SECURITY IN GRIDS

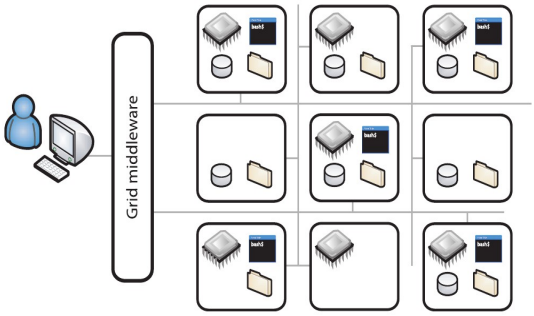
ASSIGNMENT III

João Sá - 198901299 | Vasco Themudo - 200003011

May 15, 2013

1. INTRODUCTION

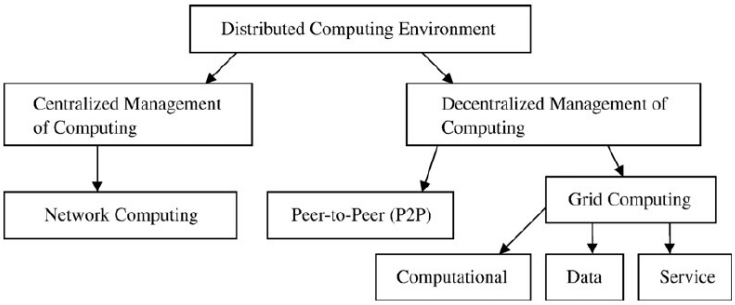
Grid computing is defined in literature as “systems and applications that integrate and manage resources and services distributed across multiple control domains”[6]. Ian Foster describes a three point checklist to characterize a grid: i) should provide resource coordination minus centralized control; ii) should be based on open standards; iii) and it should provide a nontrivial quality of service [4].



Enhanced network bandwidth, increasing complexity of computations with powerful computers and the exponential growth and the constantly rising speed of the Internet have motivated the necessity for high-performance computing and the development of grid computing, at a very low cost.

Grid computing has emerged as a significant new field, distinguished from conventional distributed computing by its concentration on large-scale resource sharing, innovative applications, collaboration over enterprises and virtual organizations boundaries, and, in some cases, high-performance orientation. It also has the objective to reduce the cost of computing, improve quality of service and increase flexibility and reliability.

The grid concept enables to any user to get access, through a “simple and easy to use” Grid middleware, to a group of resources (computational, data or services) in a very transparent way. This application software hides from the user the complexity of the system.



This figure depicts the place that grid computing occupies within the distributed computing environment. We won't develop here, but there are many differences between Network computing, P2P environments and Grid computing: the type of ownership, organization, trust level, security solutions, etc.

Since I. Foster and others described and popularised the concept of “Grid”, one of the central challenges for this style of computing has been finding the means to put in place effective security measures.

Nowadays, the security in grids is a significant concern of grid computing, as the goal of grid computing is to only provide secure grid service resources to legal users. Without security, a grid setup would left vulnerable to unauthorized users, malicious processes and data tampering that could possibly render it useless.

For this assignment we start by describing the main challenges in grid security and which are the requirements these mechanisms should satisfy in a grid environment. Then we present two examples of different security implementations that are widely in use today. In the next section we classify types of security systems into four general categories. Finally, we'll talk very briefly about some creative and interesting security methods currently in development.

2. CHALLENGES IN GRID SECURITY

The main issues of security that have been addressed by grid architects have to do with achieving authentication and authorization of users, and their programs and systems on which they will execute or be stored. Grid security itself presents several unique security challenges, quite hard to overcome, including:

- managing user identities across local and global networks (within different administrative domains)
- managing the diversity of local resource/user/process security systems
- trust relationships between entities, end-user key and credential management (federation issues)
- providing security to resources against malicious acts from grid users.
- need to continuously check system evolution
- dynamic creation of services and trust domains

And all this security mechanisms preferably without decreasing performance! Administrators may not even be aware of which services are being offered by individual machines at any time.

