subject to significant compromises in security. The importance of security-related issues will amplify as Grid usage becomes more common place. Before a user runs an application on a particular machine, the user may need assurances that the machine has not been compromised. When a user's job executes, the job may require confidential message-passing services, which might not be the default. [4]

A user or the Grid infrastructure software may set up a long-lived service such as a specialized scheduler and require that only certain users be allowed to access the service. In each of these cases, the developer of the application must expect these security requirements and design with invoker of these applications must understand how to check if these security services are available. The purpose is to review the various Grid usage scenarios and analyze their security requirements and implications. These scenarios are designed to provide guidance for the Grid user, the Grid application developer, and the Grid resource provider.

We propose a security framework policy for grid systems that addresses requirements for single sign-on, interoperability with local policies of any grid city of India, and dynamically varying resource requirements. It focuses on authentication of users, resources, and processes and supports all combinations of users, resources and processes authentication. We also describe security framework with adaptive protocols that implement policy in context of Indian scenario.

Grid Computing enables the creation of virtual organizations, including many participants from various governmental agencies of India (e.g., state and federal, local or metro cities etc.). This is necessary in order to provide the data needed for government functions, in a real-time manner, while performing the analysis on the data to detect the solution aspects of the specific problems being addressed. The formation of virtual organizations, and the respective elements of security, is most challenging due to the high levels of security in government, renowned private sector, and the very complex requirements.

The heterogeneous nature of resources and their differing security policies in India are complicated and complex for security schemes of a grid computing environment. These computing resources are hosted in different security domains and heterogeneous platforms in different Indian cities' functionality. The major security requirement for the grid is centered on the

dynamic configuration of its security services, such as data integrity, confidentiality, and information privacy in potentially volatile environments. [5]

The problem thus becomes altogether new as grids are yet to come in existence. The topography and in an entire network of grid of India is in blueprint stage and the study will be useful in days to come. The Indian Grid Certification Authority (IGCA) provides X.509 certificates to support the secure environment in grid computing. IGCA is an accredited member of the APgridPMA (Asia Pacific Grid Policy Management Authority) for Grid Authentication. We require a grid security model that allows users to create entities and policy domains in order to create and coordinate resources within virtual organizations.

## II. MOTIVATION TOWARDS GRID SECURITY

It is no unusual situation for Grid system that plenty of resources handling confidential data are shared on multiple sites by a large number of users from a variety of organizations. Security of such system is a critical issue, because not only data, but also hosts, resources and computations have to be secured from improper access. Based on such characteristic, several aspects of Grid security will be presented.

The identity of every user has to be confirmed in order to enter the system. In addition, authentication of the server can ensure that resources and data are not provided by an attacker. Every authenticated user has to be authorized to access individual resources. It is difficult mostly because of the scalability and evolution of Grid systems. Besides, resources are often owned by multiple administrative domains, which make the administration difficult and demands complex, distributed authorization policies. One of the aspects is to enable users to use multiple resources without the need to authenticate multiple times on their providers' hosts.

Secure communication has to be encrypted and signed. Encryption is a technique to ensure confidentiality prevents the communication from being eavesdropped by an unauthorized third party. Digital signature ensures the communicating parties that the messages have not been modified on their mode or manner.

We should have to protect the code running on shared computational resources from others; on the other hand, we have to ensure that no user's code will negatively affect the system, other computations or data. Violations can occur, indeed. In such situation it would be sensible to have some logs and chains of accountability for actions that took place on the system, to find the liable user. The ability should be to limit or charge for consumption of grid resources.

## III. VIRTUAL ORGANIZATIONS (VOS) IN GRID

A virtual organization is either an individual or an organization willing to share their resources with others [3]. A resource could be compute power, software or storage. Service level agreements define how a member of a virtual organization can access the resources. Virtualization is the logical separation between services

and the underlying physical resources. It is possible to run entire operating systems, applications, or services independent of the underlying system. The ability to display a desktop from one computer on another computer is called desktop virtualization. Prominent examples are Virtual Network Computing. Just like network virtualization, storage virtualization is a logical abstraction of physical storage. A RAID over one or more disks is fitted for the example. The ability to run whole operating systems inside a container is called server virtualization or machine virtualization. The container is named virtual machine.

