GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

STUDY OF DIFFERENT SECURITY ISSUES ON GRID COMPUTING

Amit Kumar Painkra[1], Rakesh Patel[2], Krishna Rathore[3]
Student,B.E.(IT) Kirodimal Institute of Technology,Raigarh(C.G.),India[1,3]
Lecturer,Department of Information Technology Kirodimal Institute of Technology Raigarh(C.G.),India[2]

ABSTRACT

Grid computing provides high computing power, enormous data storage, and collaboration possibilities to its users. A Computational Grid is a collection of heterogeneous computers and resources spread across multiple administrative domains with the intent of providing users uniform access to these resources. There are many ways to access the resources of a Computational Grid, each with unique security requirements and implications for both the resource user and the resource provider. A comprehensive set of Grid usage scenarios are presented and analyzed with regard to security requirements such as authentic cation , authorization, integrity, and confidentiality. The main value of these scenarios and the associated security discussions are to provide a library of situations against which an application designer can match, thereby facilitating security-aware application use and development from the initial stages of the application design and invocation. A broader goal of these scenarios are to increase the awareness of security issues in Grid Computing. In the networked access to computation with a single-sign-on system as the portal to the possibilities of world wide computing grids security plays an important role.

Keywords: Grid Computing, Security, Intrusion detection system etc

I. INTRODUCTION

Security is a latest topic today for the smart grid, and progresses are being done in this field every day. Most communications uses standard cryptographic algorithms AES-128 to protect the data on the network. Grid computing is a technique which provides high-performance computing; in this resources are shared in order to improve the performance of the system at a lower price. According to literature, “Grid computing is a system where multiple applications can integrate and use their resource efficiently”. According to Foster and Kesselman , “A grid is a system that has three important categories: coordination of resources not under centralized control, use standard general purpose interface, and it delivers nontrivial quality of service”. Kon et al define grid computing as, “coordination of resource sharing and dynamic problem solving in multi-institution virtual organizations”

One goal of software designed as infrastructure supporting Computational Grids is to provide easy and secure access to the Grid’s diverse resources. First we survey security problems which exist in grid computing and then we analyze security requirements. At the end we introduce a framework which Erin Cody has posed as a solution for security problems of grid computing. The classification system group grid security solutions according to system solutions, behavioral solutions, hybrid solutions as well as technologies related to grid that could be useful in providing grid security.

II. SECURITY REQUIREMENTS

Grid systems and applications require standard security functions which are authentication, access control, integrity, privacy, and no repudiation. Authentication and access control issues are. It provides authentication to verify the users, process which have user’s computation and resources used by the processes to authenticate (2) allow local access control mechanisms to be used without change. To develop security architecture we have to satisfy the following constraints which are taken from the characteristics of grid environment and application.

Single sign-on:
A user should authenticate once and they should be able to acquire resources, use them, and release them and to communicate internally without any further authentication.
Protection of credentials: User passwords, private keys, etc. should be protected.

Interoperability with local security solutions:
Access to local resources should have local security policy at a local level. Despite of modifying every local resource there is an inter domain security server for providing security to local resource.

Exportability:
The code should be exportable i.e. they cannot use a large amount of encryption at a time. There should be a minimum communication at a time.

Support for secure group communication:
In a communication there are number of processes which coordinate their activities. This coordination must be secure and for this there is no such security policy.

Support for multiple implementations:
There should be a security policy which should provide security to multiple sources based on public and private key cryptography

III. THE GRID SECURITY PROBLEM

We introduce the grid security problem with an example illustrated in Fig. 1. This example, although somewhat contrived, captures important elements of real applications..