> *Secure operations in a Grid environment requires that applications and services be capable of supporting a variety of security functionality, such as authentication, authorization, credential conversion, auditing, and delegation. Grid applications need to interact with other applications and services that have a range of security mechanisms and requirements. These mechanisms and requirements are likely to evolve over time as new mechanisms are developed or policies change. Grid applications must avoid embedding security mechanisms statically in order to adapt to changing requirements.[13]*

The following security requirements have to be satisfied [12]:

- Authentication: confirm the validity of each user and resource, and only the valid users and resources can process the works;
- Delegation: users can give the rights of using resource to an entity. The entity can access resources on behalf of users, which will be more convenient;
- Single sign-on: in grid environment, a work is usually completed by a number of resources. If every resource has to be authenticated, it is very cumbersome. Therefore, the property of single sign-on allows a user to log in once and to gain access to all resources without being prompted to log in again at each of them;
- Data confidentiality and integrity: when the important data is stolen or modified, the grid system will be destroyed. Therefore, we have to prevent the data from unauthorized access and modification. Data encryption systems are also implemented;
- Certificate revocation and life-span: when a user delegates the rights to an entity, the user will give a certificate to this entity. The entity can use the certificate to prove the validity. However, each certificate life span should be limited. When the certificate is expired, it will be invalid automatically. Furthermore, if the work is completed, the certificate should be withdrawn to prevent data from changes;
- User-based trust relationships: if a user has the right to use multiple sites, then the user should be able to use all sites together without requiring that each site's security administrators interact;
- Resource protection and secure communications between grid nodes.

There are three main types of computer grids in use today: computational grids, data grids, and service grids. Each has its own set of vulnerabilities, particularly in the security area, as referenced in this table [3]:

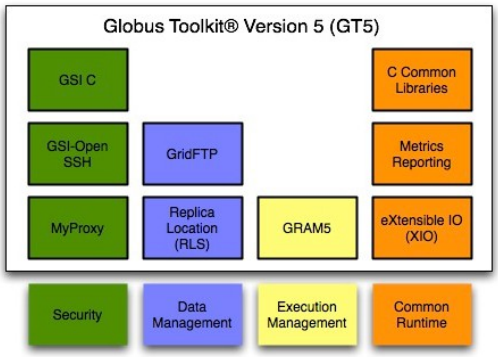
Type of grid computing system	Brief explanation	Most common vulnerabilities
Computational grid	Grid architectures that focus on setting aside resources specifically for computing power; i.e. solving equations and complex mathematical problems; machines participating in this type of grid are usually high-performance 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 [27]	Users can use the service grid to launch Denial of Service Attack (DOS) against another site

3. TWO GRID SECURITY MODELS

In this section we'll describe two examples where some of the most common and general security models are present: the Globus Toolkit and Climateprediction.net.

As many other grid implementations, the **Globus Toolkit** uses Grid Security Infrastructure (GSI) to protect grid computing security. The necessity for secure communication between entities on the Grid has motivated the development of GSI. It provides integrity, protection, confidentiality and authentication for sensitive information transferred over the network in addition to the facilities to securely traverse the distinct organizations that are part of collaboration. This mechanisms must be durable across multiple hosts, in different security domains, and for scalability, possibly require the identification of users.