Applications benefit from this type of virtualization as they can run unmodified and have an entire software stack e.g., libraries. System-level virtualization allows to run multiple, logically distinct system environments on a single instance of an operating system kernel. It is based on the change root concept available on all UNIX systems. Para-virtualization attempts to avoid the drawbacks of full virtualization by presenting Virtual Machine Monitor that is similar, but not equal to the underlying hardware. The approach promises higher performance, but it requires modifications to the guest operating system.

VO lifecycle includes phases such as identification, formation, operation/ evolution and dissolution. The identification phase is dealing with setting up the VO; this includes selection of potential business partners by using search engines or looking up registries. VO formation deals with partnership formation, including the VO configuration distributing information such as policies, agreements, etc, and the binding of the selected candidate partners into the actual VO. After the formation phase, the VO can be considered to be ready to enter the operation phase where the identified and properly configured VO members perform accordingly to their role. Membership and structure of VOs may evolve over time in response to changes of objectives or to adapt to new opportunities in the business environment. Finally, the dissolution phase is initiated when the objectives of the VO has been fulfilled.

Generally, relevant identification information contains service descriptions, security grades, trust and reputation ratings, etc. Depending on the resource types, the search process may consist in a simple matching e.g., in the case of computational resources, processor type, available memory and respective data may be considered search parameters with clear cut matches or in a more complex process, which involves adaptive, context-sensitive parameters.

During the formation phase a central component such as a VO Manager distributes the VO level configuration information, such as policies, SLAs, etc. to all identified members. These VO level policies need to be mapped on local policies. This might include changes in the security settings e.g. open access through a firewall for certain IP addresses, create users on machines on the fly, etc. to allow secure communication.

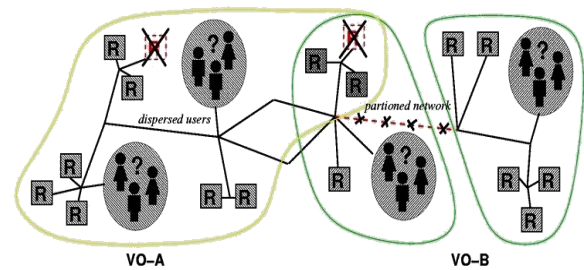


Figure 1: Secure Computational VOs Grid: Resource sharing coordinated problem solving

Throughout the operation of the VO, service performance will be monitored. This will be used as evidence when constructing the reputation of the service providers. Any violation -e.g. an unauthorized access detected by the access control systems- and security threats -e.g. an event detected by an intrusion detection system- need to be notified to other members in order to take appropriate actions. Unusual behaviors may lead to both a trust re-assessment and a contract adaptation. VO members will also need to enforce security at their local site. For example, providing access to services and adapting to changes and the violations.

During the dissolution phase, the VO structure is dissolved and final operations are performed to withdraw all contractual binding of the partners. This involves the billing process for used services and an assessment of the respective participants' (or more specifically their resources) performances, like amount of SLA violations and the like.

In Grids, independent sites or institutions having similar interests are forming loosely coupled virtual organizations for collaboration and resource sharing. In a Grid environment, where identities are organized in VOs that transcend normal organizational boundaries, security threats are not easily divided by such boundaries. Identities may act as members of the same VO at one moment and as members of different VOs the next, depending on the tasks they perform at a given time. Virtual organizations need to share resources such as data archives, computer cycles, and networks, underlying any sharing mechanism is the ability to authenticate the identity of the requestor of a resource, and to determine if the requestor is authorized to make the resource request. [6]

An further risk is there in Indian environment, that have multiple sites in many of Grid' cities in which when multiple VOs or sites share a virtualized resource such as a server or storage system where each of participating VOs may not trust each other and therefore, may not be able to validate the usage and integrity of the shared resource. Security solutions that focus on establish a perimeter to protect a trusted "inside" from an un-trusted "outside" (e.g., firewalls, VPNs) are of only limited utility in a Grid environment. Each site has a local intranet security solution such as Kerberos or Public Key Infrastructure (PKI).

