INTEGRATING MULTI-DISCIPLINARY RESEARCH THROUGH ACADEMIC GRID COMPUTING

INTEGRAREA CERCETĂRII ŞTIINŢIFICE MULTIDISCIPLINARE PRIN GRID COMPUTING ACADEMIC

CĂLIN M., CHIRUŢĂ C., FILIPOV F.
University of Agricultural Sciences and Veterinary Medicine of Iasi, Romania

Abstract. *Grid Computing technologies have the potential of dramatically changing the use of computers in solving problems. Complex Grid Computing projects are under development worldwide. The paper presents the mainlines of the concept and mentions a number of such systems that had impact on different branches of agriculture. An academic Grid computing project that joins forces of four universities and one research institute of Iasi, Romania, is also described.*

Rezumat. *Tehnologiile Grid Computing au potenţialul de a schimba în mod dramatic utilizarea calculatoarelor în rezolvarea celor mai diverse probleme. Pe plan mondial sunt în diferite faze de dezvoltare proiecte complexe de tip Grid Computing. În lucrare sunt prezentate caracteristicile principale ale conceptului şi sunt menţionate câteva astfel de sisteme în care agricultura are un rol important. Este prezentat, de asemenea, un proiect dezvoltat în colaborare de patru universităţi şi un institut de cercetare din Iaşi. Printre parteneri se numără şi USAMV Iaşi.*

INTRODUCTION

Grid Computing is a modern concept that emerged in the last decade. It denominates an advanced infrastructural proposal for parallel/distributed computing that implies using component organized software that runs on a large number of computers [1]. The practical situations that led to this approach were linked to a series of issues that appeared more and more frequently in using computers in problem solving. Some of them are enumerated further on:

- the need for increasing computational power and storing capacities;
- the need to access databases being stored on different computers, maintained by different organizations and having different data structures;
- the need to access software applications that run on remote computers and to use their outputs on a synergic manner;
- the need for efficient and secure multi-disciplinary cooperation within research programs.

By its nature, agriculture is a field in which research and production require large scale coordination of efforts both at a geographical level as well as from a multi-disciplinary point of view. In this respect, the benefits that Grid computing can bring were accounted and powerful Grid projects were developed worldwide to integrate different agricultural branches with other fields of activity. Some relevant achievements in this direction are subsequently pointed out.

In the USA, two relevant examples can be pointed out. One of them is the Colorado State University project for a national animal identification system that will rely on Grid computing technology to process massive amounts of animal tracking data [5]. Another example of Grid system with agricultural purpose is the partnership between the US Cornell Theory Center (CTC) and Cornell's College of Agriculture and Life Sciences that focuses on using CTC's computational infrastructure and expertise to develop science-based technologies support of farmers [2].

In Japan, the National Agriculture Research Center, Tsukuba, is developing a project named *GRID for Agricultural Decision Support* [3]. The basic premise for starting this project was that in agriculture one must combine data from various different databases such as weather data, soil data, crop data and market data. This data is available on geographically widespread computers.

As genetic research [4] has an important impact on agricultural sciences, a European Grid Computing initiative in this field must be mentioned. The project is developed by the European Bioinformatics Institute (EBI), a non-profit academic organization that ensures that the growing body of information from molecular biology and genome research is placed in the public domain and is accessible freely. The EBI serves researchers in molecular biology, genetics, medicine and agriculture from academia, and the agricultural biotechnology.

THE GRAI PROJECT

In 2006, four faculties and a research institute in Iasi, Romania started the research project named *Academic Grid for Complex Applications*. The acronym of the project is GRAI and it runs under a CEEX grant (the excellence research framework created by the Romanian Ministry of Education and Research following the EU FD7 model). The five participants in the project are:

- The Technical University of Iasi, Faculty of Automatic Control and Computer Engineering (code name UTI-CE), which also holds the leadership of the GRAI project;
- Institute for Computer Science, Romanian Academy, in the location of the Faculty of Electronics and Telecommunication (code name AR-IIT);
- The “Al. I. Cuza” University of Iasi, Faculty of Computer Science (code name UAIC-I);
- The University of Medicine and Pharmacy Iasi, Faculty of Biomedical Engineering(code name UMF-B);
- The University of Agricultural Sciences and Veterinary Medicine of Iasi, Faculty of Horticulture (code name USAMV-H).