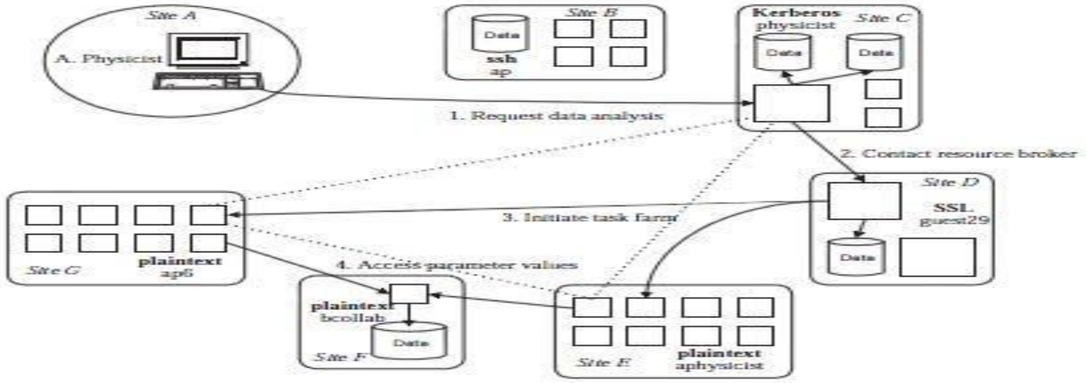


Fig. 1: Example of a large-scale distributed

We imagine a scientist, a member of a multi-institutional scientific collaboration, who receives e-mail from a colleague regarding a new data set. He starts an analysis program, which dispatches code to the remote location where the data is stored (site C). Once started, the analysis program determines that it needs to run a simulation in order to compare the experimental results with predictions. Hence, it contacts a resource broker service maintained by the collaboration (at site D), in order to locate idle resources that can be used for the simulation. The resource broker in turn initiates computation on computers at two sites (E and G). These computers access parameter values stored on a file system at yet another site (F) and also communicate among themselves (perhaps using specialized protocols, such as multicast) and with the broker, the original site, and the user. This example illustrates many of the distinctive characteristics of the grid computing environment:

- The user population is large and dynamic. Participants in such virtual organizations as this scientific collaboration will include members of many institutions and will change frequently.
- The resource pool is large and dynamic. Because individual institutions and users decide whether and when to contribute resources, the quantity and location of available resources can change rapidly.
- A computation (or processes created by a computation) may acquire, start processes on, and release resources dynamically during its execution. Even in our simple example, the computation acquired (and later released) resources at five sites. In other words, throughout its lifetime, a computation is composed of a dynamic group of processes running on different resources and sites.
- The processes constituting a computation may communicate by using a variety of mechanisms, including unicast and multicast. While these processes form a single, fully connected logical entity, low-level

communication connections (e.g., TCP/IP sockets) may be created and destroyed dynamically during program execution.

- Resources may require different authentication and authorization mechanisms and policies, which we will have limited ability to change. In Figure 1, we indicate this situation by showing the local access control policies that apply at the different sites. These include Kerberos, plaintext passwords, Secure Socket Library (SSL), and secure shell.
- An individual user will be associated with different local name spaces, credentials, or accounts, at different sites, for the purposes of accounting and access control. At some sites, a user may have a regular account (—ap, —physicist, etc.). At others, the user may use a dynamically assigned guest account or simply an account created for the collaboration.
- Resources and users may be located in different countries. To summarize, the problem we face is providing security solutions that can allow computations, such as the one just described, to coordinate diverse access control policies and to operate securely in heterogeneous environments.

IV. GRID SECURITY CHALLENGES

Multiple resources provide the control policies to the third party. The VO is one which coordinates the resource sharing and use. The dynamic policies and entry of new participants in the system gives the need for three key functions which are:

Multiple security mechanisms:
Organizations which participate in a VO have investment in security mechanism and infrastructure. Grid security interoperates with these mechanisms.

Dynamic creation of services:
Users must be able to create new services (e.g., "resources") dynamically without administrator permission. These services should coordinate and interact with other services. So, we must be able to name the service with acceptable identity and should be able to grant rights to that identity without any contradiction with the governing local policy.

Dynamic establishment of trust domains:
VO needs to establish coordination between its user and all the resources so that they can communicate easily. These domains must establish trust dynamically whenever a new user join or leave a VO. A user-driven security model is needed to create new entries of the user so that they can coordinate with the resources within the VO.