Libvirt library is collection of software that provides a convenient way to manage virtual machines and other

virtualization functionality, such as storage and network interface management. These software pieces include an API library, a daemon (libvirt d), and a command line utility. A primary goal of libvirt is to provide a single way to manage multiple different virtualization providers.

```
import libvirt
import sys
conn
libvirt.openReadOnly(dom1.IndianCity1(),dom1.OSType
())
if conn == None:
print "Failed to open connection"
sys.exit (1)
```

Table1: Program of Libvirt shows running VO's

In particular, we have to deal with the fact that for a variety of issues relating to certification, group membership, authorization, and the like, participants in such VOs represent an overlay with respect to whatever trust relationships exist between individual participants and their parent organizations. Two organizations, A and B each operate their own corporate security solutions that address certification, authentication, authorization, and so forth. Between the two organizations, however, no trust relationship exists. We now assume that an entity in sub-domain IndiansubCity A1 wishes to access a resource managed by another individual in sub-domain IndiansubCity B2 with whom he is engaged in some collaborative activity.

In principle, the establishment of such a sharing relationship should be straightforward. In practice, however, it can be extremely difficult for at least three different reasons:

#### A. Cross Certification

The entity from A can obtain a credential certified by some certification authority in domain A. But in the absence of a trust relationship between A and B, an entity in domain B cannot enforce policies requiring that that credential is issued by an approved certification authority. We need a means of establishing cross certification between A and B or rather we need a means of establishing cross certification among the entities participating in the VO. VO participants agree to use X.509 credentials and GSI protocols as common mechanisms. To address the cross certification requirement, they also agree to trust a VO service, the Kerberos-CA service, as a means of gateway from domain A's Kerberos credentials to VO X.509 credentials. An entity in A that wishes to issue a request to an entity in B must thus first issue a Kerberos-authenticated request to the Kerberos-CA service to obtain an X.509 credential that asserts the requestor's Kerberos principal name. [7]

#### B. Mechanisms and Credentials

Assuming that the cross certification problem is solved, we then face another problem. A, B both may rely on quite different security mechanisms and credential formats. The A1 entity, the requestor, can then present this credential to the entity in B1. The latter entity has a

trust relationship with the Kerberos-CA service and can thus verify the authenticity of the credential. Example by checking the signature chain prior to applying VO policies based on the requestor's Kerberos principal name and or local policies to determine whether the request should be granted.

#### C. Distributed Authorization

Another difficulty that arises is that individual entities in one domain are not necessarily well positioned to know all foreign requestors and thus to enforce fine grained policies based on identity or other characteristics. A solution to this problem is to outsource fine grained policy administration to a trusted third party within the requestor's domain or the VO domain, who can more easily maintain information about all requestors. The local domain can, of course, continue to maintain and apply coarse grained policy locally.

The application consists of several grid services that pre-process and analyze large video files. An input video is split into several smaller parts to facilitate parallel execution of the analysis processes. The analysis consists of a face detection algorithm that includes several other algorithms. Every frame of a video snippet is analyzed to find shapes that look like faces. Every face that appears and the length of its appearance are stored; making it is possible, for example, to determine the total time that different characters appear in the material. Depending on the result of a frame's analysis, some deeper analysis might be needed. Being able to execute an application on multiple remote sites is one of the big advantages of multi-site grid computing. Nevertheless, this is not possible on most of the sites because the nodes are kept private and not accessible to the outside world. Once these changes, proper mechanisms to shield the nodes as well as the data need to be in place. An efficient solution for sharing grid computing resources on a single physical machine is to use virtualization.

## IV. SECURITY TECHNOLOGIES IN THE GRID

The traditional security areas play an important role in defining security for the Grids and the associated technologies. We build this analysis on previous surveys on security for the Grids [8] [9].

#### A. Authentication

Authentication deals with verification of the identity of an entity within a network. An entity may be a user, a resource or a service provided as part of the Grid. Authentication is one of the mechanisms helpful in implementing certification trust. One of the technologies playing a central role in authentication is Public Key Infrastructure (PKI), which defines message formats and protocols that allow entities to securely communicate claims and statements. The most popular PKI is defined by the IETF's PKIX working group, which defines a security system used for identifying entities (users and resources) through the use of X.509 identity certificates. In this PKI, highly trusted entities know as certificate authorities (CA) issue X.509 certificates where essentially a unique identity name and the public key of

an entity are bound through the digital signature of that CA.

PKI relies upon the periodic distribution of Certificate Revocation Lists (CRLs) in order to allow those relying upon certificate to gain confidence in their present validity. The use of CRLs needs careful management, particularly in relation to the frequency of updates. An important issue in authentication is the storage of credentials. Credential-storage systems take the responsibility of storing credentials securely, so that users can get credentials anytime on demand. Users are registered only at their home site rather than at each resource provider. Resource providers rely on users' home sites to provide identity information as well as attributes about users.