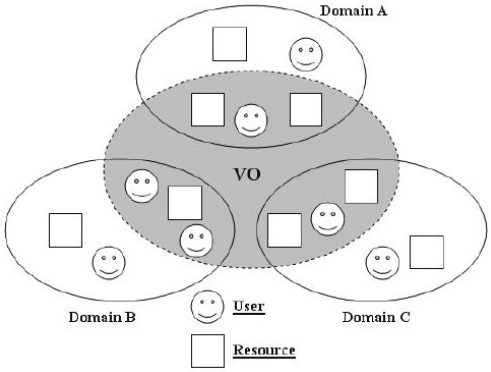
GSI is based on public key infrastructure (PKI) and applies secure socket layer (SSL) protocol/transport layer security (TLS) to provide the security communications between the grids and users. Furthermore, the user certificate, whose private key is protected by a password, is used to generate and sign a temporary certificate, called a proxy certificate, which is used for the actual authentication to Grid services and does not need a password. As possession of a proxy certificate is a proof of identity, the file containing it must be readable only by the user and a proxy has, by default, a short lifetime (typically 12 hours) to reduce security risks if it should be stolen.



GSI applies X.509 proxy certificate to achieve authentication, delegation, single sign-on, data confidentiality and integrity. There are two methods to revoke it: i) using Certificate Revocation List (CRL) to record the revoked certificates; or ii) submit a short-term proxy certificate.

The difference between public key certificate and proxy certificate is the issued entities. Public key certificate is issued by the certification authority (CA) while proxy certificate is issued by the public key certificate or another proxy certificate.

Globally the grid user community is grouped in to Virtual Organizations (VOs): collections of various and distributed individuals that are looking to share and utilize different resources in a synchronized fashion. This concept has been launched to define the relationships between a set of grid components comprising computing resources, data, applications and users.

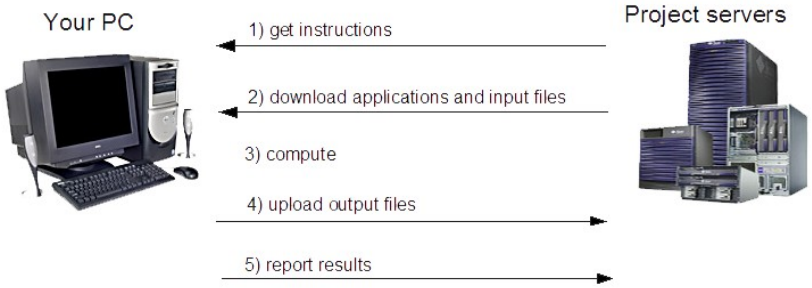


Before the Grid resources can be used, a user must read and agree with the rules and regulations of the VO he wishes to join, and register some personal data with a Registration Service. Once the user registration is complete, he can access the Grid Services.

The second, **climateprediction.net** (currently using the BOINC platform), reveals different security issues that is related to protecting hosts and to the reliability of results. This project arose from the observation that modern home PCs were equipped with enough power to permit them to run a credible climate model, previously the preserve of supercomputers.

One of the greatest security priorities was that participants should join in large numbers and there must be no taint of compromise to participants' privacy or the integrity of their machines. To encourage retention, the project used web-based community tools and visualization tools, and employed code signing that assure the safety of the software.

The question of whether climate data returned to the centre truly arose from a run of the model, was much harder to tackle. A mitigation for the problem of bogus results was achieved by sending identical tasks to different participants. This works well if there are sufficient participants.

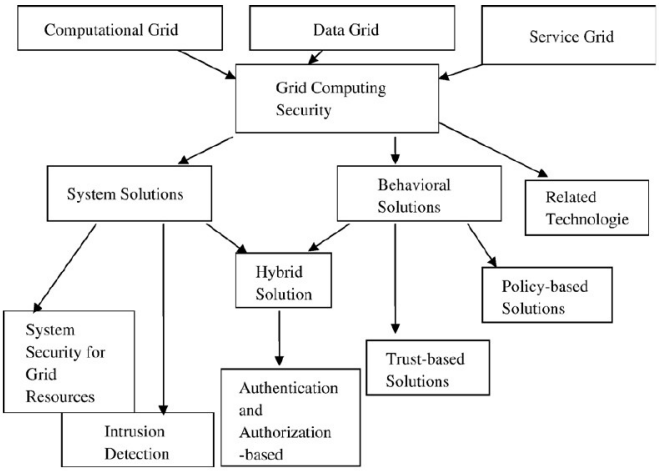


4. SOLUTIONS IN GRID COMPUTING SECURITY

In this section we'll briefly classify types of security systems into four general categories, based on this [3]:

- **System Solutions**: the 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 category
  - System security for grid resources (hardware and computing equipment, applications, data and communication between grid nodes): protect resources and implement access control; separate the portion of the resource dedicated to the grid from the portion that the owner wishes to keep private (sandbox, data encryption, virtual private grid, firewalls, DHCP, private IP)

- Intrusion detection systems: is a technological concept which can be implemented using any one of several software and/or hardware methods; involves accessing global grid informations, setting/ queering security parameters, auditing grid functions, statistical analyses from user's behaviour, sharing of information between resources, etc.



- **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; focus on security by policy, human action and management controls instead of hardware/software solutions
  - Comprehensive policy controls (rules and regulations): address all areas of grid computing, including authorized user selection, sign-on procedures and access control, and local vs. global security settings; manage groups of users; local control access policies; the security policies must also support uniform credential and certification infrastructure, secure group communication, and multiple implementations, i.e. one specific technology platform should not be required across all users and resources.
  - Trust-based security solution: establishment, definition, measurement and utilization of trust in grid computing environments; can be identity-based or behavior-based; example: a user of the system can make better decisions about the interaction with its peers if it knows the reputation of that peer in the system; creating the notion of a global trust value for each user in the system can lead to segregation of the proper users of the system from the misbehaving users of the system; if a client and resource have compatible trust levels, the operation they are involved in goes on without additional security overhead. If either the resource or the client has a required trust level above that of its counterpart's trust level, then additional security measures are enacted to allow the operation to take place.

- **Hybrid Solutions**: related with authentication and authorization of grid users
  - Authentication vs. authorization: the first is “the verification of the identity of a person or process”; authorization, however, is defined as being “the process by which an entity such as a user or a server gets the right to perform a privileged operation”; an Authentication and Authorization Infrastructure (AAI) is a vital yet highly complex component of every Grid infrastructure. The AAI is the framework over which Grid resources, users and Virtual Organizations can authenticate one another by means of their policies.
  - Authentication and authorization based solutions:
    - Globus/Kerberos (on section 3.)
    - Secure Highly Available Resource Peering (SHARP): agents and resource managers are bound to public-key signed digital certificates, and claims are cryptographically signed to make them unforgeable
    - LegionFS: this file system offers technological security for grid environments through its three level naming scheme and carefully controlled access control lists
    - Accounting system for grid users: keeps track of who is doing what on grid system; involves: mapping resource usage to resource users, defining resource economies or methods for resource exchange, and describing implementation standards that minimize and compartmentalize the tasks required for a site to participate on the grid.
    - Delegation logic: deals with authorization only, and is accomplished by a “proof of compliance” method; i.e. when an entity can provide credentials to show that they have passed certain requirements (determined by the resource or the grid) needed for entry.

- **Related Technologies solutions**: mobile intelligent agents and virtual environments

5. CASE STUDIES: SOME EMERGING ARCHITECTURES

a) Swarm-based approaches [16]

Scalable new approaches are needed to manage security efficiently. Swarm-based approaches map nicely to computer security problems precisely because of computer infrastructures' dynamic and decentralized properties, and they adapt to changing threat levels. In addition, swarm-based approaches are robust, since swarms select for colony survival and do not depend on particular individual agents.

Swarm solutions prescribe relatively simple rules for interaction that produce emergent behaviors sometimes referred to as self-organization.