The GRAI project aims to develop a grid computing structure for research and for other academic purposes. To achieve them, two main directions must be followed:

1. Development of a grid computing system that would interconnect the scientific and computational resources of the five partners.
2. Development of grid services and specific applications based on them.

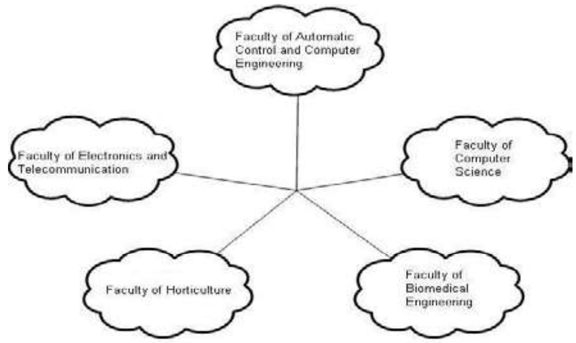
Faculty of Automatic Control and Computer Engineering
Faculty of Electronics and Telecommunication
Faculty of Computer Science
Faculty of Horticulture
Faculty of Biomedical Engineering

Figure 1 - The GRAI network

The computational resource of the grid will be geographically situated (figure 1) in the five locations of the project partners:

Each of the five locations will have a grid node that includes a high performance server and a group of workstations (figure 2). These workstations will be used both as computing support within the grid and in developing grid services and applications.

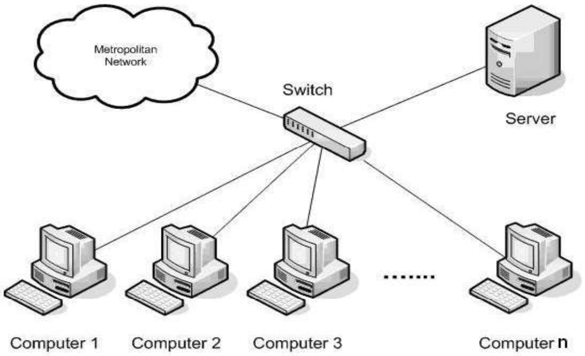

Figure 2 - Node structure

The University of Agricultural Sciences and Veterinary Medicine of Iasi (partner USAMV-H) participates in the project not only with computational power, but also with research in developing multi-disciplinary applications based on the grid services that will intensively use the GRAI Grid resources. Some directions are enumerated further on.

Decision Support. This activity is a natural continuation of previous multi-disciplinary research programs approached the domain of Decision Support Systems (DSS) at USAMV-H. New algorithms for different situations are currently under study. These algorithms are meant to be useful in practical applications. The project partner USAMV-H will design and implement a DSS whose goal is to support decisions regarding the durable exploitation of pedoclimatic resources in horticulture.

E-learning. In the domain of e-learning there are many things to be done in agricultural higher education, as the potential of this approach is not yet used in appropriate way. USAMV-H can benefit of the research expertise that the partner UAIC-I has in the domain to develop e-learning modules.

Data mining. This modern domain emerged at first as a profit oriented economic research activity, but subsequent studies showed its potential to solve decision problems in different areas. USAMV-H can cooperate with the partners UTI-CE and UAIC-I to develop agricultural applications of data mining algorithms.

As one can see, the development of the GRAI academic grid will bring benefits on all of the directions that were pointed out in the introductory section as demands that led to the success of the Grid Computing concept. All partners will have their parts of contribution and benefit, but only the ones specific to the agricultural research were emphasized here.

Grid computing networks are long term projects which finally bring undoubted benefits that can be measured through financial effect, scientific and social impact. However, they have an initial costly investment phase and the discussed worldwide examples reveal that both government agencies and private companies participated with money and equipments software in building an appropriate infrastructure.

CONCLUSIONS

The Grid Computing is a long-term, complex, but cost effective approach.

In several American, European and Asian countries, the usefulness of Grid computing for agricultural research and production was already proved.

The perspective of integration with the European Community demands the development of such entities that are already active in many European Countries.

The development of the GRAI project by several academic institutions of Iasi, Romania, follows this line of action.

