

# Chapter 4.12

## Data Protection and Data Security Regarding Grid Computing in Biomedical Research

**Yassene Mohammed**  
*Georg-August-University, Germany*

**Fred Viezens**  
*Georg-August-University, Germany*

**Frank Dickmann**  
*Georg-August-University, Germany*

**Ulrich Sax**  
*Georg-August-University, Germany*

**Jürgen Falkner**  
*Fraunhofer Institute for Industrial Engineering  
IAO, Germany*

**Thomas Lingner**  
*Georg-August-University, Germany*

**Dagmar Krefting**  
*University Medicine Berlin, Germany*

### ABSTRACT

*This chapter describes security and privacy issues within the scope of biomedical Grid Computing. Grid Computing is of rising interest for life sciences (Konagaya, 2006) and has been used since many years in sciences like high energy physics. Anyhow, medical applications on the grid require a special focus on data security and data protection issues. Based on general security and privacy rules, the authors describe the current state of the art of grid security. Then they describe which additional security measures have to be established in different biomedical grid scenarios. Legal aspects have to be taken into account as well as the current possibilities and flaws of grid security technology. Describing the enhanced security concept in MediGRID (MediGRID, 2005) they outline how medical Grid Computing could fulfill privacy regulations used in more demanding environments.*

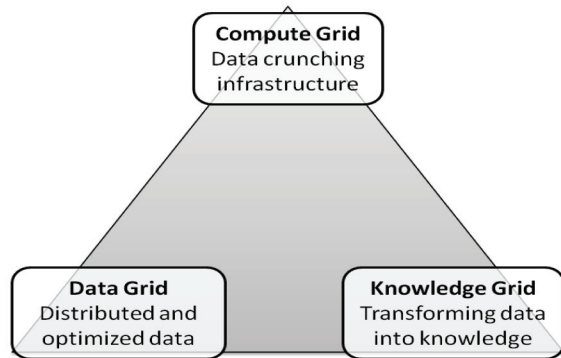
### INTRODUCTION

Following the power grid paradigm, Grid computing implies, that a grid user has easy and transparent access to compute power, storage resources, data,

and applications (I. Foster & Kesselmann, 1999). In practice there are still some hurdles in doing so. Nevertheless Grid Computing will become a key infrastructural component on the way to a broadly applied computational medicine (EU-SHARE, 2006; Iakovidis, 2005). In this context HealthGrid contains three aspects: the computing

DOI: 10.4018/978-1-4666-0879-5.ch4.12

Figure 1. Three aspects of grid-functions in health-care (adapted from Iakovidis, 2005)



aspect for highly intense calculation tasks, the data aspect for distributed access to a large amount of data and the knowledge aspect for a sophisticated utilization of data (Figure 1).

Within biomedical Grid projects, a grid infrastructure for medical and biomedical research has been established mainly using Computing Grid resources. It enhances interdisciplinary and widely location-independent collaboration of researchers. The interoperability between different medical and biomedical grids provides a broader range of applications and datasets for the biomedical applications and provides opportunities for new collaborations (Montagnat et al., 2008).

Concerning security matters of medical and biomedical applications, different types of grid usage need different security levels according to legal and ethical (Iavindrasana et al., 2008) requirements as well as Good Clinical Practice GCP (Mohammed, 2006). These requirements include privacy as well as intellectual property issues. Whereas privacy addresses confidentiality of identifying data of patients and intellectual property is directed to protect clinical and research information from unauthorized access. Trust in privacy upholds patients trust in health services. Without trust patients might avoid healthcare services which can lead to severe problems, for the patient but nonetheless for the whole healthcare

system of a society. Also beyond doubt scientists and healthcare professionals need to have full confidence in the offered grid infrastructure in order to store their precious data onto the Data Grid. Thus technical implementations must ensure a reliable confidentiality of any information transfer and storage. (Garcia, Dikaiakos, Kyprianou, Bilas, & Marazakis, 2008)

While Computing Grid applications have to decide whether a user may use one resource or not, Data Grid applications can only be operated securely with fine grained access control with respect to data elements. Security solutions for Knowledge Grids still have to be outlined, as liability requirements have to be met additionally.

Regarding access control for the Computing Grid scenario, most authentication and authorizations challenges are solved due to the usage of grid proxy certificates and virtual organization solutions (Pommerening, 2006). Fine grained access control solutions - the right to access one document within a data store, or even accessing different sections within the same document (e.g. medical structured documents) - are still under development (Mohammed, Sax, Viezens, & Rienhoff, 2007; Schiffers, 2008; Witzig, 2008).

For Data Grid applications in patient care and medical research the usage of international standardized ontologies, terminologies and nomenclatures is essential (Blanquer, Hernandez, & Segrelles, 2006). The problem of how to establish data repositories using standardized terminologies could not be solved by the grid projects yet, although for example caBIG and caGRID (Oster et al., 2007; Welch et al., 2003) try to tackle those issues. Knowledge Grid applications are not to be found yet in biomedical Grid Computing (Konagaya, 2006).

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/data-protection-data-security-regarding/64525](http://www.igi-global.com/chapter/data-protection-data-security-regarding/64525)

## Related Content

---

### Mind Genomics With Big Data for Digital Marketing on the Internet

Jakob Salom (2021). *Handbook of Research on Methodologies and Applications of Supercomputing* (pp. 282-289).

[www.irma-international.org/chapter/mind-genomics-with-big-data-for-digital-marketing-on-the-internet/273407](http://www.irma-international.org/chapter/mind-genomics-with-big-data-for-digital-marketing-on-the-internet/273407)

### Distributed Adaptive Windowed Stream Join Processing

Tri Minh Tran and Byung Suk Lee (2013). *Development of Distributed Systems from Design to Application and Maintenance* (pp. 102-126).

[www.irma-international.org/chapter/distributed-adaptive-windowed-stream-join/72249](http://www.irma-international.org/chapter/distributed-adaptive-windowed-stream-join/72249)

### A NoC-Based Infrastructure to Enable Dynamic Self Reconfigurable Systems

Leandro Möller, Ismael Grehs, Ewerson Carvalho, Rafael Soares, Ney Calazans and Fernando Moraes (2010). *Dynamic Reconfigurable Network-on-Chip Design: Innovations for Computational Processing and Communication* (pp. 1-27).

[www.irma-international.org/chapter/noc-based-infrastructure-enable-dynamic/44219](http://www.irma-international.org/chapter/noc-based-infrastructure-enable-dynamic/44219)

### Grid Service Level Agreements Using Financial Risk Analysis Techniques

Bin Li and Lee Gillam (2010). *Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications* (pp. 686-710).

[www.irma-international.org/chapter/grid-service-level-agreements-using/40823](http://www.irma-international.org/chapter/grid-service-level-agreements-using/40823)

### Transforming the Method of Least Squares to the Dataflow Paradigm

Illir Murturi (2021). *Handbook of Research on Methodologies and Applications of Supercomputing* (pp. 114-121).

[www.irma-international.org/chapter/transforming-the-method-of-least-squares-to-the-dataflow-paradigm/273398](http://www.irma-international.org/chapter/transforming-the-method-of-least-squares-to-the-dataflow-paradigm/273398)