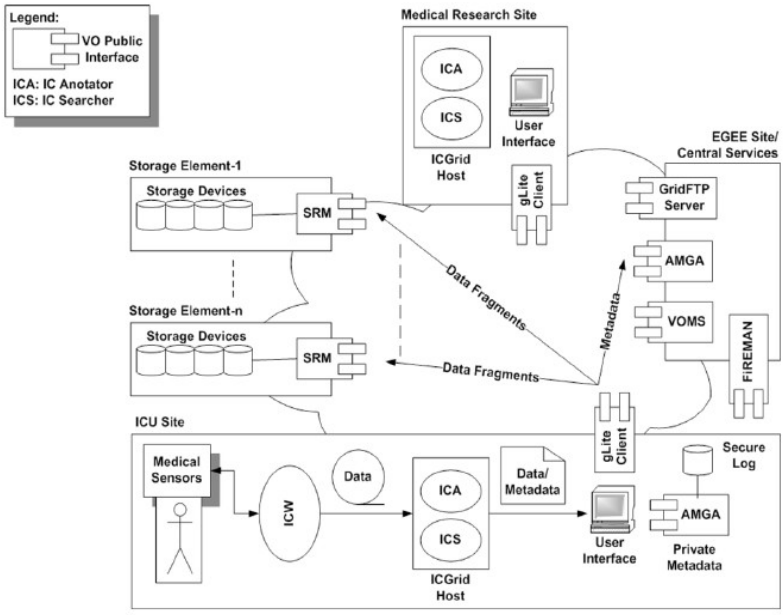
The digital ants framework is a hierarchy consisting of the Supervisor, Sergeant, Sentinel and Sensor levels. The different levels form a mixed-initiative approach, where human administrators' decision-making and authority is complemented with the computational resources of rational agents.

- Supervisors (or human administrators): provide overall governance to the infrastructure and interact primarily with the next level;
- Sergeants: responsible for a local subset of a computer infrastructure called an enclave (a set of geographically or topologically collocated machines that has a single owner and is managed under a common policy); they provide situational awareness to the Supervisor and create enclave policies based on Supervisor guidance
- Sentinel agents: provide status to their Sergeant and enforce the Sergeant's policies on enclave hosts; also enable Sensors to traverse the geography, the digital ants overlay network
- Sensors: search for a single, atomic indicator such as network connection frequency, number of zombie processes, or number of open files
  - their power is in their numbers, diversity, and stigmergic communication
  - as they wander, Sensors randomly adjust their current direction similar to the movement of real ants
  - compare findings at the current host with findings in their recent visits; if the findings are outliers, the Sensor reports this to the Sentinel.

b) ICGrid Architecture [15]

Current health grid authentication and authorization systems are unable to enforce access control close to the Storage Elementes (SEs) and the data itself. In other words, an attacker that bypasses these security mechanisms (by using a local account with administrative privileges or by physical access to the disks) will have full control over the stored data. Unfortunately, merely using cryptography at the SEs is not enough because encryption keys can be leaked by a local attacker.

Now we introduce a data-centered protocol designed to address these particular privacy concerns which uses three basic mechanisms:



1. An information dispersal algorithm providing high availability and assurance for the ICGrid by means of data fragmentation. In a fragmentation scheme, a file f is split into n fragments, all of these are signed and distributed to n SEs, one fragment per SE. The user then can reconstruct f by accessing m fragments ($m \leq n$) arbitrarily chosen.
2. A symmetric cryptosystem implemented at the SEs, i.e., via a hardware security module, which is able to provide confidentiality to the stored data, while keeping a good balance between security and performance.
3. An Message Authentication Code mechanism to protect the private metadata stored at the ICU's premises.

c) Trigon-based dual authentication [9]

The authentication protocol, presented in the figure, enhanced the grid security because the authentication mechanism uses two servers for authentication: Authentication server and Backend server. Moreover, the protocol that uses the fundamental properties of the trigon and the trigon parameters, made the grid more secure as the alienated passwords had been derived from these trigon parameters.