REFERENCES

1. **Aflori, C., Craus, M., Sova, I., Butincu, C., Leon, F., Amarandei, C-M., 2006** - *GRID, Tehnologii si aplicatii*. Ed. Politehnium, Iasi.
2. **Emmen, A., 2004** - *Cornell Theory Center and College of Agriculture and Life Sciences partner*. Primeur Monthly, http://www.hoise.com/primeur/04/articles/monthly/AE-PR-08-04-23.html.
3. **Ninomiya, S., 2002** - *Network Computing for Agricultural Information Systems -GRID for Agricultural Decision Support*. Proc. 3rd AFITA; Asian Agricultural Information Technology and Management. Ed. F. Mei: 26-30.
4. **xxx., 2002** - *European Bioinformatics Institute Enters GRID with Platform Computing* http://www.platform.com/Newsroom/Press.Releases/2002/PR.01-22-2002.htm.
5. **xxx., 2005** - *Grid Powers Nat'l Animal Tracking System at Colorado State*. GRIDToday, http://www.gridtoday.com/grid/392144.html.

DATA SECURITY

SECURITATEA DATELOR

POP IOANA, ALDEA FLORICA, MICULA MARIA
University of Agricultural Sciences and Veterinary Medicine Cluj-Napoca

Abstract. *Security is fundamentally about protecting assets and it represents a continuous process not a destination. In this paper we identify the basic elements of security and using It security principles we give possible solutions for secure applications.*

Rezumat. *Prezentul articol isi propune sa identifice problemele care apar in securizarea datelor si sa ofere solutii de securizare a acestora. Datorita progresului stiintific asigurarea securitatii datelor reprezinta un proces continuu si de aceea principiile avute in vedere prezinta un mare caracter de adaptabilitate a solutiilor prezentate.*

INTRODUCTION

Security is fundamentally about protecting assets. In our case, assets may be tangible items, such as a Web page, your customer database or credit card information, or they may be less tangible, such as your company's reputation. Security is a continuous process, not a destination. As you analyze your infrastructure and applications, you identify potential threats and understand that each threat presents a degree of risk.

IT security is a critical element in the system life-cycle. Security must be incorporated and addressed from the initial planning and design phases to disposal of the system, because in time, the threats are changing and evolving.

Security is many times costly and rigid so we have to identify potential trade-offs between reducing risk on one side, increased costs and decrease in other aspects of operational effectiveness on the other side. The objective is to reduce risk to an acceptable level. In other words, security is about risk management and implementing effective countermeasures.

Security is also a question of discipline and training. From simple users to system administrators and program managers, everyone should have a basic understanding of the security principles governing the system they are using

BASIC ELEMENTS OF SECURITY

Security relies on the following elements:

- **Authentication:** Authentication addresses the question: who are you? It is the process of uniquely identifying who is trying to use the computing resources such as files, services, disk space, databases, network connections, devices, etc. These might be end-users, other services, processes, or computers. In security terms, authenticated clients are referred to as *principals*.

- **Authorization** addresses the question: what can you do? It is the process that governs the resources and operations that the authenticated client is permitted to access. This process is checking if the principal has the right to use a certain resource or operation and also the allowed access rights (read-only, read-write, execute, append, shared-mode or exclusive-mode, etc.). The access rights can be defined at high-level, such as a database, but also al low-lever such as a table row or system-level resources (registry keys and configuration data). Operations include performing transactions or accessing a program option, such as setting or changing customer data. Authorization is also including licensing issues, copyright protection, special behavior or functional limitations of illegal copies, concurrent access limitations.
- **Auditing** Effective auditing and logging is about keeping a track of the resource accessing and operations performing. This mechanism guarantees that a user cannot deny performing an operation, accessing a file or database, etc. For example, in an e-commerce system, this mechanism is required to make sure that a consumer cannot deny the order. It can also be used to be able to undo database changes, or other operations.
- **Confidentiality** also referred to as *privacy*, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users that are trying to access data directly or by network monitoring applications that are intercepting data packets crossing the network. Encryption is frequently used to enforce confidentiality. Access control lists (ACLs) are another means of enforcing confidentiality.
- **Integrity** is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks. Using hashing techniques, checksums or other message authentication codes typically provides integrity for data in transit. Auditing and journaling file-systems are also helpful to recovery the lost data.
- **Availability** From a security perspective, availability means that systems remain available for legitimate users. The goal for many attackers with denial of service (DoS) attacks is to crash an application or to make sure that it is sufficiently overwhelmed so that other users cannot access the application.