### B. Authorization

Authorization deals with the verification of an action that an entity can perform after authentication was performed successfully. In a grid, resource owners will require the ability to grant or deny access based on identity, membership of groups or virtual organizations, and other dynamic considerations. Thus policies must be established that determine the capabilities of allowed actions. Authorization is closely related to access control trust. A good description of the current state of authorization in Grid computing appears in [Cha05].

There are more than a few architectural proposals for handling authorization in Grids. One of the earliest attempts at providing authorization in VOs was in the form of the Globus Toolkit Gridmap file. This file simply holds a list of the authenticated distinguished names of the Grid users and the equivalent local user account names that they are to be mapped into. Access control to a resource is then left up to the local operating system and application access control mechanisms.

The Community Authorization Service (CAS) allows a resource owner to grant access to a portion of his/her resource to a VO (or community hence the name CAS), and then let the community determine who can use this allocation. The resource owner thus partially delegates the allocation of authorization rights to the community. This is achieved by having a CAS server, which acts as a trusted intermediary between VO users and resources. Users first contact the CAS asking for permission to use a Grid resource. The CAS consults its policy and if granted, returns a digitally self signed capability to the user optionally containing policy details about what the user is allowed to do. The EU DataGrid and DataTAG projects developed the Virtual Organization Membership Service (VOMS) [Alf03] as a way of delegating the authorization of users to managers in the VO. VOMS is a system to attach a set of membership information (VOname, group and/or roles) to a user's own credentials, therefore allowing services to authorize users on the basis of these attributes instead of having to specifically list all users.

For authentication, Akenti relies on X.509 certificates and the SSL/TLS protocol to securely authenticate a user, like most PKI-based systems. For authorization, Akenti uses a pure pull model. When a resource request comes, the Akenti policy engine collects all relevant certificates

from both the user and the resource, and derives the user rights from them. It is the server side that contacts all authorities once the user gets authenticated. One potential problem within Akenti is its policies are expressed using a proprietary XML format rather than X.509 based. Unlike Akenti's distributed and hierarchical policies, the policy in PERMIS is a single attribute certificate stored in a LDAP directory. It supports the role based access control (RBAC) paradigm, which means PERMIS infers the access right (roles and attributes) according to the given user's DN, a resource and an action.

### C. Confidentiality & Privacy

The data being processed in a Grid may be subject to considerable confidentiality constraints, either due to privacy concerns or issues of intellectual property. As mentioned in [Bro03b], confidentiality is usually associated with the encryption of data only, however there are many aspects to be considered for the case of Grids. The use of Grids implies that confidential data is stored in online accessible databases. Access to their interfaces must be carefully controlled, both to allow access only to appropriate users, and also to allow queries and simulations to run over these highly confidential data without that data being compromised or revealed. If the database is to be shared in a Grid, it might need to be operated by a trusted third party. A further novelty of Grid applications is that they may entail running confidential code or using confidential data on a remote resource; running a job on a dynamically-selected cluster according to load may be good resource management.

Confidentiality is extended also to the privacy requirements of the actual users and resources. Users are protected under privacy laws and these must be adhered by all components of proposed Grid technology. Privacy-Enhancing Technologies (PET) have been defined as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system" [Bor01]. PET could increase privacy of Grid applications. Adaption and implementation of these technologies for Grids are areas of open research.

There are several principles in consideration when building PET: transparency, being aware of what personal data is transmitted / prompted and how it is processed; data minimization, reduction of processed personal data by anonymity and pseudonymity procedures, minimizing the link ability between a person and the personal data; system integration, privacy protection built into the system; user empowering, privacy self-protection for users; and multilateral security, realization that only minimal trust in other parties is required. Examples of existing PETs include: Wallets of multiple virtual identities; which allow the efficient and easy creation, management and usage of unlink able virtual identities; and, anonymous credentials, asserted properties/attributes or rights of the holder of the credential that don't reveal the real identity of the holder and that only reveal so much information as the holder of the credential is willing to disclose.

## V. SECURITY CHALLENGES OF GRID COMPUTING IN INDIAN CONTEXT

In India computational grids, the problem of resource discovery and matching the job to suitable resources is a real challenge because of the large number of resources, their heterogeneity, availability and the variety of resource attributes such as CPU load and disk space. The grid must also cater for multiple users from different sites of India, who may potentially be interested in the same resource, without knowledge of each other's existence or interests. One grid composed of many smaller grids joined together, forming a global network of computers that can operate as one vast computational resource. Across India, researchers and software engineers are working to bring "the grid" closer to achieving the dream.