V. OVERVIEW OF GRID COMPUTING SECURITY

Since the research papers discussed here deal with security risks that could be faced by any type of grid, it is assumed in this paper that the term —grid computing system includes each of these three types. Note that while the types of grid listed in Table 1 represent the three common categories of grid computing systems, some grid systems can employ aspects of several or all of the three types, making them —hybrid grid computing systems. These grids could then face any of the vulnerabilities faced by the grid types they are made up of. Considering the grid environment's diverse and geographically separated resources and wide variety of users, each with unique needs and goals for the grid system, the issue of managing the security of users and resources becomes an issue. The users of a grid, be it computational, data, or service oriented, may have conflicting interests with each other, and thus would want some assurance that their grid-based transactions are safe from the eyes of other users. Without security, a grid setup would is left vulnerable to unauthorized users, malicious processes, and data tampering that could possibly render it useless.

According to the classification system for grid computing security research, grid computing security can be classified into the following parts: systems, behavioral, hybrid, and related technologies, as shown in Fig. 2. This classification provides several benefits to the research

Type of grid computing system	Brief explanation	Most common vulnerabilities
Computational grid	Grid architectures that focus on setting aside resources specifically for computing power; i.e. solving equations and complex mathematical problems; machines participating in this type of grid are usually high-performance servers.	Programs with infinite loops can be used to bring down nodes of this grid, decreasing functionality
Data grid	Grid architecture responsible for storage and providing access to large volumes of data, often across several organizations	Users can overwrite data of other users if they exceed their available space-this corrupts the other users' data
Service grid	A grid which provides services that are not available on a single machine	Users can use the service grid to launch Denial of Service Attack (DOS) against another site

Table 1: Types of grid computing systems

VI. SYSTEMS SOLUTIONS

This section discusses papers that propose system-based solutions to secure grid computing environments. Rather than discussing the implementing of security policies and behavior-based solutions (as discussed in Section 4), this part of the classification deals with solutions whose focus is to manipulate the hardware and software of a grid system directly in order to achieve security. Box-product technologies, topologies and architectures, and intrusion detection systems are addressed in this section.

(a) System security for grid resources

This section deals with research focused on system-based solutions toward grid security. Proposed solutions falling into this category seek to protect resources on the grid. Access control is a valid method for protecting resources, however it cannot be the only line of defense to ensure that grid nodes, applications, data, and communications are safe from malicious users. This category focuses on protecting the grid resources, which include hardware and computing equipment, applications running on the grid and the data that they contain, as well as communication between grid nodes. Solutions falling into this category address the data and

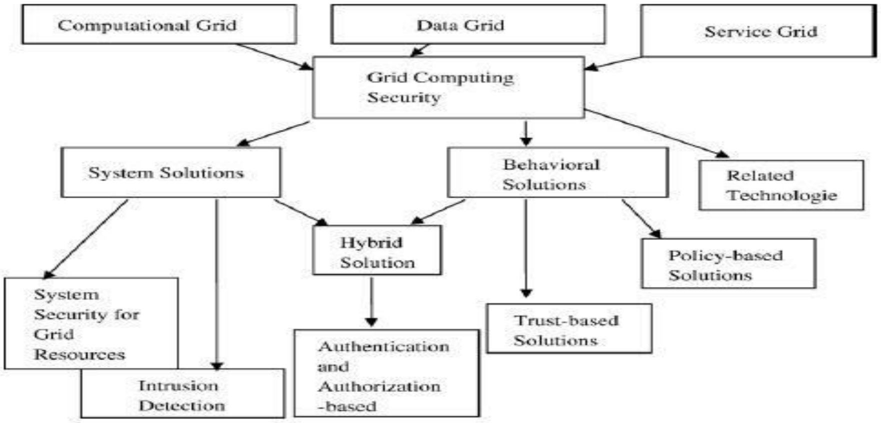


Fig. 2: Classifications for grid computing security grids (Table 1) and the security situations of Immediate Job Execution and Accessing of Information.

(b) Intrusion detection systems (IDS) in grid computing

This section discusses papers that present an intrusion detection system (IDS) model for securing the grid environment. For the context of this article, an —intruder into the grid is defined as any grid user who intends to harm the grid or its resources, or intends to use the grid for purposes other than what it was designed for. Rather than being a specific software package or brand name box product, intrusion detection is a technological concept which can be implemented using any one of several software and/or hardware methods. IDS grid solutions function in the computational and service grids (Table 1) and address the security solutions of Accessing Grid Information, Setting/Querying Security Parameters, and Auditing Grid Functions.