THREATS, VULNERABILITIES, AND ATTACKS

A threat is any potential occurrence, malicious or otherwise, that could harm an asset. In other words, a threat is any bad thing that can happen to your assets.

Vulnerability is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques. Weak input validation is an example of an application layer vulnerability, which can result in input attacks.

An attack is an action that exploits vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application or flooding a network, a computer or a process in an attempt to deny service.

To summarize, a threat is a potential event that can adversely affect an asset, whereas a successful attack exploits vulnerabilities in your system.

BUILDING SECURE APPLICATIONS

It is not possible to design and build a secure application until you know your threats. An increasingly important discipline and a recommended part of the application's design phase is threat modeling. The purpose of threat modeling is to analyze the application's architecture and design and identify potentially vulnerable areas that may allow a user, mistakenly or not, or an attacker with malicious intent, to compromise your system's security.

After you know the threats, you have to design the application by applying timeworn and proven security principles. Developers must follow secure coding techniques to obtain secure, robust, and hack-resilient solutions. A secure network, host, and application configuration must follow the design and development of secured application on the servers where the application software is to be deployed.

1. **User and Code Security** Modern operating systems and software development environments such as .NET Framework, supports two complementary forms of security: User security and Code security. User security refers to who is the user and what can the user do, while code security answers the questions "where is the code from, which wrote the code, and what can the code do?" Code security involves authorizing the application (not the user) to access system-level resources, including the file system, registry, network, and databases. For example, some web pages include small executables (scripting code, ActiveX controls, Java modules, etc) that are launched in the web-browser when that page is loaded. In this case, it does not matter who the end user is, or which user account runs the code, but it does matter what the code is and is not allowed to do, if a certain company authenticated that code, is scripting-safe etc.

2. **Common Criteria** The Common Criteria (CC) is a repeatable methodology for documenting IT security requirements, documenting and validating product security capabilities, and promoting international cooperation in the area of IT security. Use of Common Criteria "protection profiles" and "security targets" greatly aids the development of products or systems that have IT security functions. The rigor and repeatability of the Common Criteria methodology provides for thorough definition of user security needs. Validated security targets provide system integrators with key information needed in the procurement of security components and implementation of secure IT. The approach of this document meshes with the Common Criteria methodology.

The principles described here do not apply to all systems at all times. Yet each principle should be carefully considered throughout the life-cycle of every system. Moreover, because of the constantly changing information system security environment, the principles identified are not considered to be an inclusive list. Instead, this document is an attempt to present in a logical fashion fundamental security principle that can be used in today's operational environments. As technology improves and security techniques are refined, additions, deletions, and refinement of these security principles will be required.

3. IT Security Principles

- Establish a sound security policy as the "foundation" for design.
- Treat security as an integral part of the overall system design.
- Clearly delineate the physical and logical security boundaries governed by associated security policies.
- Reduce risk to an acceptable level.
- Assume that external systems are insecure.
- Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
- Implement layered security (Ensure no single point of vulnerability).
- Implement tailored system security measures to meet organizational security goals.
- Strive for simplicity.
- Design and operate an IT system to limit vulnerability and to be resilient in response.
- Implement security through a combination of measures distributed physically and logically.
- Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- Formulate security measures to address multiple overlapping information domains.
- Isolate public access systems from mission critical resources
- Use boundary mechanisms to separate computing systems and network infrastructures.
- Base security on open standards for portability and interoperability.
- Use common language in developing security requirements.

REFERENCES

1. **Bidgoli H.,** 2006 - *Handbook Of Information Security, Ed. Wiley.*
2. **Denning Dorothy,** 1983 - *Cryptography & Data Security*, Addison-Wesley.
3. **Lehtinen R., Gangemi G.T.**, 2006 - Sr., *Computer Security Basics* **,** O'Reilly,
4. **Patriciu V. V., Voicu N.**, 2004 - *Securitatea comertului electronic* Teora.
5. **SamsNet**, 2003 - *Securitatea in internet*, Teora.