Now, a new computing paradigm appeared and resolved many of the unresolved grid problems: Today it is accepted that it is about offering different types of services. This includes applications (called software as a service), computing platforms (called platform as a service) and finally, raw computing resources (called infrastructure as a service). Usually, the last point is realized by using operating system virtualization. Although cloud computing sounds similar to grid computing, a new kind of business model: computing resources are bundled into services and offered on-demand. Customers no longer have to own their resources; they can rent/lease their resources and pay only for their actual usage. [10]

The security challenges faced in Grid computing of India are:

- i. Services hosted in different virtual organizations exist in different cities of India that have different security mechanisms and policies will be able to invoke each other through Interoperability solutions.
- ii. Interfaces should be abstracted to provide an extensible architecture with integration solutions.
- iii. Enforce trust policies within a dynamic Grid environment in Indian context.
- iv. A secure grid framework is built from multi-purpose adaptive dynamic protocols and interfaces.
- v. Secure grid computing framework allows its ingredient authentic resources to be used in a coordinated style to deliver various qualities of service such as response time and security.

The number, size, and scalability of security components such as user registries, policy repositories, and authorization servers pose new challenges.

## VI. THE GRID SECURITY PROBLEMS IN INDIA

As the computational system in India is large scale in nature. As the computational system in India are in large numbers. A grid environment involves large-scale sharing of resources within various virtual organizations established among different cities of India. Therefore it is planned in the present work to allocate the type of programming in a particular node hence when a user desires to avail the grid facility; the host node should handover the problem to the expert node when software is loaded. The other types of programs which are complex

in nature and they require the participation of many nodes. The host computer evaluates the problem and transfers the modules to the participated computers. The third types of software used to such that it is divided in modules equal to the number of grid nodes and all the participating computers processing paralleled, then the responses of each computer are integrated in the host node and which transfers the result to the originating personal computer. [11]

To consider any example, if in an analysis program, which mail code to the remote location where the data is store up (A city site). Then it needs to run a simulation in order to compare the tentative results with predictions. Hence, it contacts a resource broker service maintained by the collaboration (B city site), in order to locate idle resources that can be used for the simulation. The resource broker in turn initiates computation on terminals at two sites (C and D city site). These computers access parameter values stored on a file system at yet another site (E city site) also communicate among themselves using specialized protocols, i.e. multicast and with the broker, the original site, and the user. In this regard, we first analyze of the security problem in computational grid systems and its applications. We should be able to discuss technical and operational issues raised with grid policy, including local heterogeneity and scalability problems and it demonstrates via large-scale deployment in different sites of grid framework for India.

To considering the problem of inter-grid interoperability among different versatile sites of India, the basic idea is how to define the minimal set of Grid services. If we get the minimal set, any resource requests can be uttered by those elements in the minimal set. Based on the minimal set, we can do some translation between different resource description mechanisms. For examples, Grid city site A sends request to Grid city site B. Even Grid city site B does not understand this content of description, because they come from the same set, we can translate the request to understandable one.

The motto of the grid computing is to resolve some common problems with enterprise. The problems of applications clusters that lead to underutilized, dedicated hardware resources, the problem of very large expensive system hardly to maintain and difficult to change. The problems of distributed fragmented non-integrated information cannot be fully exploited by enterprise.[3]

Grid was brought to its knees by a distributed denial-of-service (DDOS) attack, necessitating an emergency login procedure change. While grid computing may very well revolutionize enterprise computing, the incident underscores the security risks that could prove quite harrowing for enterprises that rely on grid computing.

The attack was levied against a sample text-to-speech application made available without a login requirement. When the attack occurred, we took it in stride by moving the application inside where login is required.

One of the main problems is the shared use of the node's operating system, since it is easy to attack other users within the same operating system once on acquires the higher level of privileges needed to install software.

An efficient solution for sharing grid computing resources on a single physical machine is to use virtualization.