(c) Behavioral solutions

The following section addresses types of solutions that emphasize policy and management controls over hardware/software solutions to maintain a secure grid. Behavioral solutions are intangible and intuitive, rather .than employing a physical technology to maintain security in the grid. Accountability, group management, and trust are all issues that are addressed here.

Comprehensive policy controls

This portion of the review deals with papers that achieve security through policy definition. The papers suggesting trust as a security solution could be viewed as a subset of this portion. However, those papers were specific to trust, while the following papers cover several types of policies in their solutions, thus it seems more appropriate to group the trust-based papers separately. Research falling into the policy controls category, consequently, discusses policy sets governing a wide range of grid computing actions, rather than focusing on one area of activity while participating in a grid. These policies address all areas of grid computing, including authorized user selection, sign-on procedures and access control, and local vs. global security settings. As policy controls primarily affect the human component of the grid, comprehensive policy sets designed to manage groups of users are a logical extension of this method of grid security.

(d) Hybrid solutions

A thorough review of the literature concerning grid computing security issues revealed that the particular concept of authentication and authorization of grid users could be addressed equally by system-based solutions and behavior-based solutions alike. Thus, it is more appropriate to create a Hybrid Solution sub-category to address this issue, since it falls equally under System and Behavioral grid security solutions.

VII. GT

(a) GT2 Grid Security Model

The security technologies incorporated in the Globus Toolkit version 2 (GT2) includes services for Grid Resource Allocation and Management (GRAM), Monitoring and Discovery (MDS), and data movement (Grid FTP). These services use Grid Security Infrastructure (GSI) to provide security. GSI works on a common format based on X.509 identity certificates and a common protocol based on transport layer security (TLS, SSL). An X.509 certificate is associated with

private key that forms a unique authentication set that a Grid uses to authenticate itself to other Grid entities. The TLS-based protocol is used to provide message protection (encryption, integrity checking), according to the requirement of data stream. Gateways are used to translate information between common GSI infrastructure and local site mechanisms. For example, the Kerberos Certificate Authority (KCA) provides an interface for translation of Kerberos to GSI and vice versa. [8] Each GSI certificate is issued by certificate authority (CA), which runs a large number of organization or commercial company. To trust the X.509 communication, the CA issues the certificate to trust the entity. An X.509 identity certificate is used within GSI for establishment of a trusted communication.

In mechanisms such as Kerberos, where for inter-institutional a bilateral agreement is required atthe organizational level, trust in a CA is established unilaterally: A single entity can decide to trust any CA, without involving the whole organization. This feature is used in the establishment of VOs in which some portions of the organizations are only used and not the whole organization. GSI introduces X.509 proxy certificates, which is an extension to GSI used by X.509 identity certificates to allow a user to assign a new X.509 identity to an entity and then delegate subset of their rights to that identity. Users create this proxy certificate by issuing a new X.509 certificate signed by it without involving the CA. By this mechanism new authentication and identities can be created quickly as there is no involvement of the administrator. To create a trusted communication VOs is provided for both the proxy certificate and for security services, Example, the Community Authorization Service (CAS). According to GSI policy if any two entities have proxy certificates issued by the same user they can trust each other. This policy allows the users to create trusted communication itself by issuing proxy certificates to any services with whom they wish to collaborate.

This policy of trust between proxy holders allows then for a easy and simple trust domains but for complicated trust domains they have some limitations, for example, limited trust between multiple parties in which we can use security services such as CAS that allow flexible, expressive policy to be created for multiple users in a VO. CAS allows a VO to use the policy that has been provided to it by the resource providers in the VO. This process has three steps shown in Figure 1: The three steps of the figure are:

Firstly, the user authenticates to CAS and receives notification from CAS stating VO's policy that how the user may use VO resources. Second, after that the user presents the details to a VO resource and the usage request. Finally, then evaluation is done whether to allow the request, for this the resource checks both local policy and the VO policy expressed in the CAS assertion. CAS allows a resource to retain the authority over that resource, but it also allows the VO to control the enforced policy. Then, the VO coordinate the policy that how the resources will be shared.