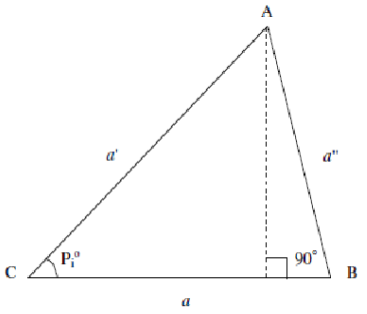
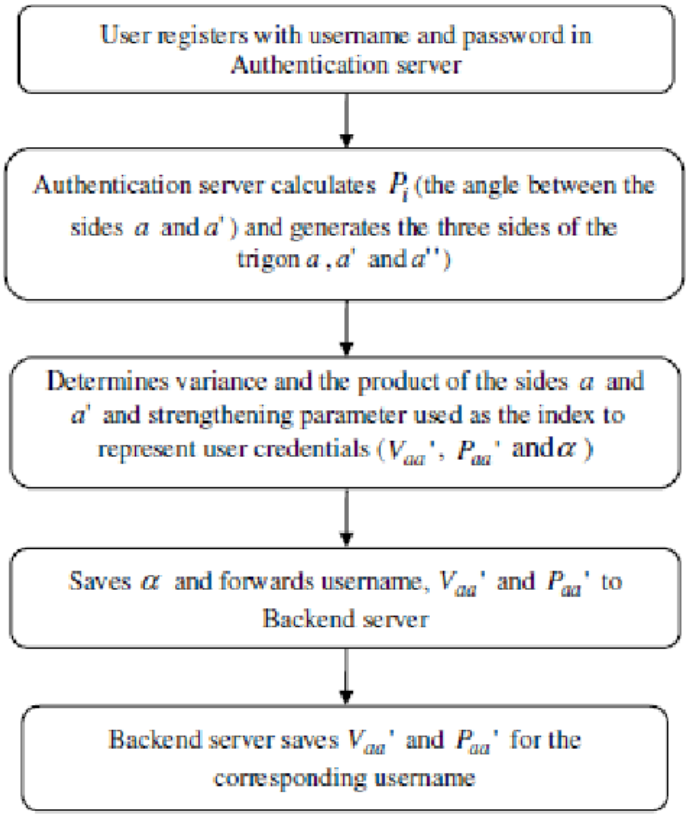


Figure 2. A sample trigon generated using the parameters a , a' , a'' and P_i



d) Encryptionless security: Winnowing and Chaffing approach [11]

It is important to seek solutions that do not rely directly on cryptography. Furthermore, another issue that arises is that use of encryption requires a substantial amount of computational resources. This is particularly so since the size of the key has to increase to protect the encrypted data. This means that the computing power available on the grid, which is the primary reason for the grid' setup, is utilized to encrypt and decrypt information rather then to perform computations.

For the issue of security in the transfer of data, an encryption-less method that still offers similar level of security, could be used. A good method that fits the bill is the Winnowing and Chaffing approach, which is summarized as below.

1. Calculate Message Authentication Code (MAC) using packet contents, packet sequence number and secret key, which is added to every packet
2. MAC is calculated using a standard algorithm like HMAC-SHA1: the parameters to this algorithm are the packet sequence number, the contents of the packet, and the secret key, which was exchanged earlier
3. Once the grid node receives a packet, it first calculates the MAC itself and then checks whether it matches with the MAC sent with the packet. If so, it “knows” that the sender is the GRB, else it discards the packet as originating from a false source.

Now, security is implemented on top of this message authentication by adding the so-called “chaff” packets. These are packets, which have the same format as the genuine data packets, but the MACs are deliberately set to the wrong value. On seeing a packet with a non-matching MAC, the grid DRM can promptly ignore it. However, any intruder monitoring traffic has no way of differentiating the right value of the MAC from the wrong, as he has no knowledge of the secret key.