In understanding protocols view, SSH provides a strong system of authentication and message protection but has no support for translation between different mechanisms. It requires that users manage their own cross-site authentication relationships, by copying public keys to each site for which remote access is required. PGP cannot support encrypted exchange of information with people who do not use PGP. Using Kerberos for inter-site authentication would require that it also be used for intra-site authentication that is simply not feasible. The practical difficulty encountered in negotiating cross-realm authentication agreements. Kerberos requires the explicit involvement of site administrators to establish inter-domain trust relationships.

Each domain typically should have its own authorization infrastructure that is deployed, managed and supported. It will not typically be acceptable to replace any of these technologies in favor of a single model. Each domain in a Grid environment is likely to have one or more registries in which user accounts are maintained.

At the protocol level, we require mechanisms that allow domains to exchange messages. This can be achieved via SOAP/HTTP. At the policy level, secure interoperability requires that each party be able to specify any policy it may wish in order to engage in a secure conversation. At the identity level, we require mechanisms for identifying a user from one domain in another domain. The security mechanism in between from Kerberos tickets to X.509 certificates.

Trust between end points can be presumed, based on topological assumptions. They are part of a VPN, or explicit, specified as policies and enforced through exchange of some trust-forming credentials. The trust relationship problem is made more difficult in a Grid environment by the need to support the dynamic, user-controlled deployment and management of transient services.

Naturally, grids are protected from external attacks with the same tools that enterprise networks use, including firewalls, authenticated access, public key cryptography and configuration management. To control access to sensitive data, grid systems must have authenticated access control, SSL communications, filtering and auditing of sensitive data, and erasure of data after use.

All these topography and processing requires a securities at each stage of functions. There arises a need for mechanisms that enable continuous discovery and monitoring of grid-entities i.e. dynamic resources, services and grid activity and check the performance diagnostics. Due to dynamic nature of grid resources, it is very important to provide seamless and high quality of service, such as authorization, access control, single logon, distributed workflow, problem determination services, resource management performance and delegation. Most grids use a large number of identical

processors running identically-configured operating systems, and that uniformity helps grid managers to monitor security issues more easily. [12]

## VII. REQUIREMENTS OF GRID SECURITY IN INDIAN CONTEXT

For an Indian grid environment, the threats listed above can form the basis for a risk assessment. An organization then needs to decide whether they want to mitigate a given risk, transfer the risk, or accept the risk based on a cost/benefit/impact analysis. The following security requirements are based on an approach to mitigate unique threats and risks. [8]

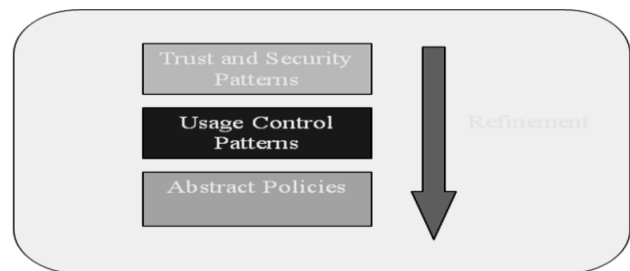


Figure2: Refinement of Trust and Security Goals into Requirements

Grid systems and its related applications may require any or all of the standard security functions, including authentication, access control, integrity, privacy, confidentiality, usage limitation, delegation; availability and non-repudiation i.e. depend on security policies of different sites at different cities or domains of enterprise environment of India. That may be:

- 1) Exclusively, we seek to provide authentication solutions that allow a user, the processes that comprise a user's computation, and resources used by those processes, to verify each other's identity; and allow local access control mechanisms to be applied without change, whenever possible. An authentication scheme based on Public Key Infrastructure should be implemented. Users' identity should be confirmed using certificates issued by a trusted CA. The authentication mechanism may be a custom authentication mechanism or an industry-standard technology. We may provide plug points for multiple authentication mechanisms. Authentication forms the foundation of a security policy that enables diverse local security policies to be integrated into a global secure grid framework for India.
- 2) Communication must be secure between collections of grid components themselves. The composition of a process group can and will change during the lifetime of a computation. Hence, support is needed for secure communication for dynamic groups. This includes providing confidentiality through something like channel encryption, as well as integrity checks to guard against tampering across the wire. This may also include satisfying a non-repudiation requirement where that is needed. Confidentiality of sensitive



data must be preserved through the life cycle of grid components.