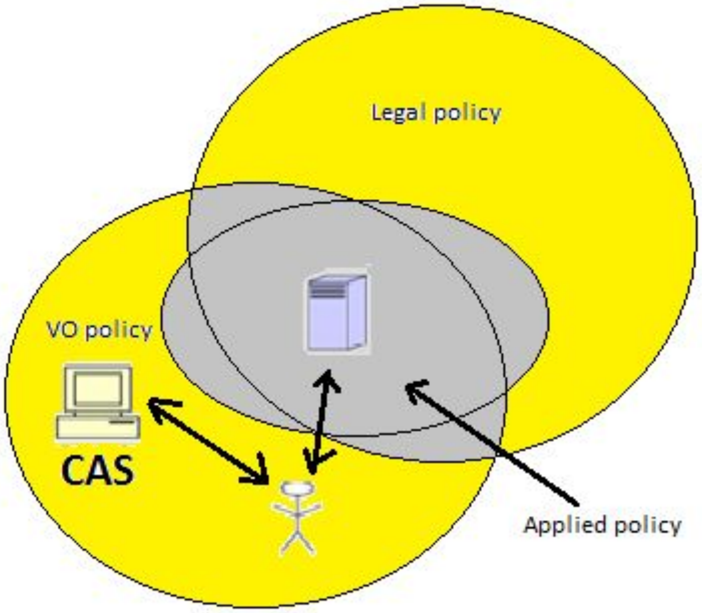


Figure . Policy of CAS and VO.

(b) GT3 Security Model

Grid security challenges are solved with Open Grid Services Architecture (OGSA) along with a set of technical specifications to integrate Grid technologies with Web services technologies. Web services technologies allow defining software component in terms of access methods, to bind these methods with specific communication mechanisms, and also to provide mechanisms for discovering relevant services. There are no particular mechanisms but few are emerging as ubiquitous. The Simple Object Access Protocol (SOAP) provides an interface for messaging using XML along with HTTP. The Web Services Description Language (WSDL) provides a method for expressing operation signatures and also bindings to protocols and endpoints in an XML document.

OGSA is a standard Web service interfaces and behaviors to add Web services with the concepts of crateful services and secure invocation, and also capabilities to address Grid-specific requirements. These interfaces and behaviors define a "Grid service" and allow users to manage the Grid service's life-cycle, according to the policies, and create sophisticated distributed services. [6] A grid service is defined as an interface for service data elements (SDEs) that other entities can query or subscribe to. OGSA introduces new opportunities and challenges for Grid security. Globus Toolkit (GT3) and Grid Security Infrastructure (GSI3) were the first to implement OGSA mechanisms. GT3's security model allows applications and users to operate on the Grid as easyand automatic manner as possible.

Security mechanisms should not be instantiated in an application but should be supplied by the surrounding Grid infrastructure to adapt on behalf of the application to meet the application's requirements.

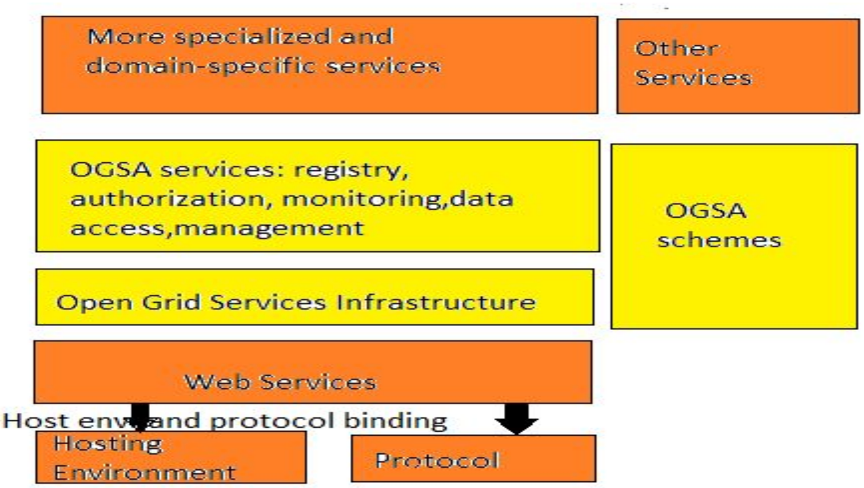

More specialized and domain-specific services
Other Services
OGSA services: registry, authorization, monitoring,data access,management
OGSA schemes
Open Grid Services Infrastructure
Web Services
Host env and protocol binding
Hosting Environment
Protocol

Figure 2. OGSA Architecture

The application should deal only with application specific policy. GT3 uses the following features of OGSA and Web services security to achieve their goals, these goals are to: First, use of security functionality as OGSA services to locate them and use the service whenever needed.