6. CONCLUSION

After this report we've realized that security in Grids is in great development and there are still a lot of research in this area (also motivated by the cloud architecture growth).

In almost every papers we've read, we found a great tension between security and performance. A well balanced grid must consider very seriously this two parameters. It's a huge challenge to maintain high security levels with minimal performance degradation.

Another important conclusion is the fact that each Grid must implement its own security model. There are no perfect mechanisms to every scenario. Each grid architecture has to adapt and configure to its own Grid system the best suitable security mechanisms.

In sum, the powerful abstraction of the Grid idea, where users may not know where their data is stored, nor where their computation has been run, is at once a great strength but also a very significant security challenge.

REFERENCES

[1] I.Foster, C.Kesselman, and S.Tuecke, “The anatomy of the grid: Enabling scalable virtual organizations”, International Journal of Supercomputer Applications (2001)

[2] A. Martin, Po-Wah Yau, “ Grid Security: Next Steps ”, May 2007

[3] E. Cody, R. Sharman, R. H. Rao, S. Upadhyaya, “Security in grid computing: A review and synthesis”, Science Direct, October 2007

[4] Ian Foster , “What is the Grid? A Three Point Checklist ”, Argonne National Laboratory & University of Chicago , July 20, 2002

[5] S. Esteves, L. Veiga, P. Ferreira, “GridP2P: Resource Usage in Grids and Peer-to-Peer Systems”, INESC-ID/ IST, Lisboa

[6] Foster, I. and Kesselman, C. Computational Grids. Foster, I. and Kesselman, C. eds. The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, 1999, 2-48.

[7] S. Subashini n, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Anna University Tirunelveli, India, March 2010

[8] M.L.Jayalal, R.Jehadeesan, S. Rajeswari, S.A.V.Satya Murty, “Moving From Grid to Cloud Computing: The Challenges in an Existing Computational Grid Setup ”, International Journal of Computer Science & Communication, 2010

[9] V. Ruckmani, Dr G Sudha Sadasivam, “A novel trigon-based dual authentication protocol for enhancing security in grid environment ”, International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009

[10] R. Bhadauria, R. Chaki, N. Chaki, S. Sanyal, “A Survey on Security Issues in Cloud Computing”, School of Technology and Computer Science, 2011

[11] S. Sanyal, R.A. Vasudevan, A. Abraham, M. Paprzycki, “Grid Security and Integration with Minimal Performance Degradation”, Tata Institute of Fundamental Research, India & Oklahoma State University, USA

[12] Chi-Tung Chen, Ming-Tsun Lin, Iuon-Chang Lin, “Using Hash Tree for Delegation Revocation in Grids”, Journal of Electronic Science and Technology, VOL. 10, No. 3, September 2012

[13] Von Welch, Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman, Steven Tuecke, “Security for Grid Services”, University of Chicago, Argonne National Laboratory, University of Southern California

[14] M. Humphrey, M.R. Thompson, “Security Implications of Typical Grid Computing Usage Scenarios”, University of Virginia, Lawrence Berkeley National Laboratory

[15] J. Luna, M. Dikaiakos, M. Marazakis, T. Kyprianou, “Data-Centric Privacy Protocol for Intensive Care Grids ”, Information Technology in Biomedicine, 2010

[16] G. Fink, J Haack, B. Crouse, J. White, Errin W. Fulp, K. S. Berenhaut , “Using Swarming Agents for Scalable Security in Large Network Environments ”, Wake Forest University & Pacific Northwest National Laboratory

[17] F. Berman, G.Fox T. Hey, “The Grid: past, present, future”, San Diego Supercomputer Center, and Department of Computer Science and Engineering, University of California, San Diego, California, Indiana University, Bloomington, Indiana, EPSRC, Swindon, United Kingdom, University of Southampton

[18] Hai Jin, “Grid Computing”, Huazhong University of Science and Technology,

[19] Grid Security Workshop, Oxford, July 2004