- 3) Open and standardized software that will run on *multiple platforms*, the underlying security mechanisms of various platforms will always be consistent. For any application-specific function that might also require authentication or special authorization, the application should be designed to utilize GSI in order to simplify development.
- 4) The impetus for delegation using proxy certificates solution is secure and integrates very well with the suggested authentication algorithm and the Public Key Infrastructure. Moreover, it provides abilities to be extended for broader fields of application, which is for advanced authentication based on attributes. The suggested solution is named the GSI Authenticator to underline its compliance with the Globus mechanisms. The concept of the GSI Authenticator is to use a simple challenge-response protocol with the requirement of tunneling the authentication process by a secure outer protocol. The single sign-on and delegation abilities will be provided using proxy certificates. [10]
- 5) Grid components themselves must be validated for security and integrity in accordance with an India's enterprise intra grid security policy interface with inter grid security policy affecting external factors i.e. government rules of many states of different sites of cities. This may include log files, cryptographic key material, or other material that is collected from a dynamic resource prior to it. We must ensure that unauthorized changes made to messages may be detected by the recipient. It is called message level integrity checking.
- 6) Provide all services, including security services themselves, with facilities for time-stamping and securely logging any kind of operational information or event in the course of time. Secure logging is the base for addressing requirements for notary, non-repudiation, and auditing.
- 7) The security assurance level that can be expected for the hosting environment. This can be used to express the protection characteristics of the environment such as virus protection, firewall usage for Internet access, internal VPN usage, etc.
- 8) Context-oriented layering of the security services infrastructure recognizing two distinguished levels: trusted network (intranet, cluster) - bypass security for performance, Collaborative network (Internet) - minimal performance concern, maximal security, Pluggable support for any extra security feature.

We also choose to satisfy the following security constraints derived from the characteristics of the grid environment and grid applications:

*Single Logon:* A user should be able to authenticate once and initiate computations that acquire resources, use or release resources, and communicate internally without further authentication of the user. This must take into account that a request may span security domains hence

should factor in coalition between authentication domains and mapping of identities. To delegate an entity's rights, subject to policy e.g., lifespan of credentials, restrictions placed by the entity.

*Credentials Protection and Renewal:* User credentials i.e. passwords, private keys, etc. must be protected. The user also needs the ability to be notified prior to expiration of the credentials, or the ability to refresh those credentials such that the job can be completed. Hence, it is imperative to employ a standard such as X.509v3 for encoding credentials for security principals.

*Authorization:* Allow for controlling access to OGSA services based on authorization policies i.e., who can access a service, under what conditions etc. Authorization should accommodate various access control models and implementation. The security policy with a range of security technologies based on both public and shared key cryptography.

*Interoperability interfacing decentralize security solutions:* Our security solutions may provide inter-domain access mechanisms, access to local resources will typically be determined by a local security policy that is enforced by a local security mechanism at decentralization mode. Instead, one or more entities in inter-domain security servers must act as agents of remote clients or users for local resources.

*Privacy:* Privacy policies may be treated as an aspect of authorization policy addressing privacy semantics such as information usage. It allows both a service requester and a service provider to define and enforce privacy policies.

Several of these so-called domain U instances usually run parallel on a single physical machine, protected from each other and under the control of a domain 0 master operating system instances that can create, suspend and terminate domain U instances on demand. CPUs, network and disk devices are virtualized for domain U domains and thus controllable by domain 0.

The security mechanisms used to establish and maintain tiny lived, ad-hoc collaborations must be fully distributed and should not require group-specific infrastructure components. An access right is "fine-grained" if it denotes a specific right of a given user to a given object. Access rights are not fine-grained if they require a right to be granted to all members in a group of users or if the right conveys access to all objects in a set of objects. Both scenarios require fine-grain rights. The ability to delegate access rights directly is also needed to provide for the necessary scalability of grid security solutions. The overhead required to delegate authorization creates barriers to the scalability of such a system. In our model the threats are categorized according to specific behaviors, this classification being considered more robust than technological categorization, because technologies may change very rapidly. This also encourages a broader view when evaluating security risks.

On considering above these requirements, intra-grid sites of cities of India interoperable or collaborate with inter-grid sites of cities of India makes foundation applications and secure framework can be built to

establish trust relationships that are required for commercial distributed computing, enterprise application integration and business-to-business (B2B) partner collaboration over the Internet.