Second, use of sophisticated host environment to provide security for applications and to adaptsecurity of application without changing it. Third, to publish service security policy for clients to discover dynamically what are the requirements and mechanisms needed for establishing trust with the service.

Fourth, to provide specifies standards for the exchange of security tokens for interoperability.[4]

(c) GT4 Security Models

GT4 Authorization implements SAML (security assertion markup language), and uses the XACML (extensible access control markup language). XACML authorization framework architecture is an implementation of the Open Grid Services Architecture is an initiative for recasting Grid concepts within a service oriented framework based on Web services. [14] In GT4, we have additional Web Services security specifications implementation.

Web Services has provided several security standards that which influences Grid computing. XACML and International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014

184SAML are the two important authorization standards. We have several other authorization systems that support Grid computing that are Akenti, PERMIS, Shibboleth and VOMS. Akenti, PERMIS and Shibboleth use the type of attributes which are needed to make authorization decision. VOMS provides user attributes used for authorization. These authorization systems have their own policies, and can be integrated with GT4 authorization framework to provide
authorization services. [5]

The whole architecture is shown below.

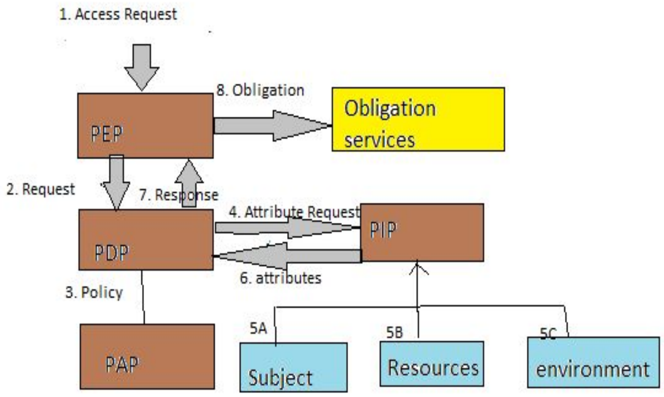


Figure 3. XACML authorization model

XACML also defines a policy language. Policies are organized in hierarchy with the Policy Sets combined using combining algorithms. A rule is has a target, an effect of that rule and a condition on which the rule works. A Policy comprises of a target, one or more rules, and an optional set of obligations .

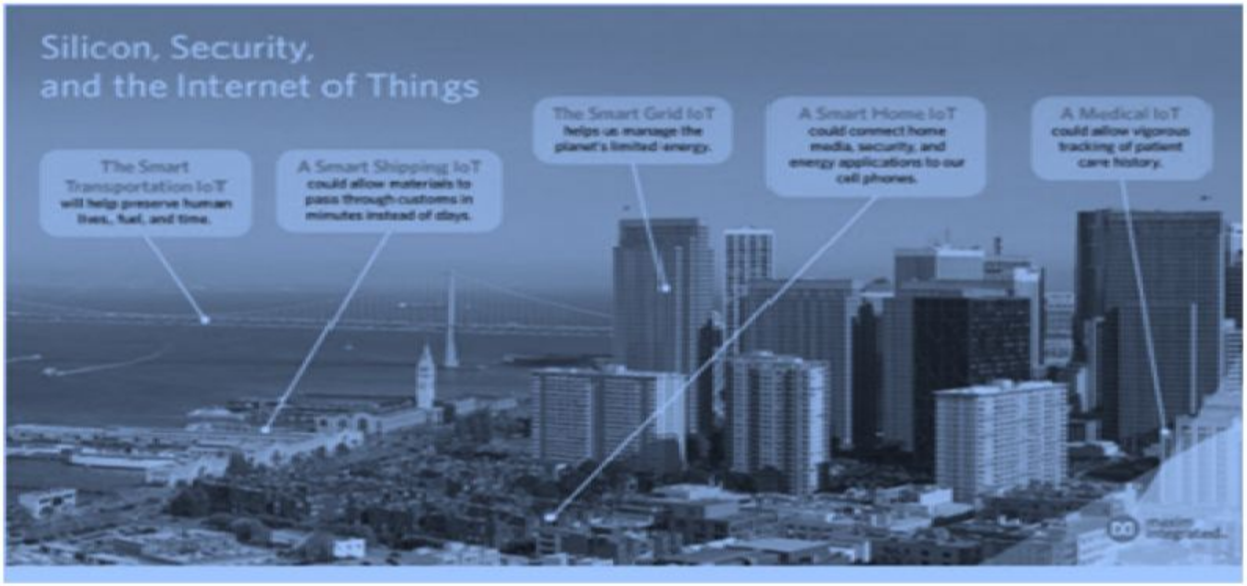
(d) SMARTGRID CYBER SECURITY:

The cyber security for the smart grid is the possibility that if in a centralized grid we have two way digital communications the grid can become susceptible to the hackers who can use customer confidential information and can cause adverse effect on the communication. This is the latest concern in the Grid to create a Smart Grid cyber security to provide the internet security in the International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014 185 Grid. There should be some policies with which we can take the benefits of the Internet and also the available computation power in a secure way [1]. Internet facility is much more reliable than electric grid due to the following reasons:

1) Internet is decentralized and is in starfish pattern and not in spider,
2) Asynchronous i.e. we don't have to use a single source we can work on different server and
3) It has many paths and not a few single connections. The Internet is a smart grid, a resilient grid, a self-healing grid that does not go down. The last connection to the grid may fail, or a particular destination may fail. The Internet makes it possible to have a more secure grid as it reliably monitor and control every part of the grid in real time.

The new smart grid will be a less centralized grid because:

1) the traditional economies that supported it has been removed by risk and uncertainty of siting, construction, operation, fuel supply, environmental impact and cost recovery,
2) There is penetration of distributed generation, storage, PHEVs/EVs as well as customer premises energy management systems
3) There is an increasing penetration of stochastic, energy sources like wind, solar and consumer dispatched generation. There is a complex grid with many points to automatically monitor and control resources.


Silicon, Security, and the Internet of Things
The Smart Transportation IoT will help preserve human lives, fuel, and time.
A Smart Shipping IoT could allow materials to pass through customs in minutes instead of days.
The Smart Grid IoT helps us manage the planet's limited energy.
A Smart Home IoT could connect home media, security, and energy applications to our cell phones.
A Medical IoT could allow vigorous tracking of patient care history.
maxim integrated.

VIII. CONCLUSION

The purpose of this review was to provide an extensive literature survey of current research in the area of security in grid computing, and to identify areas of grid computing security in which more extensive research is needed. More importantly, this paper contributes to the overall body of research concerning security in grid computing through the creation of a comprehensive framework for classification of grid security research.

Computational Grids are rapidly emerging as a practical means by which to perform new science and new applications. Each scenario in this paper is designed to provide guidance for the Grid user, the Grid application developer, and the Grid resource provider. While a given scenario can provide practical guidance for design and deployment, additional insight is gained by recognizing the general, rapidly-emerging issues such as the need for restricted delegation (giving onlya subset of your rights to something that will act on your behalf) that can be seen running through many of the scenarios.

IX. REFERENCES

[1] International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.
[2] Security Implications of Typical Grid Computing Usage Scenarios.
[3] International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013
[4] Workshop on Grid Technologies, Brussels, 22 – 23June 2000
[5] I. Foster, C. Kesselman, G. Tsudik, S. Tuecke. A Security Architecture for Computational Grids. Proc. 5th ACM Conference on Computer and Communications Security Conference,
pg. 83-92, 1998.
[6] A.S. Grimshaw, A.S. Humphrey, A. Natrajan, A philosophical and technical comparison of Legion and Globus, IBM J. Res. Develop. 48 (2) (March 2004).
[7] http://www.gridcomputingplanet.com/news/article.php/3323731 (Document view: March 28 2006).
[8] http://www.edugrid.in.