### VIII. IMPLICATION OF THE PROPOSED RESEARCH

We propose a security policy for grid systems that addresses requirements for single sign-on, interoperability with local policies, and dynamically varying resource requirements. The implication in this proposed framework with the policy focuses on authentication of users, resources, and processes and supports user-to-resource, resource-to-user, process-to-resource, and process-to-process authentication with associated protocols. It provides an in-depth analysis of the security problem in computational grid systems and its applications. A subject is a participant in a security operation.

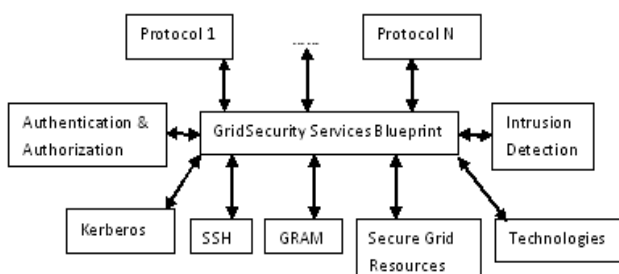


Figure 3: Implication of proposed research

In grid systems, a subject is generally a user, a process operating on behalf of a user, a resource. Both global and local subjects exist. For each trust domain, there exists a partial mapping from global to local subjects. Processes running on behalf of the same subject within the same trust domain may share a single set of credentials. The Specific technical issues raised by this policy, including local heterogeneity and scalability. All access control decisions are made locally on the basis of the local subject like the local region or city in India. I will implement standard future oriented web service tools, GRAM system and abstract software with adaptive protocols to provide security specification services to users of grid.

### IX. CONCLUSION

The proposed secure infrastructure enables full system virtualization, scalable, reliability with high availability that boosts speed, flexibility, security and save time of users communicate with low cost on demand computing among the different cities of India. The work which is at blueprint stage will be described as guidelines for the engineers engaged in the setting of secure grid in India.

### REFERENCES

[1] Foster, I., Kesselman, C. and Tuecke, S., "The Anatomy of the Grid: Enabling Scalable Virtual

- Organizations," International Journal of High Performance Computing Applications, 200-222-2001. <http://www.globus.org/research/papers/anatomy.pdf>
- [2] Jean Christophe Durand; "Grid Computing- A conceptual and practical study", 2004
- [3] Brooke, J., Fellows, D., Garwood, K. and Goble C., "Semantic matching of Grid Resource Descriptions," In Proceedings of the European Across Grids Conference, 2004, <http://www.Grid-interopability.org/semres.pdf>
- [4] Performance Analysis and Grid Computing by Vladimir Getov, 2003
- [5] I. Foster and C. Kesselman. The Globus project: A progress report. In Heterogeneous Computing Workshop, March 1998.
- [6] C. Kesselman, I. Foster. Computational grids. In The Grid: Blueprint for a New Computing Infrastructure., Morgan-kaufman edition, 1999
- [7] Kerberos: The Definitive Guide - Page ii by Jason Garman - Computers - 2003 - 272 pages
- [8] A Security Architecture for Computational Grids. I. Foster, C. Kesselman, G. Tsudik, S. Tuecke. Proc.5th ACM Conference on Computer and Communications Security Conference, pp. 83-92, 1998.
- [9] Chen, L, Shadbolt, N, Goble, C, Tao, F, Puleston, C, and Cox, S.J., "Semantics- Assisted Problem Solving on the Semantic Grid," Computational Intelligence, Vol.21, No.2,2005,pp.157,<http://www.geodise.org/files/Papers/ComputationalIntelligencePaper.pdf>
- [10] Security in Computing: Data Management in an international data grid project – by hoschek
- [11] Grid Service Specification. S. Tuecke, K. Czajkowski, I. Foster, J. Frey, S. Graham, C. Kesselman; Draft 2, 6/13/2002, <http://www.globus.org>
- [12] The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. I. Foster, C. Kesselman, J. Nick, S. Tuecke; January, 2002.

**Sanjeev Puri** is the research scholar and pursued PhD(IT) from Manav Bharti University, Solan. He is the Reviewer editorial member of IACSIT-IJCEE and Elsevier. He has done Master of Science in Computer Science in 2003. He is working as Professor (Information Technology) at SRMCEM (Now SRM University), Lucknow, India. His research interests include grid computing and its security, cloud computing and adaptive protocols working activities in communication of network system.

**Dr. Harsh Dev** has done his PhD (Computer Sc. & Engg) from Ambedkar University, Lucknow. He is working as Professor (CS & E) at PSIT, Kanpur. His research interests in Distributed database, grid security